THE UNIVERSITY *of* EDINBURGH

The Credentialisation of Identification: How Digital ID Wallets Shape Digital Identification, Citizenship and Power

Isadora Dullaert

PhD in Sociology
University of Edinburgh
August 2024

Declaration

I declare that this thesis has been composed solely by myself and that it has not been submitted, in whole or in part, in any previous application for a degree. Except where states otherwise by reference or acknowledgment, the work presented is entirely my own.

Isadora Dullaert

Abstract

This dissertation looks at the European Digital Identity (EUDI) Wallet: an app that will store digital versions of identity documents, as well as other information- ranging from social security numbers to supermarket loyalty cards- and aims to put citizens in control of these personal data. Specifically, the dissertation investigates the technological arrangement, Self-Sovereign Identity (SSI) technology, that underpins this wallet, illustrating that this set of technologies and ideas that was originally developed for the internet found its way to the heart of state-backed identification practices in the European Union. In light of this shift, the dissertation investigates how the wallet shapes digital citizenship, as well as the new power dynamics that it brings about. In so doing, it aims to elucidate the shifting sites of power in contemporary governance.

While the dissertation situates itself in two main sociological literatures, digital sociology and political sociology, it also borrows from science and technology studies. Drawing on interviews, field work at industry events and documentary research, the dissertation argues that the shift to a wallet-based identification system is not just technological; it also signifies an important societal change, which will have real implications for how identification is 'done', and how citizens gain access to services. The dissertation develops the concept of 'credentialisation' to analyse how the wallet turns different and previously separate parts of people's lives into 'verifiable' information. As this information is subsequently brought together in one wallet, this signifies the collapse of different social institutions and roles into one technical system. This, the dissertation argues, has significant consequences, because 1.) it produces a new subject- a 'user-citizen'- who is supposed to be tech-savvy and responsible, and has to decide (to an extent) on the terms of their own datafication, and 2.) it instantiates new power dynamics around identification, as there is simultaneous competition over and collaboration between state and corporate actors concerning the design of digital ID wallets. One of the first in-depth studies on this topic, this dissertation contributes to the literature on digital identification and digital citizenship, demonstrating that state-issued identification is changing, as the credentialisation of identification gives rise to new technologies, new digital citizens, and new power dynamics.

Lay summary

This dissertation looks at the European Digital Identity (EUDI) Wallet, which will eventually be an app that can be downloaded onto smartphones, and which will store different kinds of personal data such as a digital version of an ID card, but also information like supermarket loyalty cards or train tickets. An important promise of the wallet is that it will put citizens in control of the data that they store in it. The dissertation argues that the EUDI Wallet changes how identification works, and how citizens gain access to services. It makes the argument that 'credentials' play a crucial role in this, because this is a new way of storing personal data, which makes it possible to access different kinds of services through the wallet. For example, using the same wallet, it will be possible to cross a border, but also to buy a new pair of trousers online. The focus of the dissertation is three-pronged. First, it explores how a technology ('self-sovereign identity technology') that was developed for the internet is now being used in the context of the EU. This means that it is now used for citizens of EU states, instead of users of the internet. Second, it examines the new role that citizens are expected to take up in this system, and the potential (harmful) implications of this. Third, it scrutinises new power structures around digital ID wallets, and the involvement of (Big Tech) companies in particular, demonstrating that states are no longer the only ones in charge of identification.

Acknowledgements

I would like to express my gratitude to my supervisors, Dr Gezim Krasniqi and Dr Karen Gregory. Thank you for encouraging me to explore and trusting that I would get there. I would like to thank Gezim for supporting me, engaging with my thoughts, and helping me develop them, from the very beginning of my master's programme to the very end of my PhD. I would like to thank Karen for her enthusiasm, ideas, and for helping me develop my sociological imagination.

I would also like to thank other, former mentors: Dr Jay Huang, who first planted the 'PhD seed', and Dr Michael Rosie, who encouraged me to apply. I would like to thank Dr Liliana Riga and Professor Jonathan Hearn for their helpful comments during my first-year board review. Thank you Dr Pedro Jacobetty, for the friendly advice during my second year. Thank you to Dr Ben Collier and Dr Arne Hintz, for the interesting discussion and your kind feedback during my viva.

Finding my academic community after two lonely pandemic years was one of the highlights of my PhD: a massive thank you to my friends at the Platform Social, Elif Buse Doyuran, Joe Noteboom, Addie McGowan, Stella Kyratzi, Meenakshi Mani, Jim Doran, Cathy Hills, Ari Stillman and Gemma Milne. I cannot express how much it meant to me. Thank you to my office mates, Thijs Keulen and Jaida Keaveney, for the daily chats, check-ins, and brightening grey office days. Thank you to my fellow traveller Andi Haxhiu: I can't believe it has been 6 years, and I hope we graduate together. Thank you to Ellen Frank Delgado (and Lottie) for the weekly walks during lockdown – and a special thank you to Ellen and Elif for the cosy evenings and continuous support when we went 'back to normal'.

Thank you to my best friends, for always being there for me. Geerte, the phone calls, postcards (and the 60 message at a time system) lifted me up; thank you for reminding me of what is important. Nelly, I am grateful for our walks and times at the allotment; thank you for making me feel grounded. Claudia, our 'long distance friendship' worked so well. Knowing that you were cheering me on was a really big help. A special thank you to my long-eared friends Auguste, Theo, and Dottie for the extraordinary emotional support.

Thank you, Sam, for being the best partner I could have asked for. Our walks, camps, Sainsbury's treats, and your boundless patience and support sustained me. Now that both of our PhD journeys have come to an end, I can't wait for our next adventure together.

Finally, I would like to thank my family. My parents, Inge and Marc, who have supported me in every way. Without the curiosity and the care for the world around us that you instilled in me, this PhD would not have happened. Thank you for your unlimited support: the phone calls, zoom dinners and endless kitchen table chats meant the world to me. Thank you to my brothers, Julius and Floriaen, for always having my back. Finally, I would like to thank my grandparents, who always believed in me: my grandfather Leo, who called me 'Frau Doktor' since I was very small, and my grandmother An, who was so proud that I could go to school for so long. While they are sadly not here to see this project finish, they did see it start. I would like to dedicate this to them.

To Leo Dullaert and An Ikink-Engels

Table of contents

List of abbreviations

AML	Anti-Money Laundering
ARF	Architecture Reference Framework
DID	Decentralised Identifier
DLT	Distributed Ledger Technology
DMA	Digital Markets Act
DSA	Digital Services Act
EC	European Commission
eIDAS	Electronic Identification, Authentication and Trust Services
EU	European Union
EUDI Wallet	European Digital Identity Wallet
GDPR	General Data Protection Regulation
KYC	Know Your Customer
PID	Personal Identification Data
SDG	Sustainable Development Goals
SSI	Self-Sovereign Identity
UN	United Nations
VC	Verifiable Credential
VLOPs	Very Large Online Platforms

Chapter 1. Introduction

When the large gate had been opened, I drove onto the estate, following the small road towards the sizeable 17th-century country house overlooking the lake. While three members of staff were lined up on the ramp, a fourth valet-parked my small blue Citroen C1 with the monster of Loch Ness toy in the windshield alongside the Audi's and Land Rovers. Once inside, I was led to the room where the meeting was taking place. On the large mahogany table- described in the invitation as 'iconic'– sat a notepad with the country house's letterhead, a gold-coloured pen, and a bottle of still water for every guest.

I thought to myself: how did I get here? The same feeling struck me when I was barbecuing with a group of hyper-specialised technologists on a sunlit balcony in Switzerland, or at an identity fair in a refurbished brewery, dress code 'California casual'. It turns out that researching identification leads you to unexpected places. Identification has become an industry, where 'identity solutions' are offered to states, companies, NGOs and everything in between; an industry with a market size of tens of billions of dollars (Statista, 2024). It has its own politics, celebrities, and jargon.

It has gotten this big, because identification has become the starting point for most of our digital transactions. When we think about it, many of our daily actions include some form of identification or verification. On a typical morning, we might log onto Instagram or open our banking app to transfer rent. We could then stop by the post office, show our driver's license to receive a parcel, travel to work and give ourselves access to the building by swiping our employee card. These actions are often mundane and performed thoughtlessly. Some things might give us more of a pause, like showing our passport at border control or gathering the necessary documents to open a bank account. However, these are all examples of transactions where we need to prove that we really are who we claim to be, or are entitled to receive something; be it a parcel, the right to cross a border, or access to a building.

Soon, all these actions could be performed through one app: a digital ID wallet. While digital wallets have been around in the world of payments for a decade (Costronova and Fairfield, 2014), digital ID wallets are only just emerging. As the name suggests, these wallets will be able to store digital versions of identity documents such as passports, ID cards, and driving licenses. Apps that can be downloaded onto mobile phones, these wallets will- or so is the hope- make it easier to identify ourselves in various situations. As mentioned above, this identification process can take place in different locations, ranging from a post office, to a border, to on an online platform. What is more, digital ID wallets will be able to do more than help us identify ourselves in traditional ways: they will also store things like supermarket loyalty cards, social security numbers, and train tickets. While we have been able to store some documents, such as plane tickets, in existing digital wallets for a while, digital ID wallets set themselves apart because they will store any kind of information that allows someone to 'prove' who they are or that they are entitled to something. Moreover, they blur the boundaries between physical and online identification: suddenly it becomes possible to use a digital ID card

to prove our age on the internet- to buy alcohol online or to sign up to a social media platform, for example. Importantly, one of the main promises of digital ID wallets is that users will be in control of the personal data that they share. This puts these wallets in conversation with some of the pressing digital issues of these times, such as datafication (Cukier and Schönberger, 2013) and, relatedly, surveillance capitalism (Zuboff, 2019). As such, digital ID wallets are often presented as revolutionary technology, which will empower their users. At the same time, digital ID wallets may make identification more ubiquitous than ever before: they will be identification systems that we take wherever we go, folding different aspects of our lives into one app.

This dissertation looks at one such wallet that is currently under development: the European Digital Identity (EUDI) Wallet. More specifically, it investigates the technological arrangement, Self-Sovereign Identity (SSI) technology, that underpins this wallet, illustrating that this set of technologies and ideas that was originally developed for the internet, found its way to the heart of state-backed identification practices in the European Union (EU). SSI is a complex concept, which comes with a set of imaginaries, values, and promises for the future; its main promise being that it will put individuals in control of their personal data and digital identity (Tobin and Reed, 2016). The EUDI Wallet, currently the foremost implementation of SSI technology[1] will eventually be a digital ID wallet like the one I described above. It is also one of the first state-sanctioned digital wallets, which would allow citizens, residents, and businesses to identify themselves across the EU. Currently in the pilot phase, it has been described as a 'huge laboratory' for digital ID wallets (Wired, n.d.).

Exploring this shift to a wallet-based identification system, this dissertation investigates the changing nature of state-sanctioned identification practices. It situates the EUDI Wallet in the longer history of identification technologies and, in doing so, illustrates that SSI, an 'identity model' developed for the internet, has found its way to heart of state-based identification practices. In light of this shift, the dissertation investigates how the wallet shapes digital citizenship, and the new power dynamics that it brings about. In doing so, it aims to elucidate the shifting sites of power in contemporary governance. This is necessary, because the creation of the wallet involves a new assemblage of internet, state and corporate actors, which redefines what identification looks like. This has important consequences, because 1.) the relationship between citizens and the state is reconsidered through the promises of the wallet, and 2.) it calls into question the role of the state in identification practices more generally, as it is increasingly reliant on other actors.

The dissertation situates itself in two main sociological literatures: digital sociology and political sociology, and borrows from science and technology studies. Its intended audience is therefore a multidisciplinary one. Because of its focus on power and the changing meaning of (digital) citizenship, this dissertation of interest for political sociologists. The dissertation would be relevant for digital sociologists who are interested in macro structures such as (changing) institutions as well. However, this work is applicable beyond sociology alone: it is also of interest

[1] Though some, as I will show in chapter 4, argue that the EUDI Wallet is not 'pure' SSI.

to science and technology scholars interested in the (creation and implementation of) infrastructure. Finally, due to its empirical approach, this work also bears relevance for digital anthropologists who are interested how the implementation of new technology (re)shapes social relations.

The dissertation draws on interviews, field work at industry events, and documentary analysis to investigate the sociotechnical imaginaries that shape SSI and the EUDI Wallet, as well as the power dynamics that underpin it. It argues that the shift to a wallet-based identification system is not just technological; it also signifies an important societal change, which will have real consequences for how identification is 'done', and how people gain access to services. Through a process which I term 'credentialisation' – and which I will elaborate below- the wallet turns different and previously separate parts of people's lives into 'verifiable' information. This information is subsequently brought together in one wallet, signifying the collapse of social roles and institutions into one technical system. This, I argue, has significant consequences, because 1.) it produces a new subject- the 'user-citizen'- who is supposed to be tech-savvy and responsible, and has to decide (to an extent) on the terms of their own datafication, and 2.) it instantiates new power dynamics around identification, as there is simultaneous competition over and collaboration between state and corporate actors concerning the design of digital ID wallets.

While EUDI Wallet echoes other social credit systems, for example Chinese credit score systems (see e.g. Liang et al., 2018) which also aggregate various data and therefore allow to trace people across systems, the EUDI Wallet is different. This is because it explicitly presents an alternative to non-consensual data capturing and tracing (where citizens are supposed to be in control), and focuses on identification rather than an award and punishment system. Similarly, the EUDI wallet is also different from 'superapps' (Jia et al., 2022; Steinberg et al., 2022). This is because superapps typically include various, smaller apps as well as different services (Van der Vlist et al., 2024), but identification is not their primary purpose. While superapps might include an identity document, they are not specifically tailored to identification in the way the EUDI wallet is.

In some ways, digital ID wallets are new: they bring together new assemblages, speak to new (data-related) challenges, and create a new subject of these identification processes. At the same time, however, they represent a continuation of older identification regimes built around documents like passports and ID cards. Importantly, identification processes embed individuals into larger structures; be it users of the internet or citizens of the state. Identification is a social relationship infused with power: it is a means to establish a unique 'identity' for someone so that they can be differentiated from other persons, while at the same time making them part of a collective, such as a citizenry (Caplan and Torpey, 2001; Brensinger and Eyal, 2021). As such, identification processes establish a link between the individual and the collective, and between citizens and the state; they are a way of organising the social structure, and the role that individuals play in it. With this, this topic becomes deeply sociological.

1.1. Credentialisation

One of the key arguments of this dissertation is that the wallet signifies a significant societal shift, due to what I term the process of 'credentialisation'. The word 'credential' is derived from one of the technical building blocks of SSI. In its technical definition, it is a data format, which contains verifiable information about someone (Tobin, 2023). Examples are attributes (like height or age), relationships (like citizenship or parent), or entitlements (like rights or membership rewards) (Reed, Joosten and Van Deventer, 2021). I will further elaborate on its technical meaning in chapter 4.

Here, I develop 'credentialisation' as a social process. While credentials can to an extent be seen as the digitised versions of identification documents that we already have, I argue that credentialisation is more than that, as anything could be credential (Tobin, 2023). As such, it refers to a process where different, previously separate parts of people's lives are turned into 'verifiable' information and assembled in one place: the wallet. What is more, the wallet brings together different types of identification mechanisms as well; most notably identification systems belonging to the state and the internet. I identify three interrelated key elements of credentialisation:

1. It turns personal data into a standardised, verifiable format. Credentials are a standardised format containing 'high quality' data. This data is considered to be 'high quality' and valuable because it can be verified. This reflects is a deep concern with knowing: credentials are supposed to 'prove' that people are who they claim to be, or what they are entitled to. Where datafication is characterised by the collection of massive amounts of imprecise data, which produces a new way of knowing (Cukier and Schönberger, 2013), credentials contain very precise and 'high quality' data. Therefore, whether the data is valid and 'real' can – through an arrangement of technologies such as cryptography- be checked with the very source that issued it (without that source knowing that this happened).
2. It works to make people 'machine readable'. These credentials therefore turn different, separate aspects of people's lives into bitesize pieces of information that technology can read and verify. This extends beyond traditional identification mechanisms, as anything could be credentialised. Credentials therefore work to make people 'machine readable' (Van der Ploeg, 1999; Fourcade and Healy, 2017; Amoore, 2013). Importantly, the role that people play in this process is one of the key tenets of the technology, as they are promised 'control' over their credentials, meaning that they can decide which information they want to share and with whom. As such, the subjects of identification play an active role in this process.
3. It collapses different social roles and social institutions into one technical system. Once issued, all credentials are stored in one wallet. The fact that one's passport credential will be stored alongside supermarket loyalty cards, social security number and banking information, matters. It signifies collapse of different social roles and institutions into

> one technical system, as it brings together (identifying information) from institutions ranging from the internet, to companies, to universities, to the state. As such, it also brings previously separate identification mechanisms together; identification practices on the internet are combined with those of the state, and public and private services can be accessed through the same system. It will therefore impact the way in which people access and engage with services: it means that, for example, doing taxes, opening a bank account, logging onto Instagram, and purchasing a pair of trousers all happens through the same app. These were previously separate areas of our lives, that were managed through different channels. Managing these different uses through one wallet suggests a collapse of different social roles.

As I will show throughout this dissertation, the concept of credentialisation plays an important role in SSI's sociotechnical imaginary, as it is connected to one of its core promises: putting individuals in control of their personal data and digital identity- a goal which the EUDI Wallet has adopted. As I will argue, the digital citizen that is enacted through this wallet, is supposed to manage all of their credentials. This requires a tech-savvy, digitally literate citizen, who can decide over the terms of their own datafication and credentialisation. As there are differences in terms of data literacy as well as (financial) resources, this could potentially (re)produce social hierarchies. Furthermore, using the standardisation of credentials as a case, I will also illustrate the changing power dynamics between state and corporate actors.

1.2. Theoretical positioning: technologies, citizens, power

To analyse the socio-technical object of the wallet, I focus on three main pillars: technologies, citizens and power. Overall, the dissertation is grounded in the view that technology is socially shaped, and that technologies carry specific norms, values and ideas – sociotechnical imaginaries – pertaining to 'good society' and the future. Therefore, this research echoes Winner's (1980) notion that technological artifacts are not neutral (and inherently political). From this starting point, I look at the citizens that are enacted through the EUDI Wallet, as well as the production of new power relations through the development of digital ID wallets.

1.2.1. Technologies: social shaping theory

Digital ID wallets have not been widely researched yet. In fact, SSI technology is 'going from theory into reality'[2] through the EUDI Wallet. This dissertation aims to offer an in-depth exploration of the technology, paying attention to the imaginaries and actors that shape it. I see digital ID wallets as sociotechnical systems which are shaped according to specific visions, ideas, norms and values, which reveal a view of how society should be. These views are, both intentionally and unintentionally, built into technologies (MacKenzie and Wajcman, 1985;

[2] Identity & Technology Forum, Germany, May 2023.

Williams and Edge, 1996; Winner, 1980; Bijker and Law, 1992). As such, they are *socially shaped*. As Winner (1999: 32) suggests, '[t]he things we call "technologies" are ways of building order in our world', and whether this foreseen or not, they (re)structure and order society. Therefore, he argues, 'technological innovations are similar to legislative acts or political foundings that establish a framework for public order that will endure over many generations' (Winner, 1980: 128). Therefore, technological artifacts are far from neutral (Winner, 1980).

Importantly, these ideas do not just arise; they usually come from several social groups that work on these technologies, as well as larger societal structures. In turn, technologies also shape social relations: technology and society are mutually constitutive (MacKenzie and Wajcman, 1999). While the design of technologies can restructure the social order, technological development is not inevitable: it does not unfold according to a predetermined logic, but rather is the product of choices that are made, which, in turn, have real and sometimes unexpected outcomes for society and groups within it (Williams and Edge, 1996). Therefore, in my research, I pay attention to the different actors that are involved in this process. For example, when I attended industry events, I was able to immerse myself in the world of people working on this technology. As such, I could see how sociotechnical imaginaries (which I will elaborate below) are constructed, negotiated and brought to live in practice. Similarly, through my interviews with experts, in particular with members of the so-called 'expert group' working on the technical specifications of the EUDI Wallet, I was able to learn about these imaginaries, and how this technology is supposed to change society for the better. Furthermore, speaking to experts allows to connect the technicalities to larger issues: as MacKenzie (2005: 558) points out, it is important to look at '[how] the "small" structure[s] the "big" […] And how the 'big' [is] inscribed in the "small".' In other words, how the technology is connected to (the restructuring of) society and the issues within it.

Critically evaluating the choices, visions and imaginaries that underlie technologies is important, because it offers insight into the social changes that are envisioned and meant to be established through the implementation of the technology. To do this, I use the concept of *sociotechnical imaginaries* (Jasanoff and Kim, 2015). Borup et al. (2006: 286) point out that 'expectations and visions refer to images of the future, where technical and social aspects are tightly intertwined'. Importantly, these visions and expectations are performative (Borup et al., 2006; Michael, 2000) and are often 'moralised', as they are 'encoded and decoded as either utopias or dystopias' (Berkhout, 2006: 300). In other words, visions carry normative ideas about the future that are being performed at the same time, for example through a technology that is meant to bring this future about. In line with social shaping theory, Jasanoff and Kim (2015: 2) remark that technology's material dimension is still too often treated separately from its social dimension. In order to account for the inextricable relationship between the two, they coined the term 'sociotechnical imaginaries'. They define this concept as

> 'collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order

> attainable through, and supportive of, advances in science and technology' (Jasanoff and Kim, 2015: 4).

This concept therefore captures the normative views that prescribe a desirable future, to be created through a technology. Importantly, imaginaries are not only narrowly concerned with technological practices; they are tied to a larger view 'encoding collective visions of the good society' (Jasanoff and Kim, 2009: 123). Furthermore, as McNeil et al. (2017: 457) point out, terms like ideology and interests 'operate mainly in the cognitive register', whereas imaginaries allow for the inclusion of hopes, dreams, fears and expectations. As such, it is a wider term, which also encompasses the emotional component of imaginaries for the future.

1.2.2. Citizens

The social shaping of the wallet impacts the way in which people use it. Furthermore, because the EUDI Wallet is a state-sanctioned identification system, this also speaks directly to the relation between the state and citizens. As Lyon (2007: 111) remarks, identification and citizenship are inextricably connected, because

> '[m]odern bureaucratic administration demands that each person be identified to ensure that they are entitled to call themselves citizens. Without identification one can neither take on responsibilities, such as voting, nor enjoy the benefits, such as protection from external or internal threats to well-being.'

In other words, identification makes it possible for citizens to access their rights and privileges that come with citizenship. Since the wallet gives access to those rights and privileges through digital means, it is involved in the shaping of digital citizenship.

Digital citizenship has been discussed in different contexts and lacks a consistent definition across the literature. However, it is concerned with the participation of citizens in the digital society (Mossberger et al., 2007), the claiming of rights (Isin and Ruppert, 2015; 2017) and the position of citizens in intersecting regimes of (digital) power and datafication (Hintz et al., 2018; Barassi, 2019). Building on this literature, I view digital citizenship as related to participation and rights in the digital society, which is mediated through technology- which has in turn been shaped by social processes involving different actors and are underpinned by sociotechnical imaginaries (see Antenucci and Tomasello, 2023). As such, I build on STS literature that argues that technologies construct the envisaged 'users' (Oudshoorn and Pinch, 2003; Oudshoorn et al., 2004; Woolgar, 1994; Akrich, 1992) to argue that the wallet enacts a 'user-citizen.'

In its most classic formulation, citizenship is the formal relationship between a (nation) state and an individual. Identification practices, as I mentioned, formalise this relationship and give citizens access to rights and responsibilities. Citizenship studies were originally primarily concerned with these rights: in Marshall's (1950) seminal formulation, for example, citizenship is mainly related to rights: civil, political, and social rights should make sure that everyone is

treated as an equal member of society (Marshall, 1950). Joppke (2007: 38) has expanded this definition and argues that citizenship has three different dimensions: status (formal membership to a state, and the rules defining access to it); rights (the formal 'capacities and immunities connected with such status'); and identity (citizens consider themselves to be a member of a collectivity and act accordingly). As I will show, the digital citizenship that is produced through the wallet is less concerned with collective identity, and, to an extent, status. However, it is important to ground this analysis in foundational definitions of citizenship to show what is shifting.

In addition, as the wallet is an EU-wide project, it is essential to acknowledge the contested nature of European citizenship (Shaw, 2018; Bauböck, 2007; 2014; Delanty, 2007). The fact that the legislation and the technical specifications for EUDI Wallet are developed at the European level is remarkable, because matters of identification are usually handled by the member states, for they are inherently tied to matters of citizenship. However, member states will be required to produce foundational digital identity credentials (the equivalent of identity documents). This approach is in line with what European citizenship is; namely derived from national citizenship (Bauböck; 2014). Following Bauböck (2010; 2014), I do not view European citizenship as a replacement of national citizenship, but rather as part of 'citizenship constellations', where citizenships, for example at the local, national and supranational level can exist simultaneously, and rights can be determined by multiple entities. This also makes it possible to conceptualise (legal) residents- who are included in the EUDI Wallet as well – as citizens, for they are granted the same rights and services as citizens, and are members of the same political community (Bauböck, 2010; Kymlicka and Norman, 1994).

What is more, some have argued that the rise of digital citizenship regimes challenges the boundedness of citizenship to a nation-state altogether (Calzada, 2023). Also the identity and rights dimensions are challenged by process of digitalisation. As Antenucci and Tomasello (2023: 247) put it, 'the rise of a new generation of rights [belongs] to the digital sphere', while 'the wide use of technology to enact citizen participation and other concomitant phenomena point to the need to rethink the idea of citizenship according to these emerging dimensions.' One of the prominent ways in which this idea is being rethought, is by conceptualising digital citizenship as acts performed by citizens themselves, and the internet as a means for individuals to be able to claim their rights (Isin and Ruppert, 2015; 2017; 2020). This is part of a literature that no longer defines citizenship as something that is only defined top-down by a state; but is 'done' by citizens themselves through claims-making (Bloemraad, 2018; Clarke et al., 2014). However, this optimistic view is currently being revised as well: in recent years, the empowering potential of digital technology has become more complex, due to the rise of datafication and the surveillance practices that come with it (Hintz, et al. 2018; Hintz, 2020). The increasing datafication of public administration leads to increased classification, control, and prediction of citizen behaviour (Broomfield and Reutter, 2022), as well as the construction and prediction of citizen subjects through data (Cheney-Lippold, 2017; Fourcade and Healy, 2013; Fourcade, 2021). This, as several scholars have pointed out, has the potential to reconfigure state-citizen relationships in profound ways (Barrasi, 2019; Hintz et al., 2019; Fourcade and Gordon, 2020).

For example, Fourcade (2021; see also Fourcade and Healy, 2013) has pointed to the influence of 'digitality' on citizenship, arguing that the way in which digital technologies measure and rank nearly everything people do, impacts their life chances.

As such, a new kind of digital citizen emerges, where citizens are no longer only constituted through their actions, but also through the data traces they leave behind, which are analysed by different entities (Hintz et al., 2018; Broomfield and Reutter, 2022; Barassi, 2019). Hintz et al. (2018: 36) suggest that '[d]igital citizenship is not only self-constructed and self-defined, but equally constructed by the government and business realms. Similarly, Fourcade and Gordon (2020) have argued that the 'dataist state' is increasingly shaped and influenced by digital firms. It is, therefore, not just the state that shapes its citizens; digital technologies, as well as new power relations that come with the increasing importance of 'the digital', are reconfiguring what citizenship looks like.

This dissertation is also concerned with processes of datafication, but starts looking at this from a different starting point. This is because SSI technology is supposed to solve some of the issues associated with earlier identification systems, particularly in terms of control over data. Therefore, the emergence of this technology comes with a new set of questions about the position of citizens and non-citizens in these systems, as they are supposed to gain more control over their data through the wallet. This is closely related to sociotechnical imaginaries around 'control' that underpin the wallet, and that work through the process of credentialisation. Therefore, this dissertation also interrogates this proposed alternative model that the wallet represents.

1.2.3. Power

The wallet is inevitably impacted by power dynamics. This involves 'classic' power dynamics like the relationship between state and citizen, but also new ones, particularly as the different types of credentials, identification mechanisms and actors are brought together through the process of credentialisation. To address these shifting power dynamics, I combine a *transversal perspective*, which I will detail below, with Avelino's (2021; 2020; 2021; Avelino and Rotmans, 2009) framework for studying power, which is concerned with the question of how processes of social change and innovation are (re)producing existing or new power relations. I use these approaches to analyse how the wallet generates new power relations.

As I mentioned above, the wallet is new, but also 'old': since it is being implemented as an identification system for EU states, it is part of the long history of state-sanctioned identification. Power, in this sense, has traditionally been on the side of the state, as it is the state that is identifying and keeping tabs on its citizens making them 'legible' (Scott, 1998; Torpey, 2000; Lyon and Bennett, 2008). As such, it is closely linked with surveillance practices (Lyon, 2010; Amoore, 2006; Ajana, 2012), as knowing who citizens are and what they do, makes it possible for the state to govern, and, as Foucault (1977) famously argued, 'discipline' them.

Much of the political sociology literature on power focuses on power of and decision-making processes within the state (see e.g. Dahl, 1957; Bachrach and Baratz, 1962; Lukes,

2004). However, as I will show throughout this dissertation, these ways of conceptualising power cannot always account for the power dynamics around the wallet. This is because the wallet extends processes of identification beyond the state alone: as it includes various credentials, identification mechanisms and allows access to public and private services, there are more actors involved. Furthermore, because of its digital nature, other logics and interests are coming into play as well. As Bigo et al. (2019: 4) point out, politics around data-related matters ('data politics') are 'not only political struggles over data production and its deployments', but it is also important to look at 'how data is generative of new forms of power relations and politics at different and interconnected scales.' Therefore, they argue, while it is important to look at the struggles and inequalities that arise through data and datafication, it is essential to investigate the power structures that give rise to these issues in the first place (Bigo et al., 2019).

To conceptualise the different kinds of power that different actors have, I use the concept of *transversal politics*, which was coined by international political sociologists. A transversal perspective makes it possible to look at the power of actors operating at different scales: these are not simply (only) related to each other in hierarchical structures, but can also cut across them (Bigo, 2017; Basaran et al., 2017). What is more, power structures are not necessarily only tied to nation-states, but different kinds of actors such as local authorities, international organisations, experts, and corporations, are included as well (see e.g. Nogueira, 2017; Basaran and Guild, 2017). As Barasan et al. (2017: 4) explain, 'it seeks to provoke discussions about relations of power and practices of authorization in ways that do not simply condone or justify established categories and classifications.' As such, it is not limited to 'the national', but rather allows space for power on different, interconnected scales. This perspective on power and actors makes it possible to look at identification, which used to be only in the purview of the state, but now includes an increasing number of actors. For example, the fact that the EUDI Wallet is developed at the EU level, is a move away from the power that states have over identification, and, as I will show, corporations, such as Apple, are entering the domain of identification as well. This, I argue, results in simultaneous competition and cooperation.

De Goede (2016: 362) explicitly links a transversal perspective to technology, and argues that looking at (technological) objects is a good way of 'cutting through traditional hierarchies of the big and the small in international politics.' Drawing on MacKenzie (2005)- whose work I also use- she argues that looking at the small technicalities can speak to global politics, and vice versa (De Goede, 2016). As such, it becomes possible look at different actors and objects on different scales (e.g. local, national, global).

The transversal perspective is often used in conjunction with the concept of *assemblage*, which refers to a number of (shifting) actors and relations between those actors that are working together for some time – this assemblage is fluid and unpredictable, yet all of its parts function together (Müller and Schurr, 2016). Deleuze and Parnet (1987: 69) defined an assemblage as '[...] a multiplicity which is made up of many heterogeneous terms and which establishes liaisons, relations between them across ages, sexes and reigns – different natures.

Thus, the assemblage's only unity is that of co-functioning: it is a symbiosis, a "sympathy."' Building on Sassen (2006), Allen (2011: 155) uses the concept of assemblages to conceptualise how different actors with different positions can come together:

> 'one can think about any powerful arrangement that hangs together as an assorted heterogeneous mix of power and authority: from, say, the changing organisation of finance and corporate business in a more demanding economic world to the shifting tactics of civil society movements in response to global harm and injustice. The mix assembled may be different, but the arrangements themselves hold together nonetheless as some form of consistent, if not coherent, entity.'

As such, 'political actors' can be more than only entities related to (different levels of) the state; they can be public, private, local and international (Allen and Crochane, 2010). I use this concept to refer to the different actors involved in digital ID wallets: they can be public or private, can be located at different levels and have various kinds of power. They can be part of an assemblage for differing periods of time and have different functions.

To further conceptualise the power that different actors hold in an assemblage, I connect the transversal perspective to Avelino's (2021) theory of power. Developed in the context of energy transitions, Avelino (2017; 2020; 2021; Avelino and Rotmans, 2009) argues that most theories of power are concerned with stability rather than change (Avelino, 2021). Her overarching question - which I adopt in my research as well - is: 'how are processes of change and innovation transforming and/or (re)producing existing and/or new power relations?' (Avelino, 2021: 441-442). Power is usually interpreted as a social relation: in particular, it is often defined as 'a relation in which one actor is able to cause the behaviour of another actor' (Pansardi, 2012: 74). However, Avelino (2021) argues that actors do not always have power over one other, or have more/less power than them. Rather, she argues, they can have *different power*, where power is manifested in various forms, as different types of resources can be mobilised (Avelino, 2021).

She proposes a typology of three types of power: *reinforcive*, *innovative* and *transformative* power (Avelino, 2017; 2021). Reinforcive power refers to 'the capacity of actors to reinforce existing structures and institutions' (Avelino, 2017: 508). Innovative power is the power to create new resources, which should be seen as an act of power because it could result in people being less dependent on existing resources and the actors that control those resources (Avelino, 2017). Finally, transformative power refers to the 'capacity of actors to develop new structures and institutions, be it a new legal structure, physical infrastructure, economic paradigm or religious ideology' (Avelino, 2017: 509).

Therefore, in processes of change, the actors involved can have different kinds of power. This means that, for example, A can exercise transformative power, while B exercises innovative power. Importantly, this means that A does not necessarily have the power to control B or vice versa; rather, they exercise power in different ways. This can lead to synergy as well as antagonism, cooperation, co-existence, dependence or independence (Avelino and Rotmans, 2009; Avelino, 2021). Applying this framework makes it possible to show that different actors

in the assemblage can exercise different kinds of power, which allows them to work together or to be in competition.

1.3. A short social history of identification

Now that the theoretical lens through which I look at digital ID wallets have been described, it is important to place these new identification systems in historical context. Even though the wallet brings about change, for example in regard to digital citizens and power structures, it should be seen as part of a longer history of identification as well. In this section, I situate the wallet in the different histories that it is a part of. Here, it becomes both a model for understanding identity as well as a set of technological innovations with their own histories, values and ideas attached to them. It starts with a short history of identification by the state, a process that has since the turn of the century become increasingly digitised and datafied, and which has given rise to concerns about the handling of personal data. When this broader context has been set, I zoom in on a short history of the internet. This is necessary, because SSI technology was originally conceptualised as 'identity layer for the internet', and therefore also situated in a different history of identification, which is related to the power structures of the internet, rather than those of the state. The third short history looks at SSI more specifically, while locating it in the context of its ideological roots, which can be traced back to crypto-anarchism and libertarianism.

1.3.1. Identity documentation histories

Identification, the practice of 'establishing information about an individual' (Nyst et al., 2016: 28), which involves the capturing of a pre-defined set of information about a person, such as name, sex, nationality, but also biometric data such as fingerprints (Lyon, 2009), is a concept that has been long studied in the social sciences (e.g. Goffman, 1963; Foucault, 1977). Identification is a social relationship infused with power, through which, for example, states produce citizens (Torpey, 2000) and colonial powers produce subjects (Sengoopta, 2003; Breckenbridge, 2014). Identification practices have always been accompanied by socio-technical systems that facilitate this relationship that is characterised by the (one-sided) capturing of information. Registers, passports, ID cards but also databases and biometric border gates are all means through which identities are 'inscribed'; often by states, but also by other institutions such as the church, the police or the prison (Caplan and Torpey, 2001). As such, the practice of identification is concerned with establishing uniqueness; it is a means to establish a unique 'identity' for someone so that they can be differentiated from other persons, while at the same time making them part of a collective, such as a citizenry (Caplan and Torpey, 2001; Brensinger and Eyal, 2021). Therefore, identification documents are classification systems (Lyon, 2008); they are standardised so that they can be compared with others (Brensinger and Eyal, 2021). As Dardy (1998, cited in Caplan and Torpey, 2001: 2) points out:

> '[Identification] papers are at one and the same time papers of constraint and control, including control by the state, but they are also purveyors of identity. For each and every one of us, our identity—at least a certain kind of identity—is enacted and re-enacted, stamped, and affirmed in these papers.'

In other words, there is an inherent link between the establishment of control, and the continuous creation of identities. Therefore, Caplan and Torpey (2001: 8) argue that people never fully control this identity, as 'the identity document carries a threat of expropriation at the same time as it claims to represent who we "are."' However, while 'identification' is often conflated with 'identity' - as an identification document is supposed to 'prove' who we 'really' are – it is important to be critical of this notion. Seen in a social context, identity is a relational concept (Brubaker and Cooper, 2000), as our social identity can differ according to context, which means that there is no singular 'identity' (Hall, 1990 cited in Amoore, 2003). Interestingly, however, new technologies, such as self-sovereign identity technology, do emphasise identity over identification. This, in the case of SSI, has to do with the idea that people can control what information about themselves they want to release. I will interrogate this claim throughout the dissertation.

While identification as we know it today is usually viewed as a 'modern' phenomenon (Caplan and Torpey, 2001; Lyon, 2009), there have been attempts to find the earliest iteration of identification documents. For example, in what he calls a 'pre-history' of the passport, Bixby (2022: 27) goes as far as to refer to the Old Testament (Nehemiah 2:7-9), where Nehemiah asks King Artaxerxes of Persia for a 'letter of safe conduct' to accompany him on his travels to Jerusalem. Or, another option is to trace back the history of identification to ancient Egypt, where, arguably, the oldest travel 'document' was found in the shape of a clay tablet, imprinted with a letter in which King Tushratta of Mittanni demands the safe passage of his messenger to let him travel to and deliver a message to his brother, the King of Egypt (Bixby, 2022: 29). In terms of 'modern', state-issued identification documents, it was not until the 18th century that identification documents, particularly passports, became a more common and more institutionalised phenomenon (Torpey, 2000). For example, Torpey (2000) shows that the development of the passport regime is closely connected to the establishment of the nation-state, because it made it possible for states to gain the monopoly over the legitimate means of movement. Importantly, this also established the distinction between citizens and non-citizens, which has had far-reaching implications because it determines who is granted the rights and freedoms which come with citizenship (Torpey, 2000). As there are global differences in this regard, citizenship hierarchies emerged (Castles, 2005).

However, the passport is only one – albeit important – modality of identification. Examples of other identification practices include the registration of births, deaths and marriages. For example, describing the 'birth' of civil status in (18th century) France, Noiriel (2001) shows how it became important to the French state to register this information, which meant that the person declaring these facts, became a full member of the civil community. This demonstrates how identification is at the same time establishing 'uniqueness' and embedding

an individual into a collective. Furthermore, around the same time, European states also imposed identification systems upon the populations they colonised. For example, one of the earliest identification systems was established by Dutch colonisers in South Africa; in order to control the slave labour on settler farms, carrying an identity pass became mandatory (Longman, 2001). Importantly, histories of identification in formerly colonised states show how identification is entangled not only with capitalist extraction, but also with race-making and the construction of ethnic hierarchies (Weitzberg, 2020). Therefore, the creation of 'identities' is not neutral, as it facilitates inclusion and exclusion through the creation of social hierarchies. While these are only a few examples, that do not do justice to the long history of identification in its different forms, they do show that identification is inextricably bound up with power: it makes it possible to create categories, citizens and subjects; it makes people 'legible' (Scott, 2020) and defines them in relation to the state.

Digital identification is relatively recent, and while it builds on older identification systems, it is also new in some ways, particularly in terms of the sheer amount of data that can be stored, and the ways in which a person's 'identity' can be checked and verified across systems. Towards the end of the 20th century, states across the world started to develop national ID card systems, which should be seen as part of the effort to digitise government (Bennet and Lyon, 2008). ID cards differ from passports in the sense that they are not primarily designed to cross borders; rather, they are for use within states and facilitate transactions between organisations- such as the government, banks or employers - and individuals (Lyon, 2008). The rise of ID cards was catalysed by the 9/11 attacks in the United States, which caused an increased concern with security (Noxolo and Huymans, 2009; Salter, 2004). This increased focus on security made it increasingly important to 'prove' that the person carrying the passport or ID card really is who they claim to be. Ensuring this involved including more biometric information (Flynn, 2009; Palm, 2016). In theory, including a chip with biometric data in the passport was supposed to 'secure' identities, because this would establish a unique connection between the passport and its carrier, linking the document to someone's very body (Salter, 2004). However, the idea that 'the body does not lie' (Aas, 2006: 143) is, as researchers have shown, misguided, as it brings out gendered and racialised biases (Magnet, 2011), and it is more accurate to say that differences are enacted through the capturing of biometric data (Kloppenburg and Van der Ploeg, 2020).

The inclusion of biometric information led to much academic and public debate about the potential surveillance power states would gain, as this would make it possible to keep track of both citizens and non-citizens and separate them into (legitimate and illegitimate) categories (Amoore, 2006; Aas, 2011), sometimes even trying to identify them before they reach the physical border (Amoore, 2003). While these distinctions map onto older ones, technology began to automate this process, and also added new categories, for example different types of border crossers, such as 'trusted travellers', 'unwanted travellers', and those who are subject to further scrutiny (Broeders and Hampshire, 2013). Therefore, these identification processes are inherently tied up with different forms of inclusion and exclusion.

This digital acceleration of identification documents put increased emphasis on 'proving' one's identity. Müller (2004: 285) suggests this is 'the beginning of identity assurance'. Citizenship, he argues, is moving towards 'identity management', where the practices of identification shift to identity authentication and authorisation, thereby securitising identity itself (Müller, 2004: 286-7). Similarly, Van Zoonen (2013: 46) points out that 'identity management' is concerned with establishing 'single and stable identities.' These shifts show that certain elements remain the same; the need to register people, and 'prove' that they are who they say they are. At the same time, the focus on 'identity' has become more pronounced, and is increasingly seen as a singular status that can be 'proven', rather than a complex social and relational concept. This also links in with identification through the internet, which has also become more focused on single identities, which I will discuss below.

The relatively new concept of 'identity management' is reliant on the concept of 'digital identity', which is more comprehensive than a passport or ID card, because it can involve different aspects of a person's identity and be linked to access to several services. As understood by Nyst et al (2016: 28) digital identity is 'any system (or scheme) where identification, authentication and authorisation are all performed digitally'. This usually means that individuals are registered in identity databases, which enables them to assert their identity, and because of that can be authorised to access services or products (Masiero, 2023). Digital identity schemes have been established in different contexts, such as nation-wide digital identity (also called e-ID) schemes, the most established of which are Estonia's (e-Estonia) digital citizenship scheme (Beduschi, 2021) and Aadhaar in India, which is the world's largest digital identity programme (Masiero and Arvidsson, 2021). Similarly, non-state actors, such as the UNCHR have set up digital identity programmes for refugees and migrants across the world (Schoemaker et al., 2021; Weitzberg et al., 2021). Finally, there are countless digital identity programmes for different (private) sector purposes, such as banking or online retail (Beduschi, 2021). I will further expand on the digital identity literature in the next chapter.

For now, it is important to note the place of self-sovereign identity technology in this history. SSI is a digital identity model, which is inserting itself into several discussions around power. As I mentioned above, it is linked to ideas about shifting the power of states and companies, toward individuals, which is meant to be established through control over data (Giannopoulou, 2023). This is important, particularly in light of the long history of identification, which is infused with control and power over those that are being identified. However, SSI is not only situated in debates around identification by the state; it started out as a technology developed for the internet. In the next section, I zoom in on the internet histories that form the backdrop of the creation of SSI.

1.3.2. Internet histories

In parallel with states developing digital infrastructures for identification (and gaining more surveillance power), the internet has grown and changed at rapid speed, developing power structures of its own. While it is now being repurposed for several fields, self-sovereign identity

technology started out as a proposal to be the 'identity layer' of the internet. SSI evangelists present it as a way to change data ownership and consent mechanisms, as it has in recent years become clearer how 'data' has become a source of power. As such, it often comes up in the conversation on the future of the internet, for example in relation to Web3 (and even Web5) projects (see e.g. Cheqd, n.d.). While the histories of identification documents/digital identity and the internet intertwine, they are here presented alongside each other, both for the sake of clarity and to show that SSI sits between the online and the offline, and between public and private.

When the ancestor of the internet, the ARPANET, started out in the 1960s, it connected two computers, one located at Stanford University, and one at UCLA (Paloque-Bergès and Schafer, 2018). It only went more mainstream in the 90s, when Web 1.0 allowed users to connect to the internet. While it was not really possible to interact with websites yet, users were now able to read things online (Park et al, 2022). Tim Berners-Lee, the inventor of the World Wide Web, described this phase of the internet as 'read-only' (Stevens, 2022). By the 2000s, Web 2.0 introduced the possibility for users to interact with websites. They could now write a blog or chat to each other through (then new) social media platforms (Park et al, 2022). Because of this, Web 2.0 is also referred to as the 'read/write' version of the internet (Stevens, 2022). While we are currently still using Web 2.0, it has, needless to say, changed and grown exponentially over the last 20 years.

It is important to note the connection to online identification and digital identities here. In the early days of the internet, the anonymity it offered was often praised, as one could experiment with different identities online, and as such, resist the identities that were imposed in the offline world (Turkle, 1995). Therefore, when platforms started to ask for people's real names, this was met with criticism, as this removed the possibility to be 'anyone', and might force people to use identities that they did not personally identify with (Haimson and Hoffman, 2016). This shift was accompanied by debates about authenticity and accountability, especially the claim that people would behave better when their real name is known (boyd, 2012). However, boyd (2012) argues, this also removes their control over the social situation, as people do no longer control how they represent themselves differently according to the social context. As platforms grew, they started to offer the option to use the same 'identity' – such as a Facebook or Google account- across websites (Schmidt, 2018). The fact that some companies, such as Google, gained a monopoly position, makes individuals not only dependent as consumers, but also affects different roles they may have, like 'citizen', 'student' or 'patient' (Van Dijck, Nieborg and Poell, 2019). Therefore, the internet has become an identification mechanism in itself. Some of the logics at play in identification on the internet overlap with the issues I mentioned in the previous section. Particularly the idea that people need to 'prove' their 'real selves' through the use of their real name, or verifying their identity. This has resulted in, for example, a blue checkmark on X (Twitter), which proves a person's 'authenticity' (Hearn, 2017).

Using the same identity for all these services, also allowed the issuers of those identities to aggregate data across services (Schmidt, 2018). For Big Tech companies, this has led to

unprecedented power; to the extent that their power has been compared to that of states (Broeders and Taylor, 2017). For example, Nick Srnicek (2016) shows that firms like Google, Apple and Airbnb have transformed themselves into platforms, which provide the technological foundations (hardware and software) for others to operate. Platforms are able to extract and control massive amounts of data from their users, and have, as a result, been able to gain a monopoly position in the market. Because of this, only a handful of companies are able to exercise an enormous amount of power; economically, politically, and socially (Dencik, 2022). In a similar vein, Zuboff (2019) theorises the emergence of 'surveillance capitalism', where platforms sell data to the highest bidder, who will in turn be able to predict people's behaviour, and anticipate or modify it for profit.

As I briefly discussed above, the increasing amounts of data available also changed the ways in which states could relate to their citizens. The Snowden Revelations was an important event in this regard, as this brought to light that the American National Security had been gathering 'bulk data' on citizens. These were metadata of over three billion interactions and phone calls that had been recorded by companies like Facebook, Apple and Google (Van Dijck, 2014; Wahl-Jorgensen et al., 2017). According to Van Dijck (2014: 197), this event was 'more than a wakeup call for citizens who have gradually come to accept the "sharing" of personal information'. It seems, she suggests, that 'metadata have become a regular currency for citizens to pay for their communication services and security – a trade-off that has nestled into the comfort zone of most people' (Van Dijck, 2014: 197).

SSI technology situates itself in these debates and developments. According to the SSI community, this technology should change the internet. This community has been working on an 'identity layer' for the internet since the early 2000s (Infominer and Young, 2021). Fundamentally, it was concerned with what was seen as the centralising power structures of the internet, where big entities (such as Facebook) provided users with a digital identity that could only be used on their website. Instead, SSI proponents have wanted individuals to have one identity that they manage themselves and can use for everything on the internet (Preukschat and Reed, 2021). This is directly connected to surveillance capitalism as well, because SSI technology is supposed to give users control over their personal data, which would mean that it will be harder for companies to (non-consensually) harvest these data. As such, while it has its own movement, SSI technology has been mentioned in the context of Web3, which is supposed to bring about a technological shift that will 'democratise' the internet, notably through new forms of self-identification and ownership. This can refer to ownership of data, but also to NFTs (non-fungible tokens) or cryptocurrencies (Belk, Humayun and Brouard, 2022). This is, however, a very narrow conceptualisation of democracy, where ownership and control are equated with (more) equality. Importantly, this does not take different social positions and lived realities into account, as it is unlikely that everyone will be able to perform in these new systems.

1.3.3. Cypherpunks and Bitcoin: SSI's family

SSI should be seen as very normative technology, because it carries ideas about the future, and how to make the future world a better place. According to its proponents, is not just a new technology, but a 'technological revolution that will readjust existing powers and equalize them to the benefit of all (self-sovereign) individuals' (Giannopoulou, 2023: 5). Its remarkable name immediately begs the question: what does it mean to be self-sovereign? According to Ishmaev (2021: 239), it is tempting to conceptualise 'self-sovereignty' in a 'narrow technical sense', but this would ignore the normative component in the meaning of 'sovereignty'. He argues that the core promises of SSI- improved privacy, security and full control over their digital identities for individuals - are 'loaded with ethical assumptions' (Ishmaev, 2021: 239). The concept of 'sovereignty' has a much longer history, and is rooted in social contract theory by philosophers like Rousseau and Hobbes, reflecting on governance and the distribution of power in society (Reijers et al, 2016). It is closely related to the establishment of the international state system, in which states have sovereign power over a territory (Skinner, 2010). However, now that the concept is being repurposed for the digital sphere, it is gaining different meanings. Ishmaev (2016: 246) defines self-sovereignty

> 'as the concept of individual control over identity relevant private data, capacity to choose where such data is stored, and the ability to provide it to those who need to validate it, without relying on any centralised repositories of identity data.'

As such, it presents a very individualised conception of sovereignty. This comes at a time, however, where discussions of digital forms of sovereignty, such as data sovereignty, digital sovereignty and technological sovereignty are gaining attention (Couture and Toupin, 2019; Phole and Thiel, 2020; Hummel et al., 2021).

SSI technology is therefore inherently political: it raises questions about the role of individuals within larger social institutions such as internet, but also the state (Lofretto, 2012). In addition to being part of passport and internet stories, SSI technology also has roots in crypto-anarchist and cyberlibertarian movements. This means that parts of the technology are rooted in a deep distrust of any kind of intermediaries, such as banks and states (Golumbia, 2018). This is important, because, as Golumbia (2016: 9-10) argues with reference to Bitcoin ('family' of SSI), the underpinning ideology incorporates right-wing extremist views, such as the idea that there are 'elites' who control the monetary system as well as government and corporate leaders. He and others (see e.g. Faustino, Faria and Marques, 2022; Swartz, 2017) have drawn attention to the 'mythical' narratives around similar technologies, where 'believers' see technologies such as blockchain and Bitcoin as a means to 'free society from centralised power' (Faustino, Faria and Marques, 2022: 71). Therefore, this 'family' of technologies has a significant cultural and symbolic dimension. However, it is important to mention that not everyone who likes and uses these technologies is a 'believer' in the extreme sense. As I will discuss in chapter 4, many SSI proponents are not actually against the state themselves, and

they are content that the concept of SSI is being repurposed to fit the needs of the EU. As such, this is a very 'incorporative' (Swartz, 2018) version of this technology, where the system is not radically subverted, but rather, the technology is being built into the existing structures. It is, nevertheless, important to point out where the technology is coming from, as this history does shape what the affordances of this technology are, which will in turn affect the social world.

Cryptography-based technologies such as blockchain and Bitcoin can be traced back to a digital activist movement that arose in the 1990s in the United States, the Cypherpunks (Jarvis, 2021). Cypherpunk thought is primarily based on libertarian and anarchist ideas; distrust of the state and the desire to limit state interference. The movement's chief ideologue, Timothy C. May, published his crypto-anarchist manifesto in 1988. In this manifesto he proclaims a revolution, which would lead to the reduction of state power over both the social and economic realm, all made possible by cryptography (Beltramini, 2020). As May (1988: n.p.) put it himself: '[j]ust as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions.' The Cypherpunks were very concerned with privacy, and believed that only technology could ensure this, as the government could not be trusted, and cryptography was believed to be the only way diminish its meddling in people's lives (Jarvis, 2021). The idea of crypto-currencies was coined a few years earlier, by David Chaum (1985: 1031), who published a seminal article in which he lays out a system for digital transactions that 'allows individuals to protect their own interests' and would put a stop to the move to a panopticon-inspired 'dossier society' (Jarvis, 2021). The Cypherpunk movement further developed these ideas. Eric Hughes (1993: n.p.), another prominent figure in this movement, stated in his *Cypherpunk's Manifesto*: 'Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it'. In other words, they believed that the democratic system was broken, and technology could better protect their privacy and freedom than the law could (Beltramini, 2020: 15-16).

Around the year 2000, the Cypherpunk movement started to fall apart, as some of the early members had lost their enthusiasm, and the mailing list was declared 'dead' in 2001 (Swartz, 2018). For a few years, it remained silent in the crypto space. This silence was suddenly broken in 2008, when an anonymous and enigmatic figure by the name of Satoshi Nakamoto published a whitepaper in which they announced a new digital cash system: Bitcoin (Swartz, 2018). In essence, Bitcoin is an '[…] electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party' (Nakamoto, 2008: 1). Bitcoin arrived at a time when the global financial crisis made many lose trust in governmental institutions and the financial system, which opened up a space to think about alternative currencies and payment systems, and quickly gained a large following (Swartz, 2018: 629; Golumbia, 2018). Blockchain was originally part of Bitcoin, but it was soon discovered that it could be repurposed. In essence, blockchain is a distributed ledger, that is shared between and accessible by many different entities (Cornejo and Johnson, 2019). This is to ensure the non-hierarchical structure; there is

not one entity that has control over all the data stored on the blockchain. Around 2015, bitcoin hype seemed to be replaced by a blockchain hype (Swartz, 2018). As Swartz (2017: 82) points out 'it truly is difficult to overstate the claims by some blockchain enthusiasts', who suggest that 'we may be at the dawn of a new revolution', as blockchain is 'extremely disruptive technology that would have the capacity for reconfiguring all aspects of society and its operations'.
SSI is sometimes spoken about in a similar way; it, for example, presented as a 'paradigm shift', comparable to 'the shift from horse travel to train travel' (Preukschat and Reed, 2021: 3). What is more, it is related to similar thought: SSI practitioners have called Bitcoin and Ethereum (a blockchain ecosystem) the 'granddaddies' of SSI (Preukschat and Reed, 2021). David Chaum, whom I mentioned above, has also been named as the 'grandfather of SSI', as he 'was among the first to discuss how individuals were losing control over the way our personal information is used' (Infominer and Young, 2021: 311). As such, these technologies are part of the same ideology or philosophy, which emphasises the importance of privacy and control, made possible by decentralisation and cryptography. While SSI proponents might not be as radical as the early Cypherpunks, parts of these ideas still shine through.

These three histories show that SSI technology is situated in different contexts. Through the EUDI Wallet, these histories are being brought together in one technical object. Throughout this dissertation, I will address the entanglements of these histories, looking at the implementation of SSI, as an identity model designed for the internet in the context of the state (EU), the digital citizens that are enacted through this wallet, and the shifting power structures that this produces.

1.4. Overview of the dissertation

Chapter 2 situates the dissertation in the literature. Building on the three main theoretical pillars of this dissertation, technologies, citizens and power, the literature review is structured around three main blocks. First, I address the literature on digital identification, focusing on the creation and categorisation of identities, as well as the increasingly overlapping functions of (legal) identity documents. Second, I look at this literature in relation to power, paying attention to the tension between power and empowerment, different actors involved in digital identification systems, and technologies that aim to shift power relations related to governance. Third, I look at the existing literature on SSI technology. In doing so, I show that the current literature has not comprehensively addressed the literature on digital ID wallets, and SSI in particular. As such, this is the first in-depth study of SSI technology, where the concept of the technology is seen in relation to its implementation, and where its core promises are mapped out and assessed critically.

Chapter 3 introduces the methodology. In this chapter, I discuss the flexible research design that was required with this fast-moving technology. To analyse technology that is still under development, I conducted 20 semi-structured interviews with experts, attended five key events and did documentary research, which included over 300 documents. This approach allowed

me to 'scavenge' (Seaver, 2017) the data needed to analyse SSI and the EUDI Wallet. Applying a flexible, iterative approach allowed me to collect new data when it became available, and made it possible to study this technology while it is in the implementing phase. I also describe how I used LinkedIn as a research device: it helped me find and contact potential interviewees and allowed me to follow the discussions and developments in the SSI community.

In chapter 4, the first data chapter, I look at how SSI technology, originally developed for the internet, is implemented in the context of the EU. I argue that SSI's sociotechnical imaginary (Jasanoff and Kim, 2015) revolves around 'control', as the main aim of this technology is to put individuals in charge of their personal data and digital identity. Looking at the concepts of 'identity', 'decentralisation' and 'trust', I show this imaginary is inextricably linked to SSI's technical architecture. I further develop the concept of credentialisation, arguing that the social meaning of 'credentials' is changing, as they can be used across different contexts, and help construct 'verifiability' in a new way. I also introduce the case of the European Digital Identity Wallet, and argue that in adopting SSI, the EUDI Wallet is applying an imaginary that was invented for users of the internet, to citizens of EU member states. However, drawing on expert interviews, I show that the translation of this imaginary into the sphere of the state also causes friction. Specifically, some technical elements are difficult to implement, prompting some SSI experts to note that the EUDI Wallet is not 'pure' SSI. I argue that this friction around the implementation of SSI technology goes to the heart of the tension around 'control': EU states need to balance shifting a degree of power over to citizens, while simultaneously retaining control over identification processes, as identifying citizens is a classic function of the state (Lyon, 2007). However, paradoxically, as some elements of SSI technology- notably credentials - are adopted, a new assemblage of state, corporate and internet actors inevitably need to be involved in identification processes. I argue, therefore, that the credentialisation of identification brings about a new role for (EU member) states, where they are in a paradoxical position between giving away and trying to retain control, as the EUDI Wallet broadens the scope of identification.

In chapter 5, I further investigate the changing role and responsibilities of citizens within this new system. I argue that the EUDI Wallet enacts a 'user-citizen', as 'user behaviour' such as the consenting to the sharing of personal data, is being applied to citizen 'transactions' as this becomes part and parcel of gaining access to services. The user-citizen is tech-savvy and has the time and resources to make informed decisions over the sharing of their personal data. I show that both SSI and the EUDI Wallet are usually framed in terms of 'empowerment', which refers to the control over personal data that is handed over to individuals. While transferring more control to individuals could be a positive development in some ways, it is crucial to critically assess this shift, as it makes citizens responsible for deciding on the terms of their own datafication them (to an extent, as there are limitations to what is allowed), which may not always be easy to do. This, I argue, is particularly important because of the process of credentialisation: the wallet turns different parts of people's lives into credentials, and gives

access to a wide range of services. What is more, this means that there are many different types 'high quality' (as it can be verified) of data at stake. This is important, because verifiable data is considered to be valuable. Keeping this in mind, I address the covert market logics embedded in the wallet: the option to share additional personal data in exchange for discounts or vouchers. While this could be seen as a person's own right to choose, it could also lead to predatory systems where less digitally literate or financially precarious groups are more exposed to the risk of exploitation, or are unable to access essential services. This, I argue, could create new hierarchies, both between and within EU states.

In chapter 6, I argue that the power dynamics around identification are changing, as there is simultaneous competition and cooperation between state and corporate actors over what digital ID wallets should do, and how they should be designed. I show that the transition to an elaborate and fully digital identification system- and the need to do this quickly, in order to be able to compete with Big Tech companies- has led to extensive influence of technical experts over the development of the EUDI Wallet, for the legislation and the development of the technical specifications of the wallet happened in parallel. What is more, the so-called 'wallet wars' show that identification is not only within the purview of states anymore: there is a de facto competition between the EU and Big Tech companies. I show that there is an expansion into different types of identification documents and mechanisms from both sides: political bodies like the EU are trying to enter the online identification space, while Big Tech companies are trying to include traditional citizenship documents. As such, I argue, the complicated power dynamics are in part due to credentialisation, as digital ID wallets such as the EUDI Wallet are integrating different, previously separate functions. However, I argue, these actors have 'different power' (Avelino, 2021): power does not reside exclusively with states or Big Tech companies; rather there is simultaneous competition and collaboration, which makes the power over identification, previously only yielded by states, more complicated and diffused. Using the development of technical standards for credentials as an example, I show how something small like a technical standard is tied to global power battles, different political stories and competing views of the future.

Chapter 2. Literature review

Digital ID wallets are both new and old: they are new because they generate new information (credentials), new subjects (user-citizens) and new assemblages. At the same time, they are also 'old', because digital identification systems have longer grappled with issues like making identities unique, individuals legible, and establish control over populations. In this chapter, I situate SSI technology (the technological arrangement underpinning digital ID wallets) in the literature, showing both continuities and the gaps in the literature. SSI is a very new technology, which is accompanied by new promises, such as 'control' for individuals. As such, the technology comes with a different set with questions, that have not been addressed extensively in the literature yet. At the same time, because it is part of this longer history, it grapples with some of the same issues as well. As I will show, current social science literature on SSI has not addressed the technology in an empirically grounded way, where the concept of the technology is seen in relation to its implementation, and where its core promises are mapped out and assessed critically. Therefore, this dissertation is one of the first in-depth explorations of this topic, which links empirical detail to theory as well as normative concerns.

As I described in the previous chapter, the three theoretical pillars of this research are technologies, citizens, and power. Because of this, I address the literature in three related thematic blocks, whilst also paying attention to the chronological development of the literature and the different logics underpinning digital identification systems. In the first block, I address 'identification' in relation to the making and categorising of identities and citizens. The second part assesses the different ways in which power has been addressed: the tension between power and empowerment, different actors (beyond the state) involved in identification processes, and how power structures are supposed to be shifted through technology. The third section addresses SSI technology directly, and summarises the limited social science literature that has up until now been published on this topic.

2.1. Identification: creating and categorising identities

The literature on digital identification has looked at different processes through which identities are created and categorised. As I described in the previous chapter, I argue that the process of credentialisation signifies an important societal shift. It reveals, as such, an important way in which identification systems are changing. One of the things that credentialisation is very concerned with, is verifying that people really are who they claim to be. While establishing 'uniqueness' (Caplan and Torpey, 2001; Eyal and Brensinger, 2021) is not new, and in fact one of the key tenets of identification, I argue that credentialisation is a new way of establishing this uniqueness. This is not only because it is underpinned by a new data format, and a new set of technologies that make it possible to 'verify' claims, but also because it goes beyond many existing identification mechanisms, collapsing different social

institutions and roles into one wallet. As I will show, the existing literature does interrogate ways in which unique identities are established and 'sorted', but as most of this literature is concerned with legal identity documents only, it cannot account for the comprehensive identification that the wallet will be. What is more, an 'identity model' that was designed for the internet and is now being applied to the domain of the state, SSI technology is often framed as a response to data-related challenges and control. As such, it is underpinned by a different logic than previous identification systems that have been analysed in the literature, which, as I will show, were concerned with respectively increased concerns around safety and security, and the view that digital identity could be a tool for development.

The early literature on identification was primarily focused on the inclusion of digitally readable biometric data in identification documents, which has been conceptualised as 'biopolitical tattooing' (Agamben, 2002) or making bodies 'machine readable' (Van der Ploeg, 1999). While identification was not new, this literature chronicles the start of an intensified focus on surveillance, authenticity, and the desire to establish people's identities are 'real', and that they really are who they claim to be. Seen in light of the 9/11 attacks in 2001 in the United States, which spurred an unprecedented emphasis on security and identification (Noxolo and Huysmans, 2009; Flynn, 2009), this literature views identification in light of growing 'securitisation', where there is perceived to be '[...] an existential threat to a valued referent object', which 'enable[s] a call for urgent and exceptional measures to deal with the threat' (Buzan and Waever, 2003: 49). It analyses how the biometric passports and ID cards made it possible to separate people into different groups, ranked according to risk. It also assesses how both citizens and visitors are placed under increased scrutiny, and identification documents are 'securitised' – often by adding biometrics to them (Amoore, 2006; Lyon, 2010). Scholars looked at how people were sorted into 'risky' and 'unrisky' categories at the border, creating legitimate and illegitimate forms of travel (Salter, 2004; Müller, 2004; Sparke, 2004; Amoore, 2006; Epstein, 2007; Ajana, 2012). Similarly, within states, the emergence of (biometric) ID cards 'introduce[d] new levels of visibility of citizens such that the state may "see" them so much better' (Lyon, 2010: 607). Elsewhere, Lyon (2007; 2008; 2009; 2010; Bennet and Lyon, 2008) further explores this development, arguing that ID cards and other digitally mediated surveillance tools facilitate what he calls 'social sorting', the separating of groups of people into different categories, where some are perceived to be riskier than others. This literature usually employs a Foucauldian lens, emphasising biopolitics and the panoptic qualities of this phenomenon (e.g. Epstein, 2007; Müller, 2010; Leese, 2016). Furthermore, it demonstrates the beginnings of 'identity management' (Müller, 2004) which refer to the process of verification and authentication of people's identity by coupling it to machine readable identifiers such as biometrics. This literature is important, because it shows how identification mechanisms are simultaneously classifying tools, that 'sort' people in different categories, and therefore illustrates how identities are shaped through to identification mechanisms. However, as it is only concerned with legal identity documents, it cannot account for the process of credentialisation, which brings many different aspects of people's lives together.

Subsequent literature did engage more in depth with the question of how to represent people in digital identification systems. As this literature points out, 'fixing' identities is fundamentally concerned with the 'realness' and 'authenticity', to the point that stable and fixed identities are presented as a person's 'real' identity. While most of these critical studies focus on biometrics, it is important to that mention digital ID wallets are also looking to 'fix' identities. However, the question of what kinds of identities are created through digital ID wallets, and by extension what kinds of citizens this produces, has not been addressed yet. This dissertation aims to fill this gap.

Researchers have addressed challenges surrounding the question of how digital 'objects' can represent people, and how to reach a similar level of authenticity to the physical world (Allison et al., 2005; Whitley and Hosein, 2010). Most research critically interrogates biometrics, emphasising the use of the body as a site of identification (Amoore and Hall, 2009; Rygiel, 2011), which is a way to link identities across different databases as well (Ajana, 2012; 2013). Looking at the relationship between citizen and state, Lips (2010; 2013) notes that digital identification 'fixes' and 'reconstructs' identities in order to provide services. She notes, for example, that this will change the position of citizens as location will become less important, and services can be delivered in real-time (Lips, 2010; 2013). From a more critical angle, Martin and Whitley (2013) point out that there is an assumption that biometrics give access to 'truth' about identities, as it is verifiable and seems objective. Therefore, they argue, biometrics are used to 'fix' identities, according to pre-determined categories, which also reifies biometrics as a stable identifier. As such, a tension arises: between identities, that are in social theories often seen as multiple, and relationally constructed (see e.g. Bauman, 2004), and identification, which does not allow for multiplicity and is mainly concerned with creating and verifying single identities. As Lyon (2007b: 177) remarks: 'when there is pressure towards finding single unique identifiers […] the existence of multiple identities […] is a constant challenge to the would-be hegemonic system'. Others address the 'interplay' between identity and identification systems (Whitley et al. 2014), or signal the growing emphasis is placed on the importance of 'authenticity' across different social contexts including internet, national identity and cultural expressions of identity (Van Zoonen, 2013).

A more recent strand of literature focuses on the 'enactment' of identities. This literature is mainly based on STS approaches, where technology is seen as playing a constitutive role in the shaping of social relations. For example, Kloppenburg and Van der Ploeg (2020) argue that biometrics not just represent a body, but rather that bodily differences are actively enacted during identification processes. In a similar vein, other scholars have conceptualised identification practices at borders as sites of identity enactment (Pelizza, 2019; 2021; Glouftsios and Scheel, 2021; Van Den Meerssche, 2022). For example, Pelizza (2019) argues that migrants who are registered when they are entering the EU, are 'translated into "European-legible" identities' (Pelizza, 2019: 3). This literature therefore moves away from the idea that identities necessarily 'represent' a person; rather, they are enacted in accordance with the categories imposed by the registering authorities. In line with the recent literature, this dissertation also takes the approach that identities are 'enacted' rather than

representative of people. In spite of the claim that citizens will be in control of their data and digital identity, credentials are being formatted in a specific way, generating identities according to pre-defined standards, where these identities become 'real' because the information can be verified. What is more, as I will argue, the wallet enacts a particular type of digital citizen, who is supposed to be tech-savvy, data literate, and able to manage their credentials. Looking at the potential implications of this 'control' that citizens are promised is particularly important because the wallet will contain many different credentials.

However, the ramifications of such a comprehensive identification system have hardly been explored yet. While the literature is starting to address the increasing convergence of 'digital' and 'legal' identity, digital ID wallets that integrate various credentials have not yet been researched. The EUDI Wallet is an important case, as the wallet credentialises formerly distinct types of personal data, and provides access to public and private sector services, both in person and on the internet. This dissertation aims to fill this gap by providing in-depth and empirically grounded insight into the shift to wallet-based identification.

Sullivan (2018) has noted that since the conception of the term 'digital identity' in 2008, different types of digital identities (ranging from government issued identities to an account for Visa) became almost indispensable for engaging with both public and private services. Crucially, she points to the fact that there is a growing conflation of digital identity and legal identity, as national digital identity schemes are, for all intents and purposes, becoming a legal means of identification (Sullivan 2018; Sullivan and Burger, 2019). In a different article, Sullivan and Burger (2019: 236) argue that 'the digital identity required for government transactions effectively becomes the individual's digital identity for transactions generally, and that identity becomes the primary means by which an individual is recognized and can enter into transactions in the digital age.' Therefore, this shift has implications for the role of legal identity within increasingly integrated identity systems, as official identity 'documents' may be used for an increasing number of functions.

This shift has been observed by other scholars as well, though usually addressed in literature on development. For example, Sperfeldt (2021: 11) points out that the United Nations' Sustainable Development Goal (SDG) target 16.9 - which introduces the target of a 'legal identity for all by 2030' – is increasingly overtaken by digital identity solutions. As such, he points out that 'the term "digital identity" is used more frequently and has come to gradually supplant the concept of "legal identity"' (Sperfeldt, 2021: 12). Others have stressed the risks of this conflation: the combination of this SDG target and digital identity is primarily found in development contexts where there might not be a pre-existing 'foundational' identification mechanism in place, and because there is to date no real legal definition of 'legal identity', there is a risk that different actors will interpret this according to their own priorities (Manby, 2020; 2021). As such, Beduschi (2019) argues, while technology can be a powerful tool to reach the target, such systems can only potentially be beneficial if they aim to mitigate potential discrimination risks and have high privacy and data protection standards.

In addition to research addressing the conflation of digital and legal identity, there are a few studies that address how identity documents are being used for different purposes, such as

Sparke's (2004) discussion of a plan to integrate a credit card and biometric data in a passport in the United States, and Lyon's (2007: 114; 2009) observation that the then new biometric ID cards reflect a move towards consumerism and globalisation, where many ID cards are created for multi-purpose use; for both public and commercial services, and usable for 'government departments, agencies and the police.' Similarly, Husz (2018) has addressed this from a different angle, showing how the Swedish BankID has become a de facto identity document. However, while these studies point to an emerging trend, they do not encompass the same extent of services that the wallet brings together through the process of credentialisation.

In short, the existing literature on digital identification provides an important foundation for addressing concerns around the creation of identities, the implications on social relations this might have (through categorisation), and the increasingly multi-purpose nature of identity documents. However, as I will show throughout this dissertation, wallet-based identification is different in the sense that it works to establish a new paradigm for identification, which incorporates various types of information, creates a specific type of digital citizen, and generates new power dynamics.

2.2. Power and empowerment

As identification processes work to create identities, they are inevitably bound up with power dynamics, defining, for example, how identities should be created or when people should be identified. One of the main ways in which power is often discussed in the literature on digital identification, is the potential for surveillance that these systems hold (see e.g. Amoore, 2006; Lyon, 2007; Epstein, 2007). As I briefly addressed above, identification systems have been conceptualised as means to make people more 'visible' (Lyon, 2008; 2010). As such, these systems are intrinsically connected to power, as the entity - usually the state - in charge can monitor populations. As I will show in this dissertation, SSI technology is interesting in this regard, because it is supposed to fix some of the issues associated with earlier identification systems. In particular, the objective to 'empower' individuals by putting them in control of their personal data and digital identity, is supposed to be a departure from other types of 'centralised' systems, where all information is stored in one database, which facilitates surveillance (see e.g. Schoemaker et al., 2023). As I argue in this dissertation, this focus on 'control' is an important part of the sociotechnical imaginary underpinning SSI technology, and can directly be linked to the fact that SSI started out as an identity model for the internet. Now, this model is applied to the domain of the state, and, as such, citizens will be 'empowered' through control over their data and digital identity. The literature has discussed the tension between power and empowerment in digital identifications systems, though this issue has hardly been addressed in relation to control over data and digital ID wallets yet. Furthermore, most of the existing literature discussing this tension focuses on development contexts. Addressing this tension in the context of the EU has wider relevance, particularly because the EUDI Wallet has the potential to become a standard-setting technology (Tobin, 2022).

As I mentioned above, the literature can be loosely categorised according to different logics underpinning digital identification systems. After having focused on securitisation, the literature took what some have called a 'developmental turn' (Martin, 2021). This literature engages with the link between digital identity and development, as digital identity systems have been proposed as a means of granting people access to essential rights and services (Masiero and Bailur, 2021; Gelb and Clark, 2013). As such, digital identification systems are supposed to be an empowering tool, because they can allow people to access services that they might otherwise be denied. At the same time, however, this also paved the way for widespread surveillance (Center for Human Rights and Global Justice, 2022). One of the main case studies through which power and empowerment are assessed, is Aadhaar in India, which is the largest biometric ID system and data base in the world (OECD, 2018). For example, scholars have argued that Aadhaar is simultaneously a tool for surveillance and a means to financially include poor and marginalised populations (Jacobsen, 2012), or that it, despite its emphasis on service delivery to marginalised groups, also 'carries the potential to profoundly redefine the relationship between the state and its subjects in starkly transactional terms' (Masiero and Shakti, 2020: 2). Others have pointed to the negative effects of these systems, which often result in people being excluded from access, or malfunctioning systems preventing them from access (Drèze et al, 2017; Masiero and Arvidsson, 2021; Khera, 2019). Researchers have also paid attention to the role of the state; conceptualising Aadhaar as a means to reassert its power as it allows the state to be omnipresent (Nair, 2019), or the state as 'arbiter in the circulation of citizen data' (Singh, 2019: 501). In this system, citizens are datafied, giving rise to 'coded citizenship' (Masiero and Shakti, 2020: 3) which enables the state to extend its surveillance practices. Similarly, Chaudhuri and König (2018) have argued that this system is coded in terms like 'empowerment' and 'inclusion', while turning citizens into customers, responsible for their own transactions.

A related literature looks at digital identity systems in humanitarian aid. This literature is generally critical of digital identity systems, and discusses the increasing use of digital technologies to measure, monitor and experiment on refugees, and flags up the lack of transparency to refugees themselves in these systems (Lemberg-Pedersen and Haoity, 2020; Madianou, 2019; 2020; Schoemaker et al., 2021). While not directly related to state-sanctioned identification systems, it is important to mention this literature, because these systems are often seen as instances of experimentation (Madianou, 2019; Aradau, 2020) and demonstrate how digital identity developments are not happening in a vacuum, but influence each other on a global scale. As Weitzberg et al. (2021) point out, identification is inherently ambivalent, because it combines *power over* and *power to*. They argue that '[r]ather than two sides of a binary debate, surveillance and recognition are mutually compatible developments that are increasingly collapsed', and, as such, '[i]dentity technologies have opened up avenues for formal claims-making just as they have enabled extractive and intrusive forms of monitoring' (Weitzberg et al., 2021: 2). As such, there is an inherent tension between the potential for surveillance and for empowerment (Weitzberg et al., 2021; Madon and Schoemaker, 2021; Martin and Taylor, 2021). This literature therefore addresses a tension

between individuals and larger actors; between power and empowerment. As I mentioned above, this dissertation also addresses this tension: it looks at the sociotechnical imaginary of 'control' that underpins the wallet, and how digital citizens are enacted in relation to this. However, the 'empowerment' that SSI proponents mean, is not so much related to gaining access to services (although that is what the wallet does), but rather to gaining 'control' over one's data and digital identity – a promise this dissertation critically examines.

In addition, the dissertation interrogates the larger power dynamics surrounding the creation of the wallet. The credentialisation of identification means that different actors are inevitably involved, as the wallet does not only focus on state-issued identification documents. As such, it is important to pay attention to the different actors that part of the (development of) this identification system. Power structures beyond the state have not been addressed extensively in the digital identification literature. While there are references to the increasingly complex assemblage of actors, existing accounts are either very general or very specific, as they signal the increased involvement of non-state actors but do not go in depth; or do go in depth, but only regarding a specific case. This dissertation aims to contribute to this literature by paying attention to the 'big and the small' (MacKenzie, 2005; De Goede, 2016), linking the small technicalities, such as the standardisation of credentials, to larger power battles, involving, for example, the EU and Big Tech companies, as well as the technical experts involved in the development of the wallet.

Some scholars have noted the increasing influence of and dependence on corporate actors in the development of identification systems (Caplan and Higgs, 2013). Notably, Lyon (2010; see also Lyon and Bennett, 2008), has signalled the emergence of what he terms a 'card cartel'. He points out that digital IDs are, even though they are national systems, increasingly globally interoperable; that these are dependent on hardware and software; and that large corporations compete to establish identification systems. As he puts it: '[t]ogether, these factors mean that much more than "the state" is involved in IDs' (Lyon, 2010: 608). From an Information Systems perspective, Whitley and Hosein (2010) have looked at the relationship between technological expertise and decision-making in regard to the UK's identity policy. Similarly, Eaton et al. (2018) address the relationship between the financial and public sector in regard to creation of digital ID solutions in Denmark, Norway and Sweden, while Medaglia et al. (2021) interrogate the power relationships between public and private actors in the development of digital identification systems in the UK and Denmark. Van Dijck and Jacobs (2020) address how sociotechnical and political-economic choices impact the design of eID (another term for digital identity) in the context of the European Union. They argue that 'developing eIDs requires more than engineering ingenuity and legal compliance; they involve negotiation of conflicting social and political values' (Van Dijck and Jacobs, 2020: 897). Importantly, they are also among the few researchers who address the connections between identification by the state and on the internet.

Other researchers, focusing on identification for development, have pointed to the increasing influence of corporations in the construction of identification mechanisms for

refugees (Madianou, 2019; 2020) and increasing number of public-private partnerships in identification schemes (Sperfeldt, 2021; Lemberg-Pedersen and Haoity, 2021). Similarly, Singh (2019: 516) addresses how interests are balanced in public-private partnerships underpinning Aadhaar in India, arguing that it creates 'new distributive regimes of control for public–private partnerships in government services.' In a similar vein, Hicks (2020: 330) signalled the emergence of 'digital ID capitalism' in the Indian context, where 'state agencies help guarantee personal data for commercial exploitation', as they are working with businesses that gain access to this data generated by a state-managed infrastructure.

This literature shows that identification is not as simple as a relation only between states and citizens anymore; due to the increasing complexity of digital systems, as well as the availability of more data, processes of identification have become more complicated, and have increasingly become a way to make profit; either through the development software and hardware, or the use of the data that is generated through these systems. Applying a transversal perspective, this dissertation shows that different actors sometimes cooperate and sometimes compete, showing that power dynamics around the wallet are not straight-forward, as different actors exercise different kinds of power.

In addition to literature that addresses changing power dynamics by looking at actors, there is a small literature that addresses the establishment of alternative power structures through technology. Some of this literature addresses technologies such as blockchain in relation to the state and citizenship. This is relevant, as SSI technology is, as I described in the previous chapter, family of these other decentralised technologies. However, the existing literature does not address SSI or its underlying sociotechnical imaginaries.

The main case study in this regard is the 'e-Estonia' programme, which was first 'e-state' and drew attention because it allowed people and businesses outwith Estonia become 'e-residents', thereby subverting traditional membership structures (Kotka et al., 2015; Tammpuu and Masso, 2019). e-Estonia is considered one of the most advanced blockchain-based systems in e-government (Alexopoulos et al., 2021). In general, blockchain in governance has been researched in relation to new models for governance that it could bring about, focusing, for example, on its relationship to social-contract theories (Reijers et al., 2016), the role of the state in blockchain-based governance (Aztori, 2017) or the implementation of blockchain in existing (power) structures (Hoffman, 2021; De Filippi and Loveluck, 2016). More specifically, in the context of e-Estonia, this system has been praised, as it could bring about 'cloud communities', which offer 'non-territorial forms of political membership, remodel the way people think about sovereignty, and challenge the definition of the state as we know it' (Orgad, 2018: 259; see also De Filippi, 2018), but also criticised. As Semenzin et al. (2022) argue, the different narratives surrounding blockchain may contribute to exploiting the public imagination, while not actually disrupting anything, or should, as Budnitsky, (2022) puts forward, be seen as a new form of nationalism in the digital age, part of Estonia's objective to distance itself from its Soviet past. As such, this literature addresses power in a different way, as it is seen in relation to the technology that is supposed to disrupt

existing power relations. This dissertation critically interrogates similar claims, but specifically focuses on identification.

2.3. Self-sovereign identity technology

Now that this research has been contextualised with the wider literature on digital identification, it is important to look at the literature that has specifically addressed self-sovereign identity technology. While previous literature on digital identification systems has emphasised the focus on 'securitisation' and, after that, development, SSI technology does not (exclusively) match those objectives. Rather, it is underpinned by a logic that comes from the internet, which, as I will show, is mainly related to consent mechanisms and establishing 'control' over personal data and digital identities. However, the current literature has hardly explored SSI in depth. While there are a few studies, most existing social science literature only engages with SSI superficially: extensive, empirically grounded research where the concept of the technology is seen in relation to its implementation, and where its core promises are mapped out and assessed critically does not exist yet. This dissertation aims to fill this gap by looking at SSI technology in the context of the European Digital Identity Wallet, showing the sociotechnical imaginaries that underpin SSI technology and how these are adapted to the context of the state, what kinds of digital citizens it enacts and what new power dynamics it produces. In doing so, it links empirical detail to theory as well as normative concerns.

Up until now, most of the literature on SSI is written from a computer science perspective. These papers usually discuss aspects of the technological architecture such as its compatibility with blockchain (Van Bokkem et al, 2019; Mühle et al, 2018; Naik and Jenkins, 2020; Stokkink and Pouwelse, 2022), the use of verifiable credentials (Seldmeier et al, 2021; Mukta et al, 2020), or selective disclosure (De Salve et al, 2022; Mühle et al, 2023). There are also a few more sector specific studies, for example looking at SSI's potential for the education (Grech et al, 2021) or health sector (Laatikainen, 2021; Halpin, 2020). This means that while the technical dimension has enjoyed some attention, the social aspects have hardly been discussed yet. In fact, the social science literature on SSI is very limited, with only a handful of studies to date.

Some of this work addresses SSI's potential for inclusion. For example, Wang and Filippi (2020) assess the potential of SSI as a tool for economic inclusion, arguing that it could be a means to give vulnerable populations access to a working identity system. Similarly, Elliot et al. (2022) look at the possibility of SSI for financial inclusion of vulnerable populations in the banking sector. They point out that there is a tension between the promise that individuals will get full control over their identity, and the requirements banks must fulfil, in particular the information needed to comply with Know Your Customer regulation. In a similar vein, Cheesman (2020) focuses on the promises of an SSI project for refugees, arguing that SSI would still have to meet the requirements of established institutions, which makes it likely that these systems will be incorporated in existing mechanisms of power. In a different paper, Cheesman and Slavin (2021) make a similar argument: comparing two SSI projects for refugees, they argue

that the concept of SSI is being reconfigured by vendors, as they have found ways reintroduce traditional actors (Cheesman and Slavin, 2021). Gstrein and Kochenov (2020; 2021) warn that uncritical implementation of SSI technologies in both the global north and the global south, may only further entrench current citizenship inequalities on a global scale. As different citizenships already come with different bundles of rights, they argue, digital identity systems will inevitably interact with this reality, and if these issues are not addressed in the design, this is unlikely to change.

From a philosophical point of view, Ishmaev (2021) assesses the normative and ethical implications of 'self-sovereignty', pointing out that it is important to consider the deeper 'moral desirability' (Ishmaev, 2021: 250) of a persistent and singular identity. Also Zwitter et al (2020) present different definitions of identity, ranging from philosophical, to legal to technological ones. Building on these, they argue that digital identity is transforming from something that was purpose-driven (e.g. a particular identity needed for a service), into a 'self-standing activity' (Zwitter et al., 2020: 1), an infrastructural service which can be used for many applications.

Other recent studies pay attention to the discourse around SSI technology, and how this is influenced by different stakeholders involved. While in line with the topic of this dissertation, this research is still relatively general, as these studies do not focus on a specific case. For example, Weigl et al. (2023: 2) put forward that SSI is a heterogenous concept, and analyse how 'stakeholder interests and institutional properties shape the social embedding of self-sovereign electronic identification systems,' ultimately arguing that the discourse around SSI is value-laden and its socio-political ambitions are ambiguous, with stakeholders emphasising different elements. However, they argue, this ambiguity can be mitigated by enforcing limitations and constraints when the technology is implemented. Similarly, Benchaya Gans et al. (2022) point out that SSI literature often takes a simplistic view of its societal implications, as the implementation of the technology is likely to be impacted by stakeholders and bureaucratic structures, but do not go in detail about who these stakeholders are. They also reflect on SSI's potential impact on the relationship between citizens and the state, and argue that while there is potential to strengthen citizens' role, as data management is shifted from governments to citizens, there is also the risk that it might weaken their position (Benchaya Gans et al., 2022). However, this research remains theoretical, and does not include empirical data.

To date, there are two articles that look at SSI and the European Digital Identity Wallet specifically. Schoemaker et al. (2023) suggest a preliminary typology of types of digital identity, distinguishing between 'Big ID', which refers to centralised biometric systems, SSI or decentralised models (with the EUDI Wallet as example) and 'super apps', a type of digital wallet that is not decentralised, but fulfils a similar function of integrating many different functions and services in one app. They ultimately suggest that these different systems could lead to differential access to rights and services, but do not discuss the nature of these different systems in depth. Giannopoulou (2023) does focus specifically on SSI in relation to the European Digital Identity Wallet. She argues that the implementation of SSI will not solve

historical shortcomings regarding identification, such as overidentification or sharing of data between public actors. She also suggests that 'it is difficult to imagine the disempowerment of the state as an identity provider in favour of a self-sovereign decentralised identity that favours user empowerment' (Giannopoulou, 2023: 17), as the state will remain legally responsible for identity provision, which will also need to be guaranteed in the technical system. While Giannopoulou (2023) addresses an important tension, she only briefly addresses the European Digital Identity Wallet, and focuses on EU institutions that are not directly involved with the development of the wallet. The article also incorrectly assumes that SSI is always built on blockchain.

This relatively superficial engagement with SSI technology reflects a wider problem in the existing literature: most accounts only provide a basic description of what SSI is, which, except for the work of Cheesman (2020) and Weigl (2023) et al., does not involve fieldwork. As such, the literature lacks an in-depth exploration of what SSI is, according to the people who are working on it, and how it is implemented in reality – like in the case of the EUDI Wallet. Furthermore, while some of the literature, notably Gans et al. (2022) and Gstrein and Kochenov (2020; 2021), do address the potential impacts of SSI technology on citizenship, this is not grounded in a specific case, and, as such, does not address the details of what implementing this system would mean. Lastly, while the existing literature addresses power relations in the sense that it is SSI's aim to change the power dynamic between actors such as states or companies, and individuals through decentralisation (Gans et al., 2020; Giannopoulou, 2023), the literature does not address power dynamics beyond this concept. The exception to this rule is Cheesman (2020) and Cheesman and Slavin (2021) who do critically evaluate the power of actors in the humanitarian system to change SSI, but this is a different context to the one that I address. Therefore, this research is one of the first exploratory studies that provides an in-depth account of SSI and its implementation in the EU, and critically explores SSI's core goals in this context.

2.4. Conclusion

As I have shown above, the literature on digital identification has addressed several waves of technological development. Analysing the ways identities are made machine readable, 'fixed', categorised, and how legal and digital identity are increasingly conflated, this literature is an important foundation for this research. Similarly, the literature looking at different power dynamics, such as the tension between power and empowerment, the different actors involved in the (establishment of) digital identification systems and the negotiation of power structures through new, decentralised systems, is a starting point for this analysis. This dissertation takes up these issues through an in-depth analysis of the implementation of SSI technology in the form of the EUDI Wallet. With this, it contributes to the literature on digital identification by exploring a digital identity model that has hardly been researched yet. While some studies sketch the contours of the potential issues with this technology, the current social science literature on SSI has not addressed the technology in an empirically grounded way,

where the concept of the technology is seen in relation to its implementation, and where its core promises are mapped out and assessed critically. Therefore, while not a classic empirical study, as it also includes some normative suggestions, it is one of the first elaborate, exploratory studies on this topic, which links larger issues to empirical detail. It provides an in-depth account of the sociotechnical imaginaries underpinning the technology, and the adaptation of SSI technology - that was developed for the internet - to the domain of the state. In doing so, it critically evaluates how identities are created; what kind of digital citizens are enacted through the wallet. Building on this, it also analyses the new power structures that digital ID wallets produce. The dissertation ultimately demonstrates that the nature of state-sanctioned identification is changing: the credentialisation of identification gives rise to new systems, new digital citizens, and new power dynamics.

Chapter 3. Methodology

A prominent SSI figure once said 'with the European Digital Identity Wallet, we are going from theory into reality'[3]. This quote perfectly exemplifies the newness of SSI technology: while it was only a sociotechnical imaginary before, it is now on its way to becoming a tangible, material reality in the form of the European Digital Identity Wallet. The fact that the technology is still on its way to being implemented shaped the research design for this dissertation: it meant that the design needed to be flexible and iterative, so that new developments could be included as they occurred. To follow how the digital wallet is socially shaped, digital citizens are enacted and power structures are (re)configured, I interviewed experts, attended industry events, and did documentary research. In this chapter, I outline this methodological strategy.

In the first section, I introduce my research questions. I subsequently detail my approach to doing fieldwork and rationale for choosing this approach. The third part reflects on the unforeseen role that LinkedIn took in my research. This is followed by a section detailing the methods, namely interviews, attending industry conferences and documentary research. I then discuss my approach to data analysis, and close with additional ethical reflections.

3.1. Research questions

The overarching objective of this dissertation is to look at how state-sanctioned identification is changing due to the arrival of digital ID wallets. The research questions all address different aspects of this query. I look at this in the context of the European Union, as the European Digital Identity Wallet is currently the main example of this type of new identification system. As such, the first question refers to the fact that SSI technology was originally developed as an 'identity layer' for the internet - but is now being applied in the context of the EU. As such, it becomes important to investigate whether it is possible to apply these internet logics to a different sphere, and if so, how the technology needs to be adapted to do so. The second question builds on this: as this identity model is no longer applied to users on the internet, but rather to citizens in (EU) states, what does this mean for citizenship? And how could this potentially impact both citizens and non-citizens? It is important to bear in mind here that the EU is a supranational organisation (Lopez-Claros, Dahl and Groff, 2020), though it has state-like qualities and capabilities and is sometimes referred to as a 'superstate' (Glyn, 2005). Similarly, as I mentioned, European citizenship is contested, as it is derived from national citizenship in one of the member states (Bauböck, 2014). However, as I will show, the EUDI Wallet is, despite the connection between sovereign states and identification, developed at the European level. Therefore, it becomes possible to assess how digital citizenship is being shaped through this EU-wide identification system. Finally, the third question places the emergence of digital ID wallets in a larger context: because this new identification system involves a technical object,

[3] Identity & Technology Forum, Germany, May 2023.

new actors will inevitably be involved. As such, it is necessary to look at how the wallet (re)produce power dynamics, as this ultimately reveals the changing position of states in matters of identification.

1) What sociotechnical imaginaries underpin SSI technology and how is this arrangement (of technologies and sociotechnical imaginaries) translated into the context of the state through the European Digital Identity Wallet?

2) How do SSI/the European Digital Identity Wallet shape digital citizenship?
   - How may this impact citizens and non-citizens?

3) How do digital ID wallets (re)produce existing or new power dynamics?

3.2. The Scavenge: doing fieldwork

What initially captured my interest in SSI was the unlikely marriage of a technology which was originally created for the internet - and was underpinned by a distrust in institutions and a strong belief in decentralisation – to the EU, a political body that has been described as a 'superstate' (Glyn, 2005). I wanted to see how this technology would be transformed and used in the domain of the state, and what this would mean for citizens. As the technology is still under development, it still exists in part as a sociotechnical imaginary about the future, while also becoming 'real' at the same time. This position, in between the ideological and the material, offers the opportunity to look at the 'social shaping' (Wajcman and MacKenzie, 1999) of this technology. Because of this 'in between' position, I decided that the best way to study SSI was to follow this 'object' to see how it was socially shaped, and how sociotechnical imaginaries are brought to life. This meant 'studying up' (Nader, 2018): following the people who are involved in the creation of this technology. I did this through conducting interviews, attending events, and analysing this community's written outputs. As MacKenzie (2005) suggests, to understand a technology, it is necessary to speak with those involved. Knowing how a technology works, he argues, makes it possible to see its connection to larger issues and structures; how the 'big' is embedded in the 'small' (MacKenzie, 2005). In the literature, technical communities have been called 'tech workers' (Dorschel, 2022) or even 'coding elites' (Burrell and Fourcade, 2020). While the SSI community might not be quite as powerful as the elites Burrell and Fourcade (2020) describe, it cannot be denied that this group, that sometimes call themselves 'identerati' or 'credentialites', have significant influence on the development of digital identification systems. As such, asking them how the technology works, what its objectives are, can provide insight into the sociotechnical imaginaries (Jasanoff and Kim, 2015) that underpin it. For reasons of clarity, I will refer to this group as 'the SSI community' in this chapter. This also includes the people working on the European Digital Identity Wallet.

Deciding on suitable methods was not a straightforward process, as the technology is not developed in one place, and there are barriers to access, especially to the opaquer decision-making processes in the EU and some closed SSI working groups. What is more, these groups often did not meet in person; most communication happened through digital channels that were not accessible to researchers. In a methodological contribution about the ethnography of algorithms, Nick Seaver (2017) introduces 'the scavenge', where information is derived from multiple sources and multiple sites. As Seaver (2017: 6-7) puts it: 'the scavenger replicates the partiality of ordinary conditions of knowing - everyone is figuring out their world by piecing together heterogeneous clues—but expands on them by tracing cultural practices across multiple locations (Marcus, 1995) and through loosely connected networks (Burrell, 2009).' In other words, he makes the case for 'scavenging' for information, for example by finding informants in multiple sites, rather than the prolonged presence in one location. Furthermore, data are not only derived from interviews; there are other, unconventional data sources that can help supplement and triangulate the data collected. To quote Seaver (2017: 7) again: '[o]n mailing lists, in patent applications, and at hackathons, I found arguments, technical visions, and pragmatic bricolage. […] There is much to be scavenged if we do not let ourselves be distracted by conspicuous barriers to access.'

As such, a method where different types of data are combined, emerges. Researching self-sovereign identity technology and the EUDI Wallet asked for a similar approach, as my research 'object' could not be found in one place. The community working on it is globally dispersed, and, as mentioned above, the technology is sometimes discussed in closed meetings. In addition to access barriers, it was important to work with the fact that the development of the technology is an ongoing process, and new materials therefore keep being published. This asked for an iterative approach, as defining the sample beforehand would obstruct the possibility to account for new developments. As such, different types of documents, such as blogs, whitepapers, and LinkedIn posts became primary data, that reveal something about the way in which the object of SSI is socially shaped and put into the social world – these documents became part of 'the scavenge' and helped direct it. In addition, as the European Digital Identity Wallet is the result of new EU-wide legislation, relevant EU policy documents and communications needed to be included as well.

Conducting interviews with people working on the technology, and attending their industry events allowed me to immerse myself in this social world, where there are particular ways to talk about things, particular imaginaries, vocabularies and ideas about the new social order that is SSI supposed to bring about. However, events only last a few days and interviews can only go on for so long. It is for this reason that the 'scavenge' method proved very useful; it allowed me to put different types of information together and see the continuity and overlap between these different sources. For example, I would read a blog post on LinkedIn, or an interviewee would make a particular statement, which then led me to include a question about this topic in the next interview. As such, the data collection was an iterative process, where I collected data from different sources, which mutually informed each other. This was a fruitful approach to a topic that has not been widely researched and theorised yet.

Because of the newness of this research topic, this research is exploratory (Tie et al., 2019). My initial approach took inspiration from constructivist grounded theory principles, where data collection and analysis take place at the same time, and the analysis helps identify gaps where more data are needed (Charmaz, 2006; 2014). I chose this approach because hardly any research had been conducted on this topic yet, and this method would allow me to be flexible. However, I moved on from this approach as I found that theory helped better direct the research. For example, the concept of 'sociotechnical imaginaries' (Jasanoff and Kim, 2015) helped me to see the development of the technology in a particular light, and allowed me to focus on its ideological components, both in my interviews and in the way that I approached events and documents. As such, 'the scavenge' became more directed. For example, it made it possible to see how sociotechnical imaginaries enact a particular 'user-citizen' who is supposed to manage their wallet. In addition, grounded theory is less suitable to look at actors and power dynamics; applying a social shaping (Wajcman and MacKenzie, 1990) lens and power theory (Avelino, 2021) made it possible to conceptualise what is shifting. As such, while my data collection process is indebted to grounded theory approaches, it is not completely in line with the traditional grounded theory methodology - not least because grounded theory has traditionally relied on induction, where the theoretical framework is not imposed beforehand, and the theory is supposed to emerge from the data (Glazer and Strauss, 1967), and my research does have an imposed theoretical framework. As this framework was refined throughout the research process, it is more in line with an abductive approach, where the researcher goes into the field with a theoretical awareness, but should 'develop their theoretical repertoires throughout the research process' (Timmermans and Tavory, 2012: 180).

3.3. LinkedIn as research device

While I had not planned this from the outset, LinkedIn quickly became an indispensable tool for conducting my research. It did not only allow me to find research participants; it also made it possible to immerse myself in the professional world of those working on SSI, as the community would very regularly write blogs, posts, or short opinion pieces on the platform. In addition, through LinkedIn, I was informed of key events happening in the sector, and attended five of them. As such, LinkedIn became a research device that helped bring together the different materials to be scavenged. It became an important source of information, as well as a means immerse myself in 'the field', which was part online, part offline.

Being in this field allowed me to identify key SSI community members: certain 'thought leaders' who post regularly and whose opinion is widely respected in the community, almost gained the status of celebrities in this field. As such, LinkedIn helped me access most of the 20 people I interviewed. Through LinkedIn, I found several members of the eIDAS Expert Group, who develop the technical specifications for the EUDI Wallet. This was helpful, as these members are not listed on any EU website; they remain anonymous unless they decided to put it in their own online bio or CV. I also saved 250+ posts, which often referred to information

like blogs and opinion pieces. These different types of data, which I gathered over the course of 2022 and 2023, incrementally informed my research.

To establish connections with potential respondents, my own profile needed to represent my role as researcher as well. My profile included my CV, a link to my university profile, and short description of my research. As such, I had to perform my identity on LinkedIn, emphasising certain parts of my identity to cultivate my professional image (Van Dijck, 2013). Not only did this assure my respondents that I was real person; it also granted legitimacy to my research, as it was now part of my professional biography. This became clear during some of the interviews, as I noticed that some interviewees trusted me more because I was on LinkedIn. During one interview, my respondents suddenly remarked: 'sorry, I'm being very rude and stalking you on LinkedIn as I'm talking to you.' This prompted a conversation about the importance of verifiability, and being sure that someone is who they say they are. My respondent elaborated:

> 'Suppose…like I trust you because you're on LinkedIn, right? I looked you up on LinkedIn, you know if I talk to someone and they're not on LinkedIn, then I assume they are […] a Chinese spy or something, you know what I mean. But because you're on LinkedIn, there is lots of people that will vouch for you. I mean if LinkedIn issued an identity, saying "this person is a real person, they've been on LinkedIn for more than one year, they have more than a thousand people connected to them", in lots of cases, that would be an important credential.'

Therefore, being on LinkedIn helped me experience what credentialisation could mean first hand. My profile served as a de facto credential, which helped establish the validity of my claim that I am a PhD researcher interested in digital ID wallets. As such, this experience made me 'live' the research in a different way: my 'LinkedIn credential', helped 'verify' that I was who I claimed to be. Being 'verifiable', in this case, was important for the research, as it helped to establish trust between my respondents and myself. What is more, this also shows that the credentialisation of identification is about more than only legal identity documents; it could include any kind of information that helps verify an identity or entitlement. It therefore illustrates that credentialisation encompasses more than only traditional identification practices; as it works to make different aspects of our lives 'verifiable'.

It is important to highlight that the access LinkedIn offers comes at a cost: some of the more useful functions for research require payment. Looking at a profile without the person being notified that someone has visited their profile, as well as the option to send direct messages without being 'connected' to the recipient, requires having 'LinkedIn premium', which costs £55 a month. To be able to reach out to respondents, I renewed my subscription several times. There were, therefore, costs attached to access.

Another important issue I considered is the ethics of 'hanging out' in this (professional) world. As this online world includes many participants, and does not have clear boundaries to the community, it is near impossible to ask every member for consent to use their posts. There

is no consensus on the ethics of using online interaction; while some maintain that the internet is by definition a public space, which makes informed consent unnecessary (Kitchin, 2003), others argue that interactions between internet users occur in private spaces, that should not be accessed without consent (Kozinetz, 2015). An important distinction in these debates, is the distinction between 'public' and 'private': some information was never meant to be seen by members outside of the community, while other spaces are accessible to the wider public (AOIR, 2012). The information that I read on LinkedIn is publicly available. Furthermore, the data I gathered did not include any personal information, and only referred to work-related developments. Importantly, most of the posts contained opinions or suggestions that were intended to be a contribution to the professional world of SSI. I did not cite much of this information directly, and even if persons were to be recognised, it is unlikely that this would result in harm, as these are professional opinions that do not include sensitive data. Furthermore, as the space inhibits a large number of people who come and go, it would be difficult to obtain consent from each of them individually (Huang et al, 2023). For these reasons, I decided that obtaining informed consent to read and use posts, blogs and articles was not necessary.

3.4. Interviews

To analyse the social shaping of SSI technology and the EUDI Wallet, I conducted 20 interviews with experts in this field. The interviews lasted approximately one hour and were conducted over Zoom. The interviews took place online because the community working on the technology is globally dispersed. While researchers have pointed out the limitations to online interviewing, such as the fact that one can only see the other person's face, and might thus not be able to pick up body language as well (Howlett, 2022), the online format did not seem to pose any significant challenges to the interviews. As this group is used to collaborating with others online, they were familiar with this format, and did not express any discomfort over the online setting. What is more, the online format was in some cases also conducive to the interview process; on several occasions, respondents sent me links through the chat function, or even shared their screen to show me relevant information.

The interviews were semi-structured: this was to guide key themes in the interview, but also leave space to follow up on respondents' answers. While all interviews included a set of the same key questions, I adapted other questions depending on the interviewee's position and work context. Moreover, some questions changed as I gathered information and gained a deeper understanding of the issues in the field. My own understanding and insight developed as I conducted more interviews, but also because of my regular presence on LinkedIn and at industry events, where I familiarised myself with the ideas and debates in this community. As such, the iterative approach to data collection allowed me to develop and ask different or more detailed questions along the way.

I interviewed experts in self-sovereign identity technology and technical experts working on the European Digital Identity Wallet, particularly those involved with the technical

specifications of the wallet. I did this because these experts are very close to the development of the technology. Speaking to them made it possible to gain insight into the social shaping of the technology, as they told me about development processes, imaginaries and goals (Wajman and MacKenzie, 1990). What is more, this made it possible to learn about the implications for citizens, the users of the wallet, for the design of the wallet plays an important role in how they are supposed to interact with it (see e.g. Oudshoorn et al., 2004). In addition, interviewing these groups allowed me to connect the technicalities to larger issues. For example, learning about the standardisation of credentials and the political struggles around that, made it possible to connect these 'technicalities' to 'politics' (MacKenzie and Spinardi, 1988).

In addition to experts, the sample also includes one representative of a digital rights NGO that has been one of the few organisations criticising this project, as well as one employee of a large technology consultancy firm that is influential in this field. I interviewed the NGO representative to include critical voices. However, as this is the only NGO that is doing research on this topic, I was not able to include more interviewees in a similar position. I selected the tech consultancy firm representative because she is an active participant in the LinkedIn community, and I wanted to gain a sense of what big actors in the technology field might think of the move towards SSI technology. As this did not become an integral part of my research, I decided against including more respondents in similar jobs.

I identified most interviewees through LinkedIn. In two cases, they were referred to me by others, and in one case, a prominent SSI figure found me through Twitter (X). When a prospective respondent agreed to be interviewed, I obtained written consent. Respondents were sent a participant information sheet containing information about my PhD project, and were given the opportunity to ask any questions before they signed the form. The interviews were recorded and stored in an encrypted container on the University of Edinburgh's Data Store server (which is backed up in three locations), as well as in an encrypted container on my personal computer. I transcribed the interviews myself and stored them in a separate encrypted container (in the same locations). To protect their anonymity, I created pseudonyms for all respondents. As people's names are reflective of their culture and identity (Lahman, Thomas and Teman, 2023), I consulted lists of baby names from each interviewee's home country in order to generate fitting pseudonyms.

As I will also explain below, to analyse the interviews, I coded the transcripts. I performed two rounds of thematic coding: one round during which I generated broad codes, and a second round during which I derived more detailed thematic codes. The coding process helped me to structure the results and to see patterns in the data. To do this, I made mind maps to clarify the connection between the different themes. The interviews formed a key part of the results: they are the backbone of the story told in the three results chapters. Importantly, the interviews provided insight into the details of the technology and decision-making processes around it, that cannot be found in the documents. For example, through the interviews I learnt more about the EU's political goals for the EUDI Wallet, or about the technical details that showed that Apple was trying to influence the standard-setting process.

As such, the interview data helps to show the complexity of creating implementing SSI and the EUDI wallet, which is not just a technical, but also a social and political process.

One of the limitations of this approach, is that access can be difficult to obtain. Oftentimes, the people I approached would not respond to my request. In some cases, they would respond with questions, and were worried that they would not be able to help a sociologist, often because they felt that they knew about technology, and not about social concerns. It also happened several times that potential respondents initially said 'yes' but stopped answering my messages or emails. Another limitation is the lack of diversity: in this sample, only three respondents are women. Racial diversity was extremely limited too, as most respondents were white, with only one person of colour included in this sample. Finally, most respondents received a university education and had full-time jobs. However, while the diversity in this sample of interviewees is very limited, it does reflect the lack of diversity in the industry writ large, as the majority of people working in this field are university-educated white men.

Pseudonym	Role	Location	Gender
Aidan	SSI researcher for the EU	EU	M
Luke	Blockchain developer with interest in digital identity	EU	M
Patrick	SSI developer/dissident in SSI community	EU	M
Jack	SSI Expert	Australia	M
Lucas	Digital identity expert, working for several EU digital identity and blockchain projects	EU	M
Mark	Digital identity and Fintech expert	UK	M
Charlie	Director of a digital rights NGO	EU	M
Peter	SSI Researcher for large public/private research institution	EU	M
Andreas	eIDAS Expert Group member	EU	M

Olivia	SSI expert/consultant	UK	F
Marta	Digital identity consultant for a large tech consultancy	UK	F
Christoph	SSI expert	EU	M
Erik	eIDAS Expert Group member	EU	M
Carl	EUDI Wallet expert and developer, co-leading one of the Large-Scale Pilots	EU	M
Max	SSI expert	EU	M
Matteo	High-level civil servant for the EU, working on the EUDI Wallet	EU	M
Antonio	Technical consultant for the European Commission	EU	M
Sophie	SSI expert (two interviews)	USA	F
Frederico	eIDAS Expert Group member	EU	M
Marco	eIDAS Expert Group member	EU	M

3.5. Events

In addition to doing interviews, I attended five (industry) events. I attended these events to learn about SSI and the field of digital ID wallets more generally, to see how they were talked about in the sector, paying attention to current issues and goals. I went there as a researcher to get closer to this emerging field, by listening to the people who are working on this technology. Industry conferences are useful research sites, conference ethnographer Annete Nyqvist (2017: 1) argues, as this is the place where 'industries take shape and identities of professionals are created.' As such, these events can be seen as places where 'industry-specific knowledge is shared and negotiated' (Nyqvist, 2017: 5). This negotiation of knowledge also applies to the sociotechnical imaginaries underpinning SSI technology: these are created, negotiated and translated at events and conferences (Hockenbull and Cohn, 2021). Therefore,

attending industry events allowed me to learn about the field of digital ID wallets (and digital identity more generally), and how the people working on this technology imagined it would impact society. As these events are typically attended only by people in the sector, they provided insight in the professional debates that are currently taking place and how sociotechnical imaginaries are brought to life. In what follows, I use aliases for the events in order to guarantee attendees' anonymity (see Heaton, 2021).

I learned about three of these events through LinkedIn. The Identity Fair, the Identity & Technology Forum and the Digital Identification Conference are the main digital identity industry events on the European continent. I wrote to the organisers of the Identity Fair and the Digital Identification Conference, explaining that I am a PhD researcher studying self-sovereign identity, and that I would like to attend these events for research purposes. Similarly, on the website of the Identity & Technology Forum, there was the option to fill out a form to apply for a free entry pass. As the organisers were happy to open their doors to researchers, I received a complementary pass to all three events - with a combined value of £4905. These events are normally extremely expensive, and often paid for by attendees' employers. This means that for people who are interested, but do not work in this sector, there are significant barriers to access. I was invited to the two other events. One invitation was extended by one of my interviewees, who was hosting a key event in Switzerland. She invited me because the Radical Identity Meet-up was the first European version of a format that was foundational for the creation of SSI in the United States. The Country House Meeting was more obscure: this was a meeting of well-networked individuals who met for two days (in a remote country house) to discuss digital identity for refugees. I was invited because a colleague who received the initial invitation was not able to attend, and kindly gave the organisers my contact details instead.

Event	Dates	Hours
Country House Meeting, United Kingdom	October 2022	21 hours
Identity Fair, United Kingdom	November 2022	22 hours
Identity & Technology Forum, Germany	May 2023	40 hours
Radical Identity Meet-up, Switzerland	June 2023	28 hours
Digital Identification Conference, The Netherlands	June 2023	16 hours

Industry events are inherently limited in time (two to four days). However, attending these events involved working long hours, as they usually started around 8 or 9 am, and lasted till evening time, sometimes also involving drinks or dinner. As such, I was able to immerse myself in this space for an extended period of time. I did not engage in participant observation, but

rather attended these events to understand the digital ID wallet space. This consolidated my understanding, as it allowed me to see connections between different pieces of information, such as the whitepapers published, blogs on LinkedIn, and 'thought leaders' who sat on panels gave keynotes at these events - they seemed to know each other well, and often alluded to the fact that they often work and sit on boards of different organisations.

During these events, I produced handwritten notes and mind maps. These were only for my own use, and I am the only person who has access to them. The main limitation to attending events is that - as these events often attract hundreds of attendees - it is simply not possible to ask each person for consent. Guest et al. (2013) recommend reflecting on how private or public the setting is, what type of data you are collecting, and how you are presenting yourself. I did not focus on 'participants' or their interactions; rather I attended because I wanted to learn about this field and the technology. As such, I only gathered work-related information, and refrained from collecting any personal or sensitive data. I also did not record any sessions or conversations. Furthermore, when possible, I announced myself: I told people I met at these events that I was there in a research capacity. When I told them about my research, this was usually met with enthusiasm, and I was often told that SSI should get more academic attention.

During most events, it was clear that I was not a part of the community. I would often notice attended looking at my name badge, trying to figure out what I was doing there. For example, one person at the Identity & Technology Forum, who admitted to being curious enough to first google me, to then approach me and ask me more about the information he found, said: 'you are the only one taking notes.'

3.6. Documents

Documents became an indispensable part of the research because the SSI community frequently writes about the developments of SSI, and documents published by the EU are the most accessible way to gain more information about the EUDI Wallet. Blogs, whitepapers, LinkedIn posts, policy documents, EU communications became primary data, that allowed me to stay up to date in this world and engage with the debates in the technical community.

As this a rapidly growing field, I knew the number of documents available would keep on growing throughout my research. Therefore, I did not identify a sample of documents before starting the data collection process. Instead, I drew inspiration from Seantal Anaïs (2012) proposed method of seeing data as living, '[…] in the sense that new source materials were constantly being added and no prior decisions regarding what should be included were made' (Anaïs, 2012: 436). As a researcher of non-lethal weapons, the justification for her approach was twofold: by determining which documents to include beforehand, it is possible that 'rich materials may never be uncovered' (Anaïs, 2012: 436), and, secondly, as she is studying a sensitive topic, it is often shrouded in secrecy. While my topic is not as secretive, this method was useful as I studied an ongoing development: determining a sample beforehand meant running the risk of not being able to include relevant new information. This

method ties in with the 'scavenge' (Seaver, 2017), as it requires the same, flexible approach to 'scavenging' data. I structured the documents in the living archive using 'key demographics' (Gross, 2018: 546), namely their format (e.g. white paper; blog; legal document), author, data of publication and source, creating different folders in my Zotero library. The archive grew exponentially, as I learned more about the field, which voices were important to include, and which developments occurred.

Between 2021-2023,I collected five different types of documents: whitepapers, blogs, reports, policy documents and LinkedIn posts. Since its inception in the early 2000s, members of the SSI community have regularly published white papers, which I found through search engines. However, the white papers I included in my research were mostly published after 2015. This is because SSI technology started receiving more interest from companies, governments and NGOs around that time, which meant that the technology started to change and mature quickly. Faustino, Faria and Marques (2022: 70), who research white papers in relation to cryptocurrency, define them as 'key documents which govern the disclosure of technical innovation'. As such, these documents provide insights into the technical details of the technology, as well as the social, ethical or technical problems the innovation is responding to. The whitepapers that I collected were published by technical working groups working on the technology, such as the W3C, or the non-for-profit organisation the Sovrin Foundation. For example, one white paper entitled *The inevitable rise of self-sovereign identity* (Tobin and Reed, 2016) was particularly helpful for my research, as it was of the first comprehensive papers that explain the development and goals of SSI technology. Therefore, it was key to understanding the state of play of the field, as well as the ideological underpinnings of SSI technology. Importantly, therefore, white papers do not only convey technical information, but also allowed me to dive into the technical workings of the technology, but also the ideology and imaginaries surrounding it. Or, as Faustino, Faria and Marques (2022: 70) suggest, white papers can be seen as 'proposals of the techno-mediated social order'. This means that they are directly connected to the social shaping of the technology, as '[t]he things we call "technologies" are ways of building order in our world' (Winner, 1999: 32). Therefore, including whitepapers in my research contributed to the background and the findings, because they spoke to the connection between actual technical proposals and the change of the social order they promised to bring about, and therefore helped trace the social shaping of the technology.

In addition to white papers in the strict sense, I collected industry reports. These reports are usually more general, and often aimed at the more commercial side of the technology. Industry reports can be defined as 'comprehensive accounts of a particular industry, containing a depth of information, facts and statistics', such as financial statistics and details about companies in the sector (UNC University libraries, n.p.). While used less prominently in my research, reading industry reports was helpful to understand the development of SSI and digital identity more generally in relation to industry trends and the projected revenue of digital identity systems. For example, a McKinsey (2022: 4) report shows

that digital identity is a growing industry and adds reasons why 'leaders should pay attention'. Therefore, looking at industry reports adds context in terms of how the field of SSI and digital identity technology is perceived outside the community, and the impact the technology is expected to make. As such, industry reports were helpful to the background of the research, as they helped placed the technical developments in a broader context.

community regularly publishes on LinkedIn. Posts include blogs and opinion pieces, as well as news articles and links to new (SSI) developments. As I mentioned above, seeing interactions of the SSI community on LinkedIn was a valuable source of information, because it allowed me to gain insight into current issues and developments, as well as experts' opinions. In other words, it brought the SSI community to life in a way that only reading official reports could not, as reading the debates on LinkedIn gave me a detailed impression of the community and current topics of conversation. In total, I saved over 250 LinkedIn posts. These are blog posts and opinion pieces, as well as links to information about new technological and policy developments. I did not analyse these posts in a structured fashion (e.g. text or sentiment analysis). However, but these LinkedIn posts did play an important role in positioning this research, as they allowed me to follow the developments of the technology while I was doing the research, and, therefore, put the research in conversation with recent developments in the field. For example, through LinkedIn I found out when the architecture framework for the EUDI Wallet was updated, or when one of the consortia working on different use cases for this wallet made some progress. What is more, it helped to place the topic of SSI and the EUDI Wallet in a broader context, as other wallet initiatives were often discussed on LinkedIn as well. Being up to date with the current topics in the field also allowed me to adjust my interview questions accordingly, and ask about specific developments.

Most of the news articles and webpages that I gathered, I initially found on LinkedIn. Similar to the (blog) posts, these served as information that allowed me to stay up to date in regard to the developments in the field. These mainly served as background information, that helped me identify trends and key dates. As such, they informed the research as it allowed me to stay up to date with recent events and, similar to the LinkedIn posts, ask questions about recent developments during the interviews.

For the documents on the European Digital Identity Wallet, a different approach was required. Most of the documents were made available on the website of the European Commission. This includes legal documents, feedback from stakeholders and other EU bodies, general communications about the progress and aims of the proposed project, fact sheets and meeting minutes of the eIDAS expert group and press releases. Collecting these documents, which were released at different stages of the EUDI wallet project, allowed me to gain an overview of the trajectory as well as the motivations for developing the EUDI Wallet. I gathered official EU documents on the EUDI Wallet, which also included some of the documents on earlier iterations of the eIDAS legislation, published from 2014 onwards. Most documents, however, were published from 2021 onwards, as the amendment to the eIDAS legislation (which led to the EUDI wallet) was published in that year. These documents allowed me to analyse the ways in which the wallet is portrayed, as well as its projected aims and impacts.

For example, documents were an important resource for seeing how sociotechnical imaginaries of SSI were used in the EU context, how the EU framed the EUDI wallet in relation to citizens, and what they are supposed to gain from it. An important part of this was the new eIDAS legislation was essential to establish the functions and affordances of the wallet, as well as where the responsibilities about its development lie. Other documents, such as the EU's digital agenda, allowed me to place the wallet in the context of the EU's broader digital goals.

Whitepapers and industry reports	49
Saved LinkedIn posts, including blogs and articles	257
Other blogs and opinion pieces	27
EU documents	66
News articles and webpages	117

As I will describe in the next section, I coded most documents (with the exception of LinkedIn posts and news articles), generating broad themes, such as 'empowerment' or 'control'. These themes helped me write the story of the wallet, and informed the interviews. I was interested in finding broader patterns (e.g. new power structures) rather than providing a detailed account of a particular social group (e.g. the SSI community). As the information was filtered through me, the researcher, this is necessarily an act of interpretation. In line with grounded theory approaches, I aimed to explain rather than describe (Daly, 2017). This meant that the codes that I generated for the documents served to inform the story of what the wallet is trying to do in the world; how it is attempting to change existing power structures, for example. While generating codes can be seen as part of the analysis only (as it concerns sorting and bracketing data), it is necessarily a process of interpretation at the same time, for it is also a way to ascribe meaning to this data.

One of the limitations of documents is their relevance (Rapley and Rees, 2018); particularly because the sample was constructed while the research was developing, my selection has strongly impacted the research. It is, therefore, important to consider my position as a researcher, and the impact I had on the document sample. A second limitation has to do with the question where the documents come from: as discussed above, it is important to consider whether LinkedIn posts could be considered public information. The other types of documents that I collected were all published to be accessed by the public, and therefore do not pose any significant ethical issues.

3.7. Data management and analysis

As I described, the data collection process was an iterative one, where I continuously reviewed the data gathered through interviews, documents and attending industry events. This meant that data analysis took place simultaneously, and helped inform subsequent data collection. In order to do this, I transcribed the interview data as well as my field notes. I imported this data and the documents into NVivo.

Viewing the documents in conjunction with the interviews and data I gathered at events, helped me to gain a more holistic understanding of SSI technology. This allowed me to analyse how this technology is socially shaped and how sociotechnical imaginaries are put in practice. Looking at these different data sources allowed me to trace topics through documents, from the 'online' (LinkedIn discussions) to the 'offline' (conference presentations and conversations). As such, the different types of data were not only triangulated, but also mutually informed each other, and helped me crystalise interview questions as well as themes to look for in subsequent document collection. To make connections between the data, I wrote memos throughout the process, which helped me to identify themes and patterns. I also made mind maps, connecting different bits of information to see larger patterns emerge.

In the living archive, I differentiated between documents that served as background information, and documents that needed to be analysed more closely. As such, the LinkedIn posts mainly helped to guide my research and identify developments in the field. I therefore did not scrape and code the posts that I saved. However, this data was very useful as it helped me define some core themes surrounding SSI and the EUDI Wallet, and guided my thinking as well as interview questions. Being present in the community's professional world on LinkedIn helped me navigate the research; it gave me the necessary background that allowed me to assess and analyse information. The blogs and opinion pieces I used in this dissertation were carefully selected with this knowledge in mind. Similarly, news articles served as additional information that allowed me to trace the developments in the field. As it was not my aim to assess their tone or sentiment, I did not include these in the coding process either.

I did code the whitepapers and EU documents, using thematic codes. This entailed finding larger themes in the documents and categorising them accordingly. Broad codes encapsulated recurring topics in the documents, such as 'empowerment' and 'trust'. This allowed me to see the main themes that occurred across documents, and as such, to distil the sociotechnical imaginaries behind the technology.

The interview data went through two rounds of thematic coding. The first round, broad thematic coding, allowed me to identify themes in and connections between the data. I generated some key themes, including but not limited 'citizenship', 'power structures', 'values', 'empowerment' and 'future making'. After comparing these codes with my memos and other data sources, I performed a second round of coding. This focused coding generated a set of more specific codes, which crystallised patterns and connections. Examples are 'standards', 'paradigm shift', 'financialisation', and 'data exploitation'. I connected these specific codes to the broad ones to see the connections between smaller and larger patterns.

Having done this, I went through all of the information again, establishing links between different types of data, and writing additional memos. These codes and the connections between them formed the basic structure of the dissertation.

3.8. Other ethical limitations

My own position in the field urged critical reflection. The main ethical inquiry concerned my relationship with my respondents. Without exception, they were kind, interested persons, who took time out of their busy schedules to help me. Some of them sent additional information afterwards, or even invited me to events. They were often very passionate about their work, and were keen to share their ideas and knowledge with me. However, while I was very grateful for their help, I did not always share their enthusiasm. While I recognise that they are often working on this technology because they feel that this will benefit society, I am critical of some parts of the technology, and question whether it might bring about equally positive changes for everyone. The question then becomes: how to be critical of people who have so generously helped me conduct this research? Perhaps this is one of the issues that comes with 'studying up' (Nader, 2018), as I followed the people who are on the side of power, rather than the people who might suffer unintended consequences. MacKenzie (2005: 570) writes about this dilemma, pointing out that giving an interview is an 'act of hospitality', and as such, it becomes uneasy to 'condemn' the interviewee's views and insights. In this dissertation, I have tried to approach this by being mindful of this issue while writing my dissertation. I have done my best to represent my interviewees' views in a genuine and constructive way, while also reserving space to remain critical of the potential of the technology and the views underpinning it.

A second issue concerned the occasionally fuzzy boundary between being an observer and being a participant. During some of the events I attended, I was expected to participate to some extent. For example, I was once invited to the 'women's breakfast', which was organised in recognition of the fact that there is only a very small number of women in this sector. At this breakfast, there were 11 women, out of over 150 attendees. As such, it was almost impossible for me not to participate, making myself part of a group of women that were working on these issues. Similarly, as some events were more interactive, I was sometimes asked for my opinion. I have tried to take the role of observer as much as possible; during most events, I listened and observed. In situations where this was not possible, I was open about my position as a researcher and presented ideas and arguments in line with my research.

3.9. Conclusion

To analyse technology that is still under development, I used a combination of interviews, attending industry events and documentary research. This allowed me to 'scavenge' (Seaver, 2017) the data needed to analyse SSI and the EUDI Wallet. Applying a flexible, iterative approach allowed me to collect new data when it became available, and made it possible to study this technology while it is in the implementing phase. These methods allowed me to get

close to the technology, and connect the technicalities to the larger issues (MacKenzie and Spinardi, 1988): it made it possible to analyse how SSI is translated to the context of states, how the design of the technology shapes citizenship, and how the creation of the technological design is related to changing power structures. Taken together, these research questions shed light on the radically changing the nature of state-sanctioned identification.

Chapter 4. Making the wallet 'fit' (for purpose): from internet identity model to state-issued identification system

'Digital ID wallets will happen, and if the EU is doing it, everyone will do it'
(Panellist, Identity Fair, UK, November 2022).

4.1. Introduction

Self-sovereign identity technology was originally developed as an 'identity layer for the internet', where it was supposed to give internet users a consistent identity across different websites (Preukschat and Reed, 2021: 3). In an interesting twist, however, state actors became interested in using this technology as the basis for new digital identification systems. And so it happened that 'super state' the EU (Glyn, 2050) is developing the foremost implementation of a technology that has roots in libertarian and anarchist thinking. In this chapter, I introduce SSI technology and the European Digital Identity Wallet, showing how they are socially shaped (MacKenzie and Wajcman, 1999). I argue that SSI's main sociotechnical imaginary (Jasanoff and Kim, 2015) revolves around 'control' - where users are put in charge of their personal data – is being adopted by the EU through the European Digital Identity Wallet, thereby applying an imaginary that was invented for users on the internet, to citizens in EU member states. However, as I will show, SSI's sociotechnical imaginary is intimately tied to its technological architecture, while the same technological elements cannot always be implemented in the context of states. As such, friction arises in this 'translation' across contexts. As I will show, this also leads some SSI experts to argue that the EUDI Wallet is not 'pure' SSI, or to question whether the wallet can be considered to be SSI at all. I argue that this friction goes to the heart of the tension around 'control': while states can shift some degree of control to citizens, they also simultaneously need to retain some 'control', to identify citizens – a classic function of identification (Lyon, 2007). Paradoxically, however, in adopting certain elements of SSI technology, credentials in particular, other actors necessarily need to be involved. As such, I will argue that an assemblage of corporate, internet and state actors is involved in identification processes. The credentialisation of identification, therefore, brings about a new role for (EU member) states[4], where they are in a paradoxical position between giving away and trying to retain control, as the EUDI Wallet broadens the scope of identification.

The first part of this chapter interrogates SSI's sociotechnical imaginary, which revolves around giving 'control' to individuals, and shows how this imaginary is fundamentally reliant on its technological architecture. I look at this through three important concepts in this technological arrangement: identity, decentralisation, and trust. The second part explores the

[4] While the EUDI Wallet is developed and implemented at the EU level, EU member states will remain in charge of issuing foundational identity credentials, the digital equivalent of identity documents. I will address this tension more extensively in chapter 5.

European Digital Identity Wallet, showing its aims and functionalities, while placing it in a larger political context. Here, I argue that the credentialisation of identification leads to the involvement of shifting assemblages of actors in identification. The third part looks at the translation of SSI principles to the EUDI Wallet. Building on interviews with experts, it explores whether the ideological foundations of the technology can be united with a state-issued identification system. I return to identity, decentralisation, and trust to show how these concepts can or cannot be translated to the context of states.

4.2. Imagining self-sovereign identity

Sociotechnical imaginaries refer to normative views that describe a desirable future, which is to be brought about by technology. To recapitulate, Jasanoff and Kim (2015: 4) define sociotechnical imaginaries as:

> 'collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology.'

The concept is helpful, as it 'serves as a lens through which the interplay and mutual shaping of science, technology, and society can be identified and analyzed' (Mager and Katzenbach, 2021: 225). Therefore, it is a useful tool to look at the ways in which technologies (are meant to) change societies. While they initially attributed the creation of sociotechnical imaginaries to nation-states, Jasanoff and Kim (2009; 2015: 4) later redefined the concept, pointing out that sociotechnical imaginaries can be formulated by different groups, such as corporations or social movements, as well. As I will show, SSI technology was first only tied to a sociotechnical imaginary that pertained to the internet, and was defined by a group of technologists. However, it has come to be part of the sociotechnical imaginary of the EU, and, as such, part of a larger vision on control over data and technological sovereignty narratives. In other words, while it did not start out as a state-led imaginary, it has become part of one.

As Semenzin (2020: 71), building on Bory (2020) remarks, 'sociotechnical imaginaries are often characterised by a conceptual shift from a technical object to an ideological reference that may suggest certain models for the organization of societies.' Often referred to as a 'paradigm shift', SSI aims to change the organisation of society, for it is supposed to radically subvert power structures. Surrounded by the hype and optimism that often comes with technological development (see e.g. Morozov, 2013; Danaher, 2022), SSI is hailed as a radical new solution. For example, developers Preukschat and Reed (2021: 3) state that '[t]he SSI paradigm shift is deeper than just a technology shift – it is a shift in the underlying infrastructure and power dynamics of the internet itself.' As such, they feel that in terms of significance, it is comparable to other infrastructural paradigm shifts, like 'the shift from horse travel to train travel' (Preukschat and Reed, 2021: 3). Therefore, similar to other cryptography-based technologies, SSI has an ideological component; it should be seen as normative technology as it carries ideas about the future, and how to make the future world a better

place. As I described in the introductory chapter, the concept of SSI is related to ideas about freedom and autonomy: individuals should be able to make their own choices; be self-sovereign (see e.g. Cheesman, 2021).

I argue that SSI's sociotechnical imaginary revolves around 'control': it promises to put individuals in control of their personal data and identity, so that they can decide when to share their personal data (which is stored in the format of credentials) and with whom. As Ishmaev (2016: 246) succinctly defines SSI:

> 'the concept of individual control over identity relevant private data, capacity to choose where such data is stored, and the ability to provide it to those who need to validate it, without relying on any centralised repositories of identity data.'

It therefore presents a very individualised conception of sovereignty, while it is also linked to some of the big digital issues of these times, which revolve around data exploitation and surveillance (e.g. Zuboff, 2019; Meijas and Couldry). SSI technology is thus supposed to interject, by taking away power from large entities – such as large platforms that have become monopolies in their own right (see e.g. Srnicek, 2016; Sadowski, 2020) – and give it to individuals. As such, it is inextricably linked to concerns around privacy. It is important to point out, however, that 'control' is not a neutral term; it is mobilised to justify this technological development. Therefore, it is important to question the assumptions underlying this technology. As I will show, 'control' is bound up with its technological design: giving this control to individuals will be possible because of the way in which the technology is built. For this reason, I decided to look at this sociotechnical imaginary through three key components: identity, decentralisation, and trust.

4.2.1. Identity

The concept of 'identity' is a constitutive part of self-sovereign identity. Yet, what is exactly meant by it is not clearly defined. Social scientists have long debated what 'identity' entails. As Brubaker and Cooper (2000: 1) remark, for example, 'identity […] tends to mean too much (when understood in a strong sense), too little (when understood in a weak sense), or nothing at all (because of its sheer ambiguity).' To understand what 'identity' means in the context of SSI, it should be seen in the context of the internet.

As I mentioned, a small internet community has been working on an 'identity layer' for the internet since the early 2000s (Infominer and Young, 2021). This concept was first coined by Kim Cameron (2005), then chief architect for identity at Microsoft, who published the 'Laws of identity.' This was one of the main pushes for what later would become known as SSI. While the community kept working on these concepts during workshops and conferences, the next big step in the evolution of SSI was Christopher Allen's (2016) blogpost, 'The Path to Self-Sovereign Identity.' In this post he outlines both the evolution of digital identity models, as well as the ten principles that self-sovereign identity would need to adhere to, and which I will discuss below. He conceptualises SSI as an expression of digital sovereignty and became,

because of that, an important factor in the popularisation of the term 'self-sovereignty' (Giannopoulou and Wang, 2021; Ishmaev, 2021). In order to understand what SSI is supposed to change, it is helpful to look at Allen's (2016) description of the evolution of identity on the internet - with SSI being the proposed end stadium.

Phase one: centralised identity

In the early days of the internet, centralised authorities both issued and authenticated digital identities online. Allen (2016: n.p.) compares the kind of control that these authorities have to that of state authorities in the 'physical world': 'users are locked in to a single authority who can deny their identity or even confirm a false identity. Centralization innately gives power to the centralized entities, not to the users.'

Phase two: federated identity

Around the beginning of the 21st century, the federated identity model was introduced. This enabled users to use the same identity for multiple websites. This is an identity model that is still used today. For example, using a Facebook, Google, or X (Twitter) account to access different online services is still something that is part of everyday internet use. As I briefly described in the introduction, this has brought on questions around power, as it has given platforms access to a wealth of user data.

Phase three: user-centric identity

User-centric identity is an idea that was never fully implemented to the same extent as the previous two models. The concept came about in response to the centralised systems where users had little control, and focused on 'put[ting] users front and center in the quest for online identity' (Allen, 2016: n.p.). Later, this also came to include the idea that users should have complete control over their digital identity, though this never fully came to fruition. As Allen (2016: n.p.) summarises it, user-centric identity 'turned centralized identities into interoperable federated identities with centralized control, while also respecting some level of user consent about how to share an identity (and with whom).'

Phase four: self-sovereign identity

However, importantly, according to Allen (2016, n.p.) user-centric identity does not include what has become the core principle of self-sovereign identity: users 'being the rulers' over their digital identity. While there is no consensus within the community on the exact definition of self-sovereign identity, Allen (2016) has developed ten principles, which are generally accepted:

1. Existence. Users must have an existence separate from their digital identity, as the digital version can only translate certain aspects of their 'real' identity.
2. Control. The user is the 'ultimate authority on their identity' (Allen, 2016: n.p.) and should be able to control it.

3. Access. The user should always have access to their data.
4. Transparency. The systems and algorithms that are used should be transparent: anyone who wants to, should be able to look at how they work.
5. Persistence. Identities should preferably be permanent or be there for as long as the user wants.
6. Portability. Information about identities should be transportable; it should not be held by one single party.
7. Interoperability. Identities should be reusable, across as many services as possible.
8. Consent. The user must always consent to the use of their identity and information related to it.
9. Minimisation. When data is disclosed, the minimum amount of data that is needed should be disclosed.
10. Protection. The user's rights should be protected – the rights and freedoms of the user are more important than the needs of the network.

Allen (2016) emphasised that SSI sets itself apart from centralised and federated systems through its emphasis on the individual, and the decoupling of identity from existing systems, putting the user fully in control. In other words, the concept of self-sovereign identity is deeply concerned with the power that the issuers of identities have, as they are able to, for example, deny access, track people across websites, or revoke an identity (account) altogether. As such, SSI is fundamentally concerned with changing the power hierarchies of the internet. This is also explained to me by Sophie, one of the founders of SSI technology, who tells me in an interview:

> 'On an architectural level, in the architectures that people have built up till very recently, people fundamentally were not the actual actors who control the digital thing that represented them in the digital world.'

She continues to explain:

> 'The way identity was done on a computer comes from a very particular time and place […] And so when AOL showed up, you got a handle inside the AOL namespace; when Twitter showed up, you got a handle inside the Twitter namespace; when Facebook showed up you got a handle...Oh, that inside part means they can kill you anytime. And last time I checked, we have a whole bunch of human rights, and, you know, a justice system that if somebody harms my physical body, then they're held accountable. If they kill me, they're really held accountable, eventually, you know. That's not true in the digital world. In fact, it's the opposite: […] if Facebook decides tomorrow it was going out of business, it would have the legal right to kill everybody's account.'

This shows how serious a matter this is for members of the SSI community - the dissolution of digital accounts is here described as a kind of digital murder. This community places importance on being independent ('sovereign') from those structures: if we are in charge of

our own digital identity, it is not possible for Twitter or Facebook to 'kill' our accounts. Therefore, 'identity' goes to the heart of SSI's sociotechnical imaginary of control: this imbalance of power should be rectified, and SSI technology is supposed to make this possible. As Sophie explains:

> 'What we're shifting with the technology […] [is] on an architectural level. There's a different paradigm that doesn't mean I'm being assigned identifiers from other people, and that I'm only existing because of their largesse of letting me have an account.'

In other words, what is supposed to shift is the 'locus of control' (Bouma, 2019, n.p.). As Bouma (2019: n.p.) writes in a blogpost: '[s]imply put, [in] the old (centralized and federated models) the locus of control was between the other parties that could make decisions about me, whether I was in the picture or not. In the new model (self-sovereign identity), the user is put into the centre of his/her own locus of control.' Or, as another prominent SSI figure, Joe Andrieu (2016: 2) writes, the answer to what being self-sovereign means lies in the permission: '[s]elf-sovereign identity means not having to ask permission to create, provide, or terminate the use of identifying information for correlation across contexts.'

This is where identity links to the process of credentialisation. Verifiable credentials[5] will be issued by entities that have the authority to say that we have a certain identity or are entitled to something. For example, a state can issue a digital version of a passport, which can 'prove' someone's nationality. Similarly, an airline can issue tickets or loyalty cards, which entitle the holder to a seat on a plane and frequent flyer points in their account. According to SSI expert Phil Windley (2021: 7), credentials are a solution to the centralised system where identity information can only be used in a specific context, which has been the case on the internet up until now. Credentials are not 'fixed'; they are issued by different entities and can be used in different contexts:

[5] **Verifiable Credentials** (VC; credential for short) contain information (claims) about a subject, also called 'the holder' of this credential. This information can consist of, for example, attributes (like height or age), relationships (like citizenship or parent), or entitlements (like rights or membership rewards) (Reed, Joosten and Van Deventer, 2021). The claims are made by the authority issuing the credential (for example a government), which is called 'the issuer'. In addition to the holder and the issuer, there is 'the verifier': this is the entity (which can, for example, be a government, an organisation, or a person) that wants to establish that the credential is real and trustworthy. Credentials are verified through cryptography and the internet (Reed, Joosten and Van Deventer, 2021). This means that the credential can be verified with the issuer without 'phoning home', which means that the issuer is not notified that their credential is being used for something (Young, 2022). The relationship between the issuer, holder, and verifier, is the called the 'trust triangle'. According to SSI community members Reed, Joosten and Van Deventer (2021: 25) the trust triangle got its name because 'it is fundamentally how human trust relationships are conveyed over a digital network.'

> '[t]here is no central authority for all credentials. Every party can be an issuer, a holder (identity owner), or a verifier. Verifiable credentials can be adapted to any country, any industry, any community, or any set of trust relationships' (Windley, 2021: 7)

This means that credentials signify a departure from the situation where, for example, as Sophie described above, a Facebook handle can only be used within the Facebook space. In other words, the idea is that credentials can be used in various contexts, and for different purposes. What is more, anything could be a credential, so long as it allows to 'verify' an identity or entitlements (Reed, Joosten and Van Deventer, 2021). This, I argue, also signifies a change in identification processes, particularly because this system will also be used beyond the context of the internet in which it was developed. What is more, I argue throughout this dissertation that credentialisation changes identification: different and previously separate parts of people's lives are 'credentialised' and brought together in one wallet, where the credentials can be used across contexts.

Importantly, while the word 'credential' can be used to refer to identity documents (Smith, Loddo and Lorini, 2020), this is not how it is commonly used in the academic literature. In the sociological literature, credentials have mainly been discussed in the context of higher education and employment opportunities (see e.g. Collins, 2019; Tomlinson, 2008; Wheelahan and Moodie, 2022). Here, credentials, most importantly academic degrees, but increasingly also 'micro-credentials' such as specific short training courses, are linked to skills and status, with graduates competing over job opportunities (Wheelahan and Moodie, 2022). As such, these types of credentials are linked to social stratification, competition, and differentiated life chances (Tomlinson, 2008). In contrast, 'credentials' that can be stored in digital ID wallets could contain any kind of information that allows to 'verify' their identity or entitlements (Reed, Joosten and Van Deventer, 2021). What is more, these credentials are linked to the sociotechnical imaginary of 'control': while individuals will not issue their own credentials, they will have 'control' over them in the sense that when a service asks for personal data, they can decide how much they want to share. Therefore, these new 'verifiable' credentials are linked to access, control and verifiability, rather than skills and employment opportunities. In other words, this signifies a shift in the social meaning of credentials.

In this version of credentials, 'verifiability' plays and important role. What is exactly being verified, depends on the situation. Depending on what is needed, this could be, for example, age, name, or membership to an organisation. This could be similar to what is already possible, such as verifying that a person is over eighteen when they try to buy alcohol in a shop. However, an interesting example in this regard is that the EUDI Wallet will make it possible to use one's ID credential to authenticate for Very Large Online Platforms, such as Facebook or Amazon (European Commission, 2023), thus using this credential in a new context. This illustrates what I mentioned above; it will no longer be necessary to use, for example, a Facebook handle that can only be used on this website; an ID credential can be used instead. Because individuals will be able to store a wide array of credentials in their wallet, it will

essentially provide an aggregated digital identity, which consists of different credentials, representing different aspects of people's lives.

In short, 'identity' in the context of SSI is intimately linked to credentials, which function as 'proof' that someone really is who they claim to be. At the same time, individuals are promised 'control' over these credentials, as they can decide when to share them. Paradoxically, therefore, while SSI rejects centralised control, and aims to put individuals in charge, it also contributes to making it possible to 'verify' people with a very high degree of precision. What is more, while credentials are often used in the context of education and employment (Collins, 2019; Thomlinson, 2008) to 'prove' that a person has particular skills and qualifications, digital verifiable credentials could be 'anything' (Tobin, 2024) and 'verify' different attributes such as age, any kind of membership or even health records, and use these credentials across contexts. Therefore, credentialisation brings about aggregated digital identities, consisting of different credentials that represent different parts of people's lives and makes it possible to verify them.

4.2.2. Decentralisation

> *At the Identity Fair, digital identity was not seen as a stand-alone technology. Rather, it was imagined as an important part of the decentralised future society. In this society, digital identity is at the centre of an infrastructure that connects individuals to all kinds of services, both public and private. In this decentralised world, the individual will choose when and with whom they share their personal data, and they can do so with just a tap on their smartphone. SSI (sometimes also called 'decentralised identity') often came up as the solution that will revolutionise the digital landscape. The boldest dreamers saw a world where people would have a seamless digital identity that could be used around the globe, the more moderate thinkers envisioned decentralised identity as a way to mitigate some of the existing dangers related to identification. What everyone seemed to agree on, however, was that decentralised identity is an empowering tool, that could be 'leveraged' to put people 'back in control of their data.'* (Identity Fair, UK, November 2022).

This short vignette describes how SSI is often seen as more than an identity model; according to enthusiasts, it could be the missing piece to a decentralised society. In this society, digital ID wallets make it possible to connect individuals to all kinds of services, at varying levels, with global interoperability being the ultimate goal. Decentralisation is an important component of SSI's sociotechnical imaginary of 'control,' because this makes the shift of power that is envisioned practically possible: in a decentralised network, there is no central authority that is connected to every entity (node) that is part of the network (Baran, 1964), and can therefore have access to all data. Rather, data is usually stored locally, for example on personal devices such as phones (Naik and Jenkins, 2020). As Nyst et al. (2016: 98) put it: '[t]he alternative to a centralised hub is a decentralised hub, where each citizen has their own personal hub running

locally on their own device, brokering the identity transactions such that the only party that can track the citizen is the citizen themselves.' Decentralisation is thus inextricably connected to conceptions of power: it is the opposite of 'centralised' power, where one entity (such as Amazon, or a state) has control over the entire system. Or, as cryptography expert Dave Huseby (2020: n.p.) writes: '[d]ecentralization is the direction in which user sovereignty increases.' In other words, the idea is that the more decentralised the system is, the more 'control' will go to the individual. Therefore, it is directly linked to the imaginary of 'control', as the technology is supposed to encode a different power relationship.

Credentials are an important part of this, as they contain the very information that will be stored locally. In practice, this means that individuals will be able to directly present their credentials to a service provider – as the credentials are decentralised and thus stored on their phone. To present credentials, however, another decentralised part of the technology is needed: so-called 'decentralised identifiers' (DIDs)[6]. Simply put, these are addresses that are needed for a transaction. As Christoph, an SSI expert who is specialised in DIDs, explains to me in an interview:

> 'DIDs are just identifiers, right? So DIDs don't really have associated first name or last name, or date of birth. So it's just a new type of address for the Internet, right, a way, how we can refer to individuals and organizations and things. It's just a way to name things, to address things a little bit, maybe like an IP address, or an or an email address. But of course, with the very special property of being decentralised, right? So most of the most of the identifiers that we use today are dependent on some kind of central authority or hierarchy, and they're not self-sovereign. They can be taken away from us.'

This ties in with the imaginary of control that I discussed above: as Christoph points out, is that no one 'owns' their DID: they cannot be taken away. In other words, decentralisation is inextricably connected to 'control', as the decentralised nature of the network makes it possible for there not to be one central entity in charge. When I ask him what we need the DID for, Christoph continues to explain:

> 'Yes, you need it...to find each other, to connect, to initiate some kind of transactions of, for example, if you and I meet either online or in in person, and I want to know, I want to know are you really a student, right? Are you really a PhD candidate in sociology, right?

[6] **Decentralised Identifiers** (DIDs) are 'the cryptographic counterpart to verifiable credentials' (Reed and Sabadello, 2022: 157), and one of the elements that has recently been standardised by the World Wide Web Consortium (WC3, 2022). In essence, they are like an address; they are not dissimilar to an URL (the address of a webpage): it is a sequence of characters that identifies an entity (for example, a person or an object) (Reed and Sabadello, 2022). This address can then be linked to a so-called 'DID document', which is a 'machine-readable document designed to be consumed by digital identity applications or services such as digital wallets, agents, or encrypted data stores' (Reed and Sabadello, 2022: 161). The document contains metadata about the DID subject. If that is a person, that is usually cryptographic key, authentication methods and metadata describing how to enter in 'trusted interaction' with this person (Reed and Sabadello, 2022). The key point is that the person controlling the DID can, through these mechanisms, prove their control over it without having to request permission from other parties (Sporny et al, 2022).

> Can you prove that to me? And maybe you have a verifiable credential from the university that you can show to me. But in order to show that to me you need a DID, and I need a DID so that we can start this transaction, so that I can ask you for a credential, you can show it to me, and the university also has a DID, because the university issued the credential to you. So the DIDs are the underlying addressing mechanism to just make all the all the protocols and all the communication work.'

These quotes show again the concern with verifiability on the one hand (am I really who I claim to be: a PhD candidate in sociology?), and control and distrust of intermediaries on the other: the DID belongs to an individual, and no one else can control it. In other words, because DIDs are decentralised, there is no central authority that is connected to all these addresses. As such, they tie in with the sociotechnical imaginary of control, that is inherently linked to the decentralised properties of the technology.

As Bodó et al. (2021) point out, decentralised and distributed systems have often been discussed in relation to power struggles, as proponents are usually concerned with abuse of economic and political power. However, they argue, these views are often overly optimistic, for even if a technology starts off with such a design 'power can accumulate both in technical and social dimensions', and 'beyond a certain scale, power tends to accumulate in the hands of those who have enough reputation, social capital, time, and other resources to participate in the governance process' (Bodó et al., 2021: 9). Similarly, others have pointed out that there are often competing logics at play in the narratives around decentralised technologies, resulting in different practices, with some technologies remaining thought experiments (Cheesman, 2022; Sadowski and Beegle, 2023). Therefore, it is important to look at decentralised technologies in conjunction with their actual implementation, for there are factors beyond the technological design that can influence the actual distribution of power. I will address this more extensively in the third part of this chapter.

Other decentralised technologies, such as blockchain and Bitcoin, carry similar ideas around the subversion of power. In fact, to bring this decentralised future about, SSI could be built on a blockchain (Bai et al, 2022; Tobin and Reed, 2016). A few years ago, the SSI community saw blockchain as a good potential infrastructure for creating the identity layer of the internet, because of its ability to distribute the control from a central provider to all the participants in the system (Cucko and Turkanovic, 2021). As such, blockchains could serve as registries for DIDs (Hardman, 2021)[7]. However, as Giannoupoulou and Wang (2021: 3), point

[7] **Verifiable data registries**. The DID needs to be registered somewhere, in a database. This is where a blockchain could be used. The blockchain is considered to be trustworthy, because it is essentially a decentralised database, which cannot be controlled by a one single party (Reed, Joosten and Van Deventer, 2022). This means, that 'a blockchain can provide an authoritative source of data that many different peers can trust without any single peer being in control' (Reed, Joosten, and Van Deventer, 2022: 33). However, while blockchain is often mentioned as a core part of SSI (Grech et al., 2021; Naik and Jenkins, 2020) it is not necessary, as SSI could be built on other kinds of decentralised ledgers as well (Reed, Joosten and Van Deventer, 2021).

out, SSI 'is blockchain adjacent, not blockchain dependent', as the technology could also rely on other types of distributed ledgers. This independence from blockchain has since become more pronounced; since its first rise to popularity, blockchain has attracted more scepticism, both in the digital identity community and outside of it. The SSI community has moved on from blockchain, to the point that several of my interviewees made a point of telling me that SSI does not need blockchain. When I asked why they felt this was important to share this with me, Marta, who works for a large tech consultancy, replied, a bit hesitantly, 'well, there can be some resistance in the market sometimes.' Similarly, at the industry events that I attended, speakers denounced the blockchain. As one presenter put it: 'Blockchain being a hype stopped the growth [of SSI]'. 'This is because', he continued, 'people think that blockchain is Bitcoin is criminals.'[8]

In other words, there needs to be a hype for the technology to be picked up, but it needs to be the right kind of hype – and the hype cycle moves fast. As one attendee put it, reflecting on the conference: 'a few years ago, everything was about blockchain, but now no one talks about blockchain anymore.'[9] Blockchain no longer has the positive connotations of revolutionary technology that would change the future that it once had (see e.g. Golumbia, 2018; Faustino et al., 2021), but has rather become a hindrance for the uptake of SSI. As such, SSI proponents are put in a difficult position, where the technology they develop bears significant ideological similarity to blockchain, but should not be associated with it, as the hype is over. Therefore, this shows that technology is not immune from social connotations and narratives. Developers may therefore make the decision not to include blockchain, despite it being a good option, thereby shaping the technology in line with current social perceptions.

4.2.3. Trust

When I walked around and listened to presentations at industry events, the term 'trust' popped up everywhere. Questions like 'how can we establish trust?' or 'how do we generate scalable trust?' were asked and answered many times. Trust seems an inherently human and social topic; it could say something about the relationship between people, between groups in society or between citizens and their government, for instance. Sociologists who have looked at trust, often define it in relation to the future. As Sztompka (1999: 25) points out: '[t]rusting becomes the crucial strategy for dealing with an uncertain and uncontrollable future'. Similarly, according to Luhmann (1979: 10) '[t]o show trust is to anticipate the future. It is to behave as though the future were certain.'

In technical circles, however, trust or 'digital trust', is defined differently (Becker and Bodó, 2021). Similar to decentralisation, the debate around trust has featured prominently in the realm of cryptocurrencies and blockchain. For example, Nakomoto (2008: 1), the inventor of Bitcoin, famously stated that '[w]hat is needed is an electronic payment system based on cryptographic proof instead of trust.' A key point here is that the use of cryptography removes

[8] Identity Fair, UK, November 2022.
[9] Identity & Technology Forum, Germany, May 2023.

the need for any 'intermediaries' such as banks (who, according to Bitcoin 'believers' cannot be trusted (Golumbia, 2018)) to facilitate a transaction (Woodall and Ringel, 2020). As De Filippi et al. (2020: 1) explain, 'users subject themselves to the authority of a technological system that they are confident is immutable, rather than to the authority of centralized institutions which are deemed untrustworthy.' This has given rise to a discourse of 'trust in code' and 'trustless trust.' In an interview, Jack, an SSI consultant, explains 'trustless trust' in relation to blockchain:

> 'They're trustless, because you don't need to trust them. You don't need to trust them, because they prove with a consensus algorithm approach that at each moment in time, they've done the right thing by the consensus algorithm […] They put a mechanism by which they can be resilient to certain types of attack. Hence trustless, because I don't need to trust it, because it mathematically can be proved that it does this thing within certain sort of ranges of possible events.'

A similar idea of trust is discussed in the world of SSI. This particularly revolves around the question of how to be sure that we can 'trust' that a credential is real and legitimate, and, because of that, it is possible to verify that someone is who they claim to be. As Luke, a developer who has worked in the blockchain and SSI space, mentions in an interview:

> 'Before, whether you would use a service could be through a person…you would go for somebody you would trust, or they would be referred to you by someone else, which you trust. If I trust you, and you send me to this doctor, for example, […] then I'm also trusting this doctor, because I know that you trust the doctor. But now, for example, when you access services, you don't need to do know the person in order to trust [them], right, you can trust by verifying. So, you can do business with one another without...necessarily knowing the other party.'

In other words, because it can be cryptographically verified whether a person is who they claim to be, trusting other people is no longer necessary. Credentialisation plays an important role in this, because credentials make it possible to 'verify' whether a person is who they claim to be or whether they are entitled to something. As such, trust is not really about trust, it is more about risk management; it is about trying to determine with as high a degree of confidence as possible that something is 'real' or 'true'. Therefore, 'verifiability' is constructed: someone is 'verifiable' when they are able to present the right information in the right format (a credential), and it can be cryptographically determined that this information was issued by a particular institution. Seeing this in light of the history of identification, credentialisation can therefore be seen as a new way to 'fix' identities – before credentials this was primarily done through biometrics (see e.g. Martin and Whitley, 2013; Ajana, 2012; Amoore, 2006) - where it is assumed that credentials give access to an objective, verifiable truth. Paradoxically, therefore, the focus on trust in fact conveys a fundamental distrust; a distrust of people (as they may not be who they say they are, so that needs to be verified) as well as a distrust of

institutions (as the technology is based around the want to remove 'intermediaries' from transactions). In this sense, constructing 'verifiability' means putting trust in standardising information in a certain way so that it can be verified. Importantly, as digital identification researchers have pointed out, standardisation and categorisation of information is not neutral; but rather it enacts identities in a particular way (see e.g. Pelizza, 2019; 2021). This reveals the power dynamics that come into play with identification, because the entity (e.g. a state) that is asking for and categorising the information determines someone's identity. This can have significant impacts, as some information is not considered to be relevant, which sometimes means that crucial parts of people's layered, social identities are not included (see e.g. Franke, 2020; Pelizza, 2021; Leese, 2022).

Ultimately, verifiability reveals a concern with 'knowing', as trust is contingent on 'proof'. Importantly, while datafication has also been characterised as a new way of 'knowing', as everything we do turns into data (Cukier and Schönberger, 2013), credentialisation is different in the sense that credentials contain very precise and 'high quality' data. Peter, who works for a public/private organisation that is researching SSI, tells me in an interview that credentials make it possible to 'verify' with much more certainty. He points out that it is no longer necessary to store a lot of (imprecise) personal data, when one can rely on verifiable credentials instead. As he puts it: 'it is all about adding trust to the data.' The type of data stored in credentials is more 'valuable' than big data harvested online, because 'trust' has been added to it. Describing the 'current thinking' about data, he remarks:

> 'They all learnt this at Singularity University in Silicon Valley[10]: growth is exponential, and data is the new oil that you need to harvest – this is the business model. So we have to break this cycle – that data is crude oil (and we need to stop using oil anyway [laughs]) – but also: crude oil has no value; it only gains more value the moment that trust is added to this data.'

Using the famous oil metaphor, he points out that there are different kinds of data, where some are more valuable than others: 'Crude oil is not as valuable as refined oil, petrol and other products; the same way that raw data is not as valuable as data that has trust added to it.' What this means, is that the data that is stored in credentials, is perceived to be of higher value than data that is harvested online, for example to profile people. As such, while they only contain a limited amount of data, credentials are much more valuable, because this data can be verified, and therefore *trusted*. Therefore, I argue that credentialisation is not only about turning personal information into machine-readable credentials: it is also about making sure

[10] Singularity University is a corporation that offers training programmes focused on achieving impact through technology, and is, as Boenig-Lipsin and Hurlbut (2016: 239) put it 'grounded in a faith in the inevitability of radical, technology-driven social transformation.' The term 'singularity' is closely related to transhumanism and the idea that technology offers limitless opportunity and removes all (human) constraints (Boenig-Lipsin and Hurlbut, 2016).

that this information is 'high quality', as it can be verified. This has implications for the value of this data, which I will address in the next chapter.

In regard to other decentralised technologies, Vidan and Ledonvirta (2018) have pointed out that the discourse on 'trust' conceals that there always are individuals managing the system, who need to be implicitly trusted. Similarly, problems with trust arise if humans have no way to intervene. Bruce Schneier (2019: n.p.), a well-known figure in the world of web security, has argued in a *Wired* article that has become cited in the field, that what blockchain does 'is shift some of the trust in people and institutions, to trust in technology.' However, he continues, '[w]hen that trust turns out to be misplaced, there is no recourse' (Schneier, 2019: n.p.). In other words, if the technology fails, there are no human audit systems or interventions possible. Therefore, it is, in reality, hard to 'trust' technology. As such, there will continue to be a need for human governance over the system, Schneier (2019) argues.

This tension between technology and human 'trust' has also become a key debate in the SSI world: there has been a realisation that only cryptographic trust is not enough for this system to function in society; there need to be rules around this, detailing, for example, which parties get to be accepted into the 'ecosystem' (Johnson Jeyakumar et al., 2022), or more generally, rules and policies that all the parties involved in the system have to follow (Trust over IP Foundation, 2021: 19). Emblematic of this shift is the move from a 'trust triangle' to a 'trust diamond.' The trust triangle visualises the idea that the party that is verifying a credential, for example a future employer, can 'trust' that the credential, such as a degree certificate, is real. The main point here is that the verifier (the future employer) does not need to 'trust' the issuer (the university issuing the degree), because they can rely on the cryptographic process. As such, the employer does not need to 'phone home' – as it is called in SSI jargon - to the university to make sure that the credential is real (Trust over IP Foundation, 2021: 24).

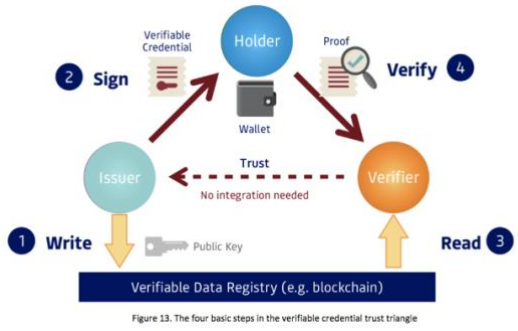


Figure 13. The four basic steps in the verifiable credential trust triangle

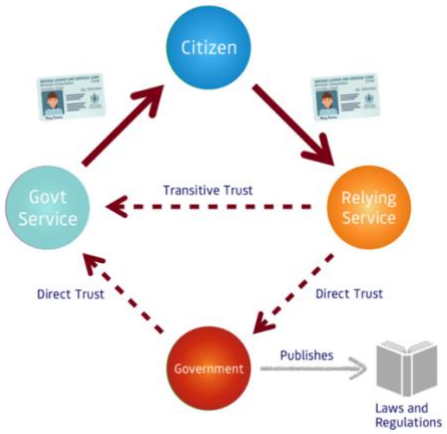


Figure 11. The governance trust diamond for government-issued credentials

Source: Trust over IP Foundation (2021: 20-23)

However, if SSI is going to be implemented in society, it becomes necessary to have rules about the technical system. In other words, there needs to be a governance framework (also called

a 'trust framework')[11] that determines what participants in the system can and cannot do (Trust over IP Foundation, 2021). As prominent SSI figure Drummond Reed (2021: 248) writes:

> 'Governance is as old as human society. In today's world, it is the job of governments, companies, and any other human organization. But the concept of a governance framework is newer. From the perspective of technology infrastructure, the ISO/IEC 38500 defines governance as "a system by which the current and future use of information technology (IT) is directed and controlled".'

This means that the advanced version of the trust triangle, the trust diamond, now includes an entity that establishes rules for the whole system. Therefore, now that SSI is coming out into the social world, certain rules and regulations need to be established to make the technology work within larger social structures.

In general, however, the concept of 'trust' is seen as a prerequisite for 'control': if the technology, rather than people or institutions can be 'trusted', individuals releasing their credentials can be in control without having to rely on others: cryptographic processes make sure that their credentials are verified. Therefore, in sum, looking at the SSI technology through the key elements of identity, decentralisation and trust, shows how the sociotechnical imaginary of 'control' is tied to the technology's technical architecture. For this, 'trust' is put in the technical workings of the system: the technology will make it possible to 'verify' whether someone's claims are substantiated or not, who can access information because of where it is stored, and to 'trust' technology, rather than people and institutions.

4.3. The European Digital Identity Wallet

> *'With the European Digital Identity Wallet, we are going from theory to reality'* (prominent SSI figure, Identity & Technology Forum, Germany, May 2023).

As Mager and Katzenbach (2021: 231) observe, writing about the concept of sociotechnical imaginaries, '[a]s it appears, the making and governing of digital technology are not two separate spaces and sets of practices […]. Most notably, much of the governing of digital technology seems to be executed in the making of digital technology and its rhetoric.' The European Digital Identity Wallet is a prime example of a technology that is being simultaneously governed and made. As I will argue, SSI's sociotechnical imaginary of 'control' has not stayed in internet circles; is it moving out of the internet sphere, and has found its way

[11] **Governance frameworks** are 'the flip side of VCs' (Reed, Joosten and Van Deventer, 2021: 36), as they detail which procedures must be followed in order to issue a trustworthy credential. They can also specify other policies, for example, relating to the issuance and exchange of credentials. In short, they are the legal, technical and business rules for using SSI (Reed, 2021). The governance framework makes it possible to scale the use of verifiable credentials; this could be in just one sector, but could also be nation-wide (Reed, Joosten and Van Deventer, 2021).

to the heart of state-sanctioned identification practices through the EUDI Wallet. In this section, I will introduce the EUDI Wallet, paying special attention to credentialisation and the new functions of this wallet-based system.

The European Digital Identity Wallet was first proposed by the European Commission in 2021 (Proposal for amending Regulation (EU) No 910/2014, 2021). This new identification system will eventually be an app that allows citizens, residents and businesses to identify themselves across the EU. In line with SSI principles, these groups are promised 'control' over the credentials that they can store in their wallets (European Commission, 2024; n.d.). The EUDI Wallet it is brought into existence through an amendment to existing legislation, the so-called eIDAS (Electronic Identification, Authentication and Trust Services) Regulation ((EU) 2014/83). Therefore, the new legislation is also colloquially known as 'eIDAS 2.0' (McConvey, 2024). It is accompanied by technical specifications for the wallet, the so-called 'Architecture Reference Framework' (ARF) and the eIDAS Toolbox, which are developed by technological experts, the so-called 'eIDAS Expert Group' (European Commission, 2024b). While these specifications are developed at the European level, EU Member States are tasked with 'certifying' wallets, which can be developed by any company or public organisation, so long as they comply with the specifications (De Rosa, 2024). As such, there will technically be more than one wallet. While it is mandatory for Member States to provide their citizens with a (free) wallet, it is not mandatory for citizens to use it. At the time of writing, the legislation has been passed (European Council, 2024), but the wallet is still under development. Currently, the wallet is in the pilot phase, and different use-cases are being tested in 'large-scale pilots' (European Commission, 2023b; 2023c), which I will further detail below.

In many ways, the EUDI Wallet is a continuation of the identification histories that I described in the introduction. It will be an identification system that allows people to 'prove' who they are: for example, a person's identity as a citizen of a particular state. This 'proving' function is similar for analogue and digital identification systems: as Sullivan and Burger (2019: 236) point out, 'uniqueness and exclusivity are […] essential features of digital identity and these features underpin schemes that use digital identity, especially for transactions.' The EUDI Wallet should therefore be seen in light of the classic features of identification, which revolve around proving uniqueness and authenticity, and establishing control over a given population (Caplan and Torpey, 2001; Eyal and Brensinger, 2021).

However, at the same time, there are also important departures from 'classic' state-issued identification documents. The EUDI Wallet uses credentials, a concept that comes from the world of SSI, and will give access to different services. For example, the wallet will be able to store credentials such as social security numbers and medical prescriptions, but also gym membership cards or university degrees (European Commission, 2023d; 2024c). As such, citizens will be able to use the wallet for different functions: they can access government services, claim medical prescriptions, or applying for bank loans all through the same app (European Commission, 2024c). It also includes a payment function (NOBID, 2024), as well as the possibility for eSignatures (Potential, 2024). The EUDI Wallet is more than a traditional

identification system: citizens will not only be able to identify themselves in different countries, but they can also use the wallet for both public and private services, and online and offline ones. This means that different assemblages of actors will be involved in identification processes. It also means that individuals will not only be able to 'prove' their identity as citizen, but can, for example, also 'prove' that they are a graduate of a particular university, or that they are entitled to a bank loan. In other words, as I described in the previous section, credentials are usable across different contexts, serving various functions.

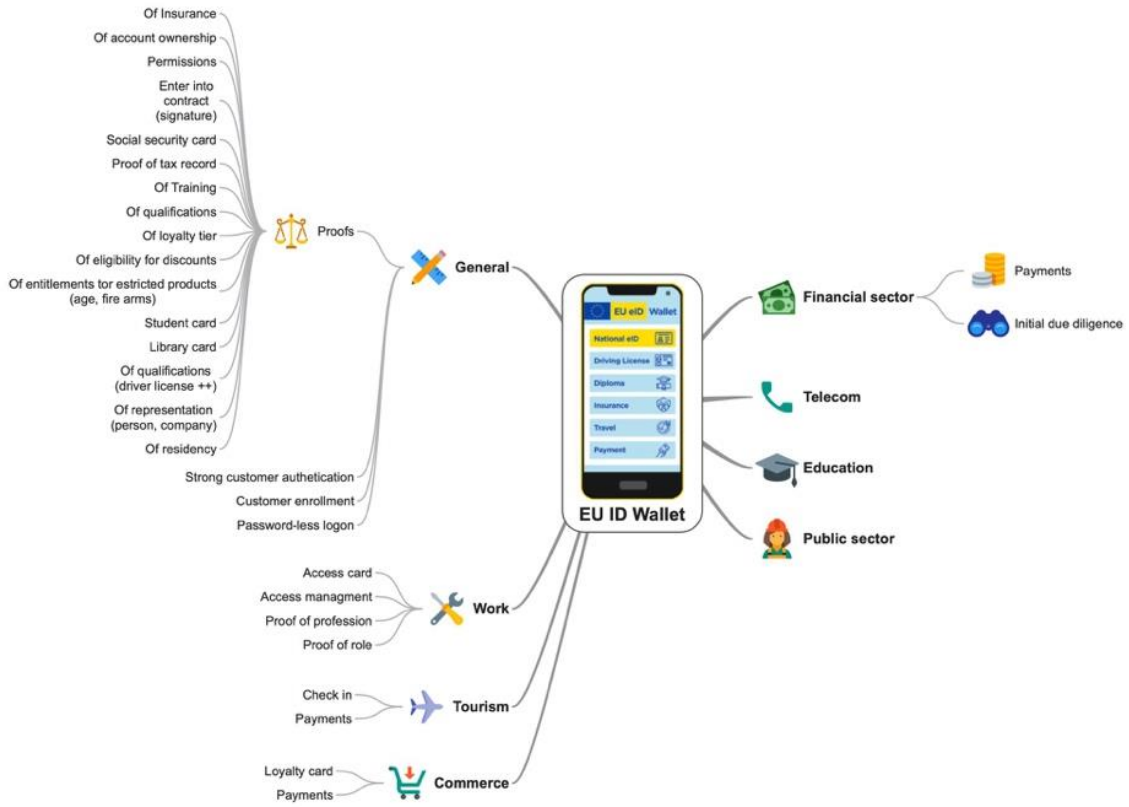
While there have been projects aiming to create identification documents for multi-purpose use before (Sparke, 2004; Lyon, 2007; 2009), the extent to which the EUDI wallet aims to integrate the public and private sector, the 'online' and the 'offline', is unprecedented. As I will argue throughout this dissertation, the process of credentialisation brings together previously separate parts of people's lives and turns them into 'verifiable' information. It is a significant shift, for it changes how identification is 'done' and how people engage with it, as different social institutions and social roles are collapsed into one technical object.

Visualisation of the European Digital Identity Wallet. Source: Cloud Signature Consortium (n.d.)

While it is still unclear what the wallet will look like in its final form, this visualisation gives an impression of what prospective users of the wallet might see. On the left-hand side there are the so-called 'issuers', these are the entities that issue the credentials that can be stored in the wallet. An example of this is a national government, that will issue a 'eID' credential, a digital equivalent of a national ID card. On the screen of the phone some examples of credentials are made visible. The right-hand-side of the visualisation illustrates the process of verifying someone's identity and authorising them to use a service. 'Selective disclosure' refers to the possibility to disclose certain (selected) information (Proposal for amending Regulation (EU) No 910/2014, 2021). For example, when someone needs to prove that they are over eighteen, they can choose to only share their day of birth, rather than all information that may be included on their eID credential (Regulation (EU) 2024/1183, 2024). In addition, users of the wallet will have access to a 'dashboard' where they can see who they have shared their data

with, the option to ask the service to delete the data they received, and report misuse (European Commission 2024d).

The second visualisation (below) provides more detail about the kinds of information that will be credentialised and stored in the EUDI wallet. For example, the 'proofs' on the left-hand include, proof of residency, library cards, and social security cards. The visualisation also shows the different services these 'proofs' can be used for, including public sector services, but also payments. In other words, therefore, it shows that the wallet credentialises different aspects of people's lives.



Functions of the EUDI Wallet. Source: Khan, R., LinkedIn (2024)

4.3.1. New assemblages

As the EUDI Wallet will include many different (public and private sector) credentials and functions, new collaborations between government and industry actors are necessary: new assemblages that are involved in identification processes are emerging. At the Identity Fair[12] that I attended, there was a general excitement about this new course of action. As one presenter remarked: '[g]overnment and industry have not always gotten on – but now their interests are totally aligned.' Similarly, others pointed out that 'the regulators are on our side', and that this new system makes it 'easier for private entities to come and play.'

[12] Identity Fair, UK, November 2022.

As I briefly mentioned above, this wide range of different functions is currently being tested in the so-called 'large-scale pilots', which are led by four consortia consisting of public and private actors from different EU member states (European Commission, 2023b). These pilots are a key example of new assemblages that are arising. Currently, four large scale pilots are in progress. The EU Digital Identity Wallet Consortium (EWC) (2023) looks at travel scenarios, where the wallet can be used for the entire journey, from buying the tickets to showing one's passport at the border. The NOBID consortium focuses on the payment function of the wallet (Røvik, 2023), which, in the future could be extended to include the digital Euro (NOBID Consortium, 2023; Boix Alonso, 2020). The Potential Consortium (2023) trials the cross-border use cases of e-government, e-prescriptions, mobile driving licenses, qualified e-signatures and opening bank accounts. Finally, DC4EU looks at different kinds of credentials, particularly educational and professional ones, as well as social security credentials such as the European Health Insurance Card (DC4EU, 2023).

As I mentioned, all of these consortia consist of different public and private actors from different EU member states. This shows that the credentialisation of identification means that new assemblages of actors need to be involved to make this work. Andreas, one of the members of the Expert Group, explains one of these pilots in an interview:

> '[One] use-case is e-health. And that is one that has quite a big cross-border figures, like e-prescription or a patient summary. If you're young enough that you might not need some drugs permanently, but if you are travelling, and have a prescription that you that you need, and if you have forgotten the drug, that…it would be pretty good to get it abroad. And that is one of the use cases is in…also for the wallet and also patient summary like allergies, or whatsoever, if you need care in another country.'

This example demonstrates the scale of this project, both in terms of functions of the wallet and its literal scale, as it is supposed give access to services across the EU. Another use case is explained to me by Carl, a digital identity expert who co-directs one of the four consortia responsible for the large-scale pilots:

> 'So the idea of the large-scale pilots is to provide certain use cases on the EU digital wallet, for […] a high range or a high amount of users, and the core scope of EU Wallet Consortium is digital travel, so you know, that's why many of the well-known travel companies are involved. Airlines are involved, […] providers, hotels, etc, but also payments. So the core idea is that you identify yourself, maybe also for business travel, that it's clear you…I can in this case […] I'm on business travel, I can get to travel, I can book my flight, I can book my hotel, I can book the train, I have to do a check-in at the airport, board at the airport. I just pay on my on my travel, and I do everything with my EU digital wallet. That's the core idea.'

This shows that EUDI wallet will be more than just a digital version of a passport; it will be a comprehensive system, where individuals handle an entire transaction, from buying a plane

ticket to identifying themselves at the border. What is more, this also demonstrates that there are many different actors that are involved in the (creation of) the EUDI wallet: to establish a system which includes many different types of credentials and functions, an assemblage of actors is needed. This suggests that identification is changing, as it is not purely managed by states anymore; I argue that the wallet requires an assemblage of state, corporate and technology actors to be able to perform its various functions. Moreover, it means that the way in which identification is 'done' is different as well: the wallet connects these different functions and services, collapsing different social institutions in one app. Or, as Marco, another member of the Expert Group, summarised it in an interview: '[w]e already have wallets, digital identity wallets, payment wallets, like Google Pay, Apple Pay, and so on. But what Europe is drafting is something different, more complete.'

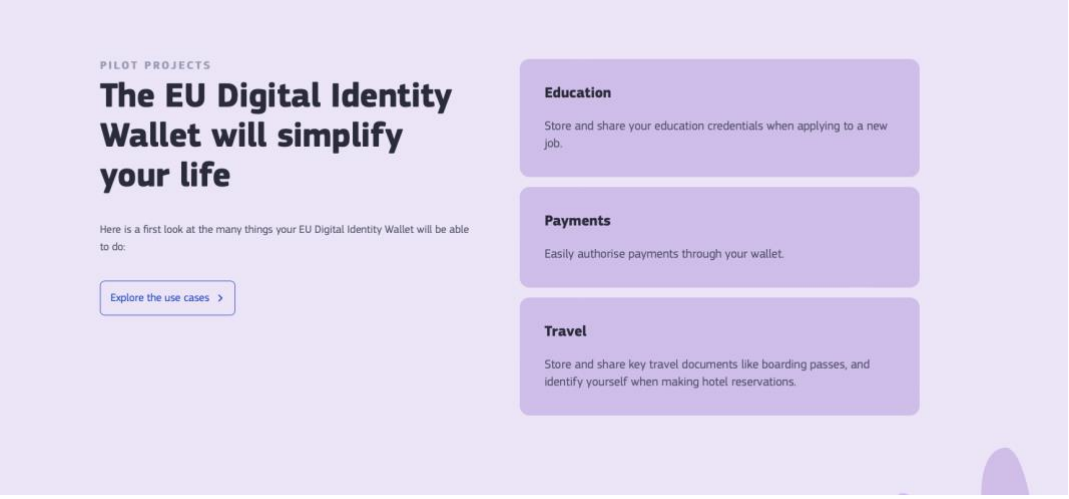
4.3.2. Online identification

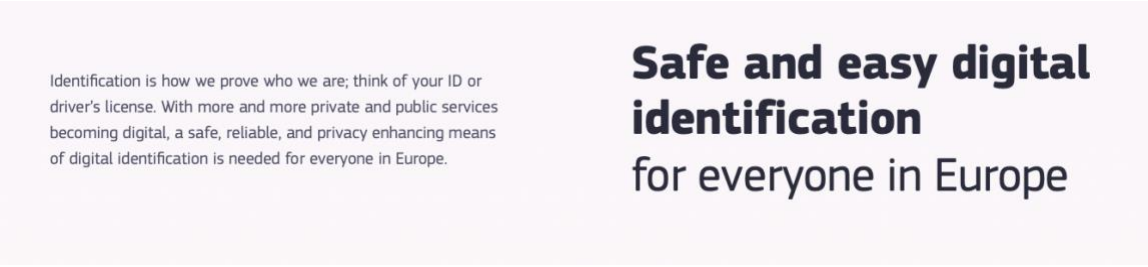
That this wallet is more 'complete' also becomes clear when looking at its digital goals. A key change is that, in addition to the blurring of public and private identification, the EUDI wallet is also blurring the boundaries between the online and offline. It is meant to respond to digital challenges, particularly the exploitation of personal data. In this new collapse of identification by the state and on the internet, the connection between SSI and the EUDI Wallet becomes clearer, as 'control' is one of the key promises. In the communications on the wallet, the European Commission (n.d.; 2024; see also European Council, 2022) heavily emphasises that big online platforms should not have as much power over data as they currently do. For example, Ursula van der Leyen, president of the European Commission, stressed this objective in her State of the Union address in 2020:

> 'Every time an App or website asks us to create a new digital identity or to easily log on via a big platform, we have no idea what happens to our data in reality. That is why the Commission will propose a secure European e-identity. One that we trust and that any citizen can use anywhere in Europe to do anything from paying your taxes to renting a bicycle. A technology where we can control ourselves what data is used and how' (European Commission, n.d.).

This means that the wallet is aiming to do more than state-sanctioned identification systems usually do; it includes identification through the internet as well. As I mentioned above, one key example is that it will be mandatory for Very Large Online Platforms (VLOPs), such as Meta/Facebook, Amazon, and Apple, to make it possible for users to log in using the EUDI Wallet (European Commission, 2023; 2023e). Similarly, the wallet can be used for other types of online transactions: this can be to prove one's age, but also to make a purchase in an online shop. Importantly, this is framed in the language of SSI, emphasising control over personal data and 'empowerment' for users. This means that the EUDI is more than an identification system alone, as it also aims to intervene in data exploitation practices. As such, it puts itself in conversation with some of the big digital issues of these times, which are related to

datafication, turning all aspects of people's lives into data (Cukier and Mayer-Schönberger, 2013), and the harvesting and selling that data for profit, 'surveillance capitalism' (Zuboff, 2019). On the special EUDI Wallet website (2024) that has been recently launched, these ideas are made clear:





Source: European Commission (2024)

Importantly, there is also a political dimension to this: with this change, the European Commission aims to regulate, and remove power from big online platforms. This is indicative of a larger power struggle, where states and other political bodies (such as the EU) are trying to reign in the power of Big Tech corporations; power that has been likened to the power of states before (Broeders and Taylor, 2017). The EU recently introduced its 'quest' for technological/digital sovereignty, which refers to 'Europe's ability to act independently in the

digital world' (Madiega, 2020: 1). This is motivated by concerns of being caught in a technological battle between the United States and China (Giddens, 2020), which is why the EU is trying to 'establish itself as a strategically autonomous third actor' (Broeders et al., 2023: 2).

While not yet framed in these terms, the General Data Protection Regulation (GDPR), which entered into force in 2018, can be seen as an early iteration of the EU's efforts to control the growing data economy. Often seen as landmark legislation, the GDPR aimed to put limits to large-scale processing of individuals by companies, and promised 'data subjects' more rights and control over their personal data (Vrabec, 2021). The EUDI Wallet builds on this legislation, as the processing of personal data is a key feature of the wallet (Sümer and Schroeders, 2021). Other recent examples include the Digital Services Act (DSA), which aims to protect users of online platforms, such as social media platforms and online marketplaces, from harmful or illegal content (European Commission, n.d.-b) and the Digital Markets Act (DMA), which aims to break the market dominance of large online platforms that are gatekeepers for certain products and services (European Commission, n.d.-c). The DSA introduced the concept of 'Very Large Online Platforms', which have at least 45 million monthly users (European Commission, 2023f), and which is, as I mentioned, used for the EUDI Wallet as well. Therefore, while the EUDI Wallet is a big change on its own, it is also related to other legislation, and should be seen against the backdrop of larger power battles.

4.4. From the internet to the state: the translation of SSI

So far, the chapter has introduced SSI technology and the EUDI Wallet, showing that the sociotechnical imaginary of 'control' and identification through credentials are being adapted to the context of (EU member) states. However, there are also points of friction: as I will show, the 'translation' of SSI to the sphere of the state is not always easy or possible. Even though SSI's imaginary of control is fundamentally reliant on its technological architecture, it is, due to political and institutional constraints, not always possible to implement this technology in a state-issued identification system. This, I argue, is because while the EUDI Wallet promises to shift 'control' to citizens, EU member states also need to retain control over identifying their citizens, a classic function of identification (Lyon, 2007). I found that, because of this 'translation' of SSI, some experts argue that EUDI Wallet will not be 'pure' SSI, while others point out that the concept of SSI is not 'crystal clear.' In what follows, I will address the frictions that arise in the translation from the context of the internet to the state, paying attention to the topics of identity, decentralisation, and trust.

4.4.1. Translating ideology

As family of other cryptography-based and decentralised technologies, SSI has made some similar promises about the future, the main one being the subversion of existing power structures. However, as scholars have pointed out in relation to blockchain and Bitcoin, it can

be difficult to implement these promises in reality. For example, Swartz (2018) distinguishes between 'radical' and 'incorporative' blockchain dreams. In this view, radical blockchain dreamers are 'oriented toward revolutionary social, economic and political change' and are hoping to bring about a new techno-economic order through the technology (Swartz, 2018: 189). Incorporative blockchain projects, on the other hand, do not have the ambition to radically subvert the social order; rather they incorporate the blockchain into existing structures, without the aim to really change things. Importantly, however, they do 'benefit from the "revolutionary" aura of the radical projects, but are far afield from the original goals of bitcoin' (Swartz, 2018: 190). In practice, she argues, the distinction between the two types of blockchain dreams is not very clear, and they move on a continuum (Swartz, 2018: 191). Similarly, Hussain (2020) distinguishes between different groups of blockchain projects in relation to governance: crypto-anarchists and crypto-institutionalists. While the former group sees blockchain as a means to detach from the state, the latter are working with states, using blockchain as a means to improve a government's efficiency, security, transparency and accountability (Hussain, 2020). In other words, while not all radical promises can be put in practice, states still use the technology. As such, it must be translated to a different context.

Researchers working on sociotechnical imaginaries, have pointed out that these often need to be 'translated' to different contexts in order to come into reality. For example, Hockenbull and Cohn (2021: 304) argue that while sociotechnical imaginaries are often transnational, 'for them to come into practice they must be made local' (Hockenhull and Cohn, 2021: 304). Similarly, Kim (2018: 176) argues that 'when technology policy moves from one country to another, it is not simply replicated; rather, it is reinterpreted, edited, adjusted, and reformed in the local environment.' In other words, in order for radical promises and sociotechnical imaginaries to work, adjustment is often needed.

In the case of SSI, there are advocates who dream of complete independence of any kind of middleman or institution and complete control over one's own data and identity (see e.g. The Moxy Tongue, 2023). However, most SSI proponents are less radical: the SSI experts I have spoken to are keen to help incorporate self-sovereign identity technology in existing governance structures. Christoph reflects on this ideological question in an interview:

> 'I think there's nothing wrong with the government or EU to build some of this right, if they are building wallets, and […] some infrastructures too, I think that if it follows, you know, the ideas of decentralisation and self-sovereignty, even to some extent, even if it's not perfect…I think it really helps the idea of self-sovereign identity. I mean, yes, you could say that in the very early days of SSI and decentralised identity, it was not the government. So it was a…it was maybe a smaller more grassroots hacker community, dreaming of some utopian SSI infrastructure. Sometimes confusing… maybe the idea of self-sovereign identity with things like anarchy or something like that right. Some people said "self sovereign means you don't have to pay taxes anymore", or something like that, and that's really not how it should be. I don't really see this…contradiction or repurposing. I mean maybe a little bit, yes, maybe it's not this super pure techno-utopian dream that a few

people had in the beginning about self-sovereign identities, and maybe it is a bit more pragmatic with some, of course, some influence by governments and certain policies.'

In other words, according to this expert, adoption by state actors is something positive, so long as the important SSI principles are adhered to. As such, there is a sense of pragmatism; not all of the original principles and technological decisions have to be implemented in order for state-issued identification systems to constitute SSI. He continues by saying that:

'I see it as something positive that because self-sovereign identity doesn't…it's not about replacing traditional authorities, right. It doesn't mean that we don't want passports anymore, or we don't want to be citizens of a nation state or so, but it means it means […] these should not be able to control the whole system, right, they should not be able to…take away my identity. They are just supporting the system and playing their traditional role, but not every…not every transaction that I do with my wallet, for example, goes through the government, right, that would not be self-sovereign, but that's not how it's planned anyway. So…like I said, I see this as generally quite positive…of "oh, this is happening".'

This raises the important point that implementing SSI in the context of the state does not mean that traditional institutions do not matter anymore: it will become an identification system that aligns with the role of the state. In another interview, Sophie tells me that she thinks that SSI is in fact in line with state-issued identification systems. Moreover, she points out, state adoption is needed for the uptake of SSI:

'And so now you can have this whole debate like, "is it okay that the states are doing it?" They start in the identity business right now, and you know, […] I think […] that SSI lines with paper-based models. Like, archetypically it's the same. And Western liberal democracies do not want to build phone home spy systems. I mean, maybe some of the spy parts the government do, but everyone else does stuff that they actually believe in Western liberal of democracy, and they believe that the government shouldn't be tracking everything citizens do. They got…they…I think they kind of saw that, and they're like, "okay, great." And I think it's fantastic. I don't know how else we would get mass large-scale adoption.'

In other words, she believes that not only there is not a conflict of values, but SSI is a logical step for Western states. She also points out that for SSI to become a widely adopted technology, actors with money (like states) must be involved. This has its downside as well, she explains:

'The other thing…okay, this is all the other thought I had about the question. Our OG, do you know that term? It's not a very European term. […] But the OG community had no interest in state stuff. Zero. And if you look at Open ID and stuff, it was really widely adopted by the commercial sector. And the commercial sector then morphed it so that it

> was really useful to them […] and made these large identity providers which weren't necessarily helpful to normal people at all. […] So now we're dancing with the states, and we'll see how they try and morph what we have to suit their needs, and they definitely will.'

In other words, any actor that becomes involved, will shape the technology according to its own needs. Therefore, the technology is not just shaped by the original SSI community: to make it work at a large scale, different actors get involved, reshaping it. This brings up a key tension, that most of my interviewees highlight: it is clear that SSI technology has to be adapted in order to be used for different purposes, but at what point does it stop being SSI?

4.4.2. Is the EUDI Wallet 'real' SSI?

This question is directly relevant to the EUDI Wallet, and whether it can be considered to be an implementation of SSI technology. An early impact assessment published by the European Commission (2021: 48) - which accompanied the legislative proposal for the EUDI Wallet - explicitly mentions SSI:

> '[u]sers expect a self-determined environment where a variety of different credentials and attributes can be carried and shared such as for example your national eID, professional certificates, public transport passes or, in certain cases, even digital concert tickets. These are so-called self-sovereign app-based wallets managed through the mobile device of the user allowing for a secure and easy access to different services, both public and private, under his or her full control.'

This report suggests that the EUDI Wallet was originally modelled after SSI technology, as this would make it possible to bring together different kinds of credentials, and put individuals in control of them. The same report states that:

> '[d]igital wallets are a practical way of implementing SSI as they offer convenient possibilities for the user to manage and exchange their own identity-related information, attributes and credentials' (European Commission, 2021: 48).

In other words, SSI technology is explicitly mentioned as the technological solution that will make the EUDI Wallet possible. Interestingly, however, the term 'SSI' was omitted from later policy documents. While the first version of the proposed legislation still mentioned it (Proposal for amending Regulation (EU) No 910/2014, 2021), the final version does not include the concept of SSI technology (Regulation (EU) 2024/1183, 2024). A potential explanation for this, is that legislation, as several of my interviewees tell me, must be 'tech agnostic'. This means that the technological solution should not be prescribed by the legislation; the legislation can merely establish what criteria the technology must fulfil.

This prompts the question whether the EUDI Wallet is an implementation of SSI technology or not. Most of the experts whom I have interviewed agree that it is, though the EUDI Wallet is not 'pure' SSI. More specifically, I found that whether the EUDI Wallet is considered to be 'close enough', depends on the level of pragmatism that each expert is willing to embrace. An important factor in this, is that the definition of SSI is not agreed upon and therefore open to interpretation. For example, Marta, a decentralised identity consultant for a global tech consultancy tells me in an interview that the EUDI Wallet is:

> 'hands down the most mature effort in the world to deliver self-sovereign identity. It's cross-border and cross-sector. This not something we have anywhere else in the world. […] What the EU is doing, is covering 27 countries and pretty much any sector under the sun, so very unique, very mature, and very impressive. And I wouldn't be surprised if other countries follow.'

However, she also points out that SSI is a slippery concept:

> 'there is no one unanimous definition of what SSI actually means. There are quite a few definitions out there. Will it be self-sovereign identity, decentralised identity in the purest sense? No. I don't think it will. But…at least in the foreseeable future…it will be actually nicely aligned to quite a few principles that are self-sovereign identity principles.'

This slightly paradoxical response, that the definition of SSI is unclear, yet the EUDI Wallet will be an implementation of it, though not in the 'pure' sense, is one I receive more often. As Carl tells me:

> 'Basically all 10 or 12 SSI principles can be fulfilled by the EU digital wallet'. […] But yeah… my question would be a little bit more "what is an SSI wallet?" There is no definition.'

These quotes show some of the practical difficulties that come with implementing a concept, that, up until very recently, was just a (sociotechnical) imaginary: as there is only a list of principles, it is hard to know what it will look like as a material reality. At the same time, I found that SSI's core imaginary, which revolves around 'control', is consistently mentioned as the EUDI Wallet's main objective as well. Erik, another member of the eIDAS Expert Group, makes a similar point in an interview:

> 'The whole concept of SSI is not so crystal clear. What does it mean? So, if it would be that everything would […] be decentralised, this will not make it happen. I think it is a step towards that direction, but it will not change everything. And there's some people who are really into this blockchain thing, I don't know. […] There are many different aspects and criteria. How you can evaluate if it's SSI, or not SSI… and well, the definition is not so clear to me that I could say that it is, or it is not. But, I think […] at least if we talk about giving more control to the citizen […] that is true.'

This shows that, while the definition of SSI is not clear to everyone, the sociotechnical imaginary of 'control' to individuals shines through, and is being translated to the context of the EU. Aidan, who researches SSI for the EU, is very enthusiastic about the prospect of control and SSI for the citizen:

> 'Because, I mean, this is… it's your… okay…you're walking around with a mobile phone device. So much data - GPS data on offer; visual tracking - like the amount of data, you create, this is insane! More with your… when you're in a smart house and, you know, your fridge is going to be talking to you and your fruit bowl is going to be talking to you and every single thing you buy in the future is going to be creating data about you and your living environment or your work environment. You're buying these devices, you're walking around, you're making friends, you're talking to people, you're interacting - it's your data, you should own it. Why should some random American company own and monetise the data that I've created?! No, we should make the money from the data or not make money if we don't want to share it, it should be completely your choice, it's your data, it's your choice. So really, I believe in GDPR like as an EU citizen, but with self-sovereign identity, it will really enable me to take advantage of it and actually start to control sell, or not sell, or basically just have a way where I can actually start thinking about who gets my data or not.'

In other words, there is some conceptual confusion around SSI. This starts with the fact that the EU Commission itself chose to omit the term from policy documents, but is also reflected in the fact that there is not one agreed upon definition. Furthermore, as not all technical elements and principles can be enshrined in the EUDI Wallet, experts often told me that the EUDI Wallet will not be 'pure' SSI. At the same time, however, they did consistently mention the sociotechnical imaginary of 'control' as one of the core aims of the EUDI Wallet. Therefore, this leads to a slightly paradoxical situation, where the definition of SSI is unclear, yet the EUDI Wallet will be an implementation of it (though not in the 'pure' sense). Therefore, I found that whether experts call the EUDI Wallet 'SSI' depends on the level of pragmatism they are willing to embrace.

4.4.3. Identity

Not all experts I spoke to were equally pragmatic: some believe that not enough SSI principles will be implemented in the EUDI Wallet. Max, SSI expert, tells me that he does not believe the EUDI Wallet to be a self-sovereign solution, because of the role that governments will play in the issuance of ID credentials. As he points out, the status of the wallet will be dependent on the foundational identification information that is provided by states:

> 'the type 1 configuration will include the most valuable credential. That's kind of the identification credential provided by the government, right, to… for the statement of who you are, and there will also be, depending on if this credential is valid, and in your wallet, your wallet will have a different state compared to if it's not in the wallet.'

This refers to discussions in an earlier stage of development of the EUDI Wallet: initially, the wallet was only supposed to work when this foundational credential (the so-called 'PID': Personal Identification Data) had been loaded onto the wallet. However, in a later amendment, this was changed; the wallet will now still be able to operate, but will not give access to all services if this credential is missing (De Rosa, 2024). The status of state-issued identification goes to the heart of the tension between SSI and state-sanctioned identification: following SSI in the 'pure' sense, states are not supposed to have a special status, or any kind of additional control over the wallet, as this would mean that the individual is not completely sovereign over their identity. As such, this shows that 'identity' as envisioned in the world of SSI does not align with the objectives of the state: being a user on the internet is different to being a citizen of a state - and for states it is necessary to remain in control over the identification of their citizens. As Frederico, member of the eIDAS Expert Group, tells me in an interview:

> 'Okay, okay, okay, I have to be sincere with you. […] When we are born, who assigns the identity to the to the citizen? The public service. […] At the same time…So this is one of the most important exceptions for the level of assurance, because […] the nation, the state, the public service, is the trusted third party. Otherwise, I may say "I'm batman." At the same time, yeah, the ideological problem or the wrong assumption… At the same time, we have enabled anonymous authentication, and also pseudonymisation. So Isadora is able to be authenticated like Moana, she has created a pseudonym […]. But at the same time the wallet […] gives the proof that this is our citizen, and [that it is] a secure solution.'

In other words, even though the wallet will make it possible to be anonymous and create pseudonyms, the core identity will always be assigned by the state. In other words, states will always maintain power over the issuance of citizen identities, meaning that individuals will not be completely in control. This goes to the heart of identification practices, as it is the state that is making people 'legible' (Scott, 1998), and confers the status of citizen through documentation (Torpey, 2000). As Frederico explains:

> 'So […] we have enabled technically, the issuance of your identity. And that's self-sovereign, but it's not identity, you know, it's a pseudonym [laughs]. Well, the this…all these terms belong to Web 3, that's something like a revolution that was driven by money, digital assets. So this revolution […] came up with assumptions […] and we are the deciding what is useful to the system and to the citizen, for the welfare of the all the participants, and what is just a false assumption. So in this field we are working to re-evaluate the meaning of self-sovereign identity.'

This shows how SSI technology needs to be translated to the context of state-issued identification, so that 'identity' as created for the internet, which I described in the first part of this chapter, and 'identity' for citizens align. What is more, this signifies that, despite the promise of control to citizens, states need to retain control over the identification process. I

will dive deeper into the connection between digital identity and digital citizenship in the next chapter.

4.4.4. Decentralisation

In a similar vein, because of the involvement of states, complete decentralisation is hard to realise. For some, this is reason for concern. Lucas, who works for the European Blockchain Services Infrastructure, and co-othered a Digital Identity Manifesto, has his doubts about the 'control' that citizens will be granted:

> 'There is a lot of…like you had green washing…you have a lot of SSI washing at this moment, because we had […] a panel discussion with some people of the Commission. The political message is fully SSI-based about data empowerment, data ownership, self-sovereignty. So the political high-level message is there. But if you look at what the implementation is, it is very classic. They have centralised service providers. Now they tend to say "okay, but it's hybrid so that we can do both," but it's a bit difficult, and you cannot be centralised and decentralised, and have ownership on both sides. That is a bad model, so they tend to compromise it…but there is washing on that aspect.'

As he points out, there is a tension between the political narrative and the actual implementation. Again, this involves the distribution of control: how to balance transferring a degree of control (over data) to citizens, but also remain in control of the identification system? This highlights how the sociotechnical imaginary of 'control' for individuals is being adopted by the EUDI Wallet, but also has to be translated to fit in with the real-world power structures that underpin state-issued identification systems. This becomes clear when looking at the extent to which SSI principles and building blocks, such as decentralisation, can be implemented. Andreas, eIDAS Expert Group member, tells me that he does not think that the wallet can be fully decentralised:

> 'The let's say "pure" approach of a self-sovereign identity, is…does not match perfectly. In a process like taxes, it's not you as a citizen being in control of the number of identities you create, and as which person you approach the authority. It might be in your interest, in particular for tax splitting [laughs]… but […] in the "pure" meaning that it is the user in control of creating identities, that doesn't match the requirements you have in a regulated area.'

However, he continues, the EUDI Wallet is not just for public sector services, also for private sector ones. Therefore, he thinks, in particular for services that do not require any stringent identification procedures (like so-called 'Know Your Customer' procedures do, for example) by law, decentralisation would be possible. Be that as it may, to what extent the EUDI Wallet will be decentralised, 'will pretty much depend on the member state implementations.' As an

example, he refers to the current digital identity system in Austria, and describes its privacy-preserving features. He remarks:

> 'In the Austrian case, for instance, it will be unlikely that that we throw away that investment in what we assume a pretty privacy preserving way of doing identification, just because other initiatives claim the decentralised or self-sovereign identity is the way to go. So that will pretty much depend on the member states, whether it will be a completely decentralized system, whether member states built upon existing systems, or whether it will be a hybrid between a [centralised and a] decentralised system.'

Therefore, to what extent wallets are decentralised will also depend on different member states, as they are in charge of certifying wallets for their citizens. This shows that SSI's technical components and principles can only be implemented to the extent that it fits within existing (power) structures, both between citizens and states and between different member states in the EU.

4.4.5. Trust

Relatedly, Antonio, who is a consultant to the European Commission on this topic, remarks that it is not possible for the EUDI Wallet to be completely decentralised, as centralised governance will always be necessary for states to remain in control over the identification of their citizens.

> 'Antonio: I'll just say there is a kind of hype around this self-sovereign identity, it's about not trusting anybody. That's not true. I mean, it's what we are not buying, basically.
>
> Isadora: Okay. Why not?
>
> Antonio: [laughs] Because I mean…mainly this is related to the blockchain thing and…blockchain at the end…it's a technology done for cryptocurrency, where there was kind of a specific requirement that was necessary in that case. For Bitcoin, for example. In this case it's not needed. I mean, you are trusting every day your government, you are trusting every day a lot of things, and if you don't have trust, if you don't find a way to establish the trust, it doesn't make any sense what you're doing in this in this field, you know. […] You'll always have centralised governance. So the model we are promoting is going to be decentralised in terms of functions and functionalities, but obviously the governance is going to be centralised, because at the end is the member state responsible to identify you. You cannot…I mean who else is it going to be, who else are you going to trust to identify you, if not the member state that recognises you?'

This connects decentralisation directly to the topic of 'trust': because it is not possible to make the system fully decentralised, it is necessary for there to be a certain level of trust in the state. While 'trust' in the technical jargon refers to minimising risk, which can be established through

cryptography in combination with rules and policies, a different kind of trust is needed to make a state-issued identification system work: institutional trust. Institutional trust can, for example, be based on cultural factors (Kaasa and Adriani, 2022), or personal circumstances, such as socio-economic position (Lipps and Schraff, 2020; Kim et al, 2022). This type of trust is necessary for the system to work, as there needs to be a governance framework created by the EU and member states to make the EUDI Wallet function. As such, 'trust' is not only put in technology or cryptography; there also needs to be trust in the government to facilitate identification and therefore access to services. Peter emphasises that it is important to consider the differences between the American and European SSI movement:

> 'You see the American movement is acting much more on SSI in relation to autonomy because they trust the government less. And so SSI becomes a means to act independently, separate from the government. This is much more about self-issued credentials, with a certain form of assurance, rather than a digital foundational identity […] which is what we are all actually waiting for in The Netherlands. So there is an Atlantic Ocean between these ways of thinking.'

As such, even though the emphasis on 'control' is the same in the EUDI Wallet, the cultural connotations attached to it may be different. As Peter suggests, there might be a higher level of trust in the government in the EU than in the US. This shows that, even though the same terms are used, there are important local differences, which influence how sociotechnical imaginaries are put in practice in these local contexts (Kim, 2018). Another interviewee makes a similar point: Erik, member of the eIDAS Expert Group, tells me that he thinks that this level of trust also varies from country to country within the EU. He points out that in the Nordic countries, the level of trust of citizens in their government is quite high and he is not sure if decentralisation is absolutely necessary:

> 'I think people in Nordic countries, they are quite happy with the public administration, and we tend to trust the authorities quite much. So it can depend on where the member state is located and so on […] the history and everything.'

Therefore, if institutional trust is high, as Erik suggests, citizens might not be very interested in a decentralised system. What becomes clear in these conversations, is that the politics and local systems in the different (member) states matter. The level of 'trust' is not the same in different places, and the trust that citizens place in their government and administration may also influence the perceived need for a decentralised identification system.

More generally, these different views show that even though the sociotechnical imaginary of 'control' is being translated from the context of the internet to the context of the state, some of the technical components are not as easy to adopt. This suggests, I argue, a tension between giving more 'control' to citizens, and states wanting to retain control over identification processes.

4.5. Conclusion

This chapter interrogated the move from an identity that was developed for the internet, to the context of the state. It introduced SSI technology and the European Digital Identity Wallet through the lens of sociotechnical imaginaries (Jasanoff and Kim, 2015). I argued that SSI's sociotechnical imaginary revolves around 'control' – putting individuals in charge of their personal data – and addressed three key parts of the technology- identity, decentralisation and trust- to illustrate the link of this sociotechnical imaginary to SSI's technical architecture. I argued that the EUDI Wallet adopts the sociotechnical imaginary of 'control', and therefore applies an imaginary that was invented for users on the internet, to citizens in EU member states. Importantly, however, while this imaginary has been adopted, it is not always possible to implement all of SSI's (technical) elements in the context of states, resulting in friction in this 'translation' across contexts. Accordingly, interviewees often told me that the EUDI Wallet is not 'pure' SSI. I argued that this highlights the tension around 'control' that states face: while they can shift some control over to their citizens, they need to simultaneously make sure that they retain the control over identifying their citizens. As such, there is a tension between the classic functions of identification, where states make their citizens 'legible', and SSI's emphasis on self-sovereignty. At the same time, and paradoxically, with the move to a wallet-based system, the EUDI Wallet also requires the involvement of different actors. I argue that the fact that the EUDI Wallet adopts the use of credentials – which come from the world of SSI – and aims to give access to a wide range of services, means that new assemblages of corporate, internet and state actors will be involved in identification processes. Ultimately, therefore, the credentialisation of identification signifies that identification processes are changing, and bring about a new role for states, which have to find a balance between giving away and trying to retain control while the scope of identification widens. In the next chapter, I will address what the sociotechnical imaginary of 'control' means for citizens and the new role they will have to take up in this system.

Chapter 5. Encoding Citizenship: how the European Digital Identity Wallet enacts 'user-citizens'

> *A prominent SSI figure asked the audience who is currently using Apple Pay or Google Pay. After a show of hands, he announced that what is happening to digital payments will happen with digital ID wallets as well: 'in five years,' he predicted, 'the wallet is going to be at the centre…pervading everything'* (Identity & Technology Forum, May 2023).

5.1. Introduction

Landon Winner (1980) famously asked whether artifacts have politics. While looking at the social and economic structures around technology is important, he argued, technologies themselves are 'ways of building order in our world' (Winner, 1980: 127). Specific design choices influence the way people go about their lives for a long time. Therefore, he suggests that 'technological innovations are similar to legislative acts or political foundings that establish a framework for public order that will endure over many generations' (Winner, 1980: 128), as successful technologies structure and order society. As I discussed in the previous chapter, SSI technology aims to rearrange power relations between states and companies on the one hand, and individuals on the other, by technologically enshrining the sociotechnical imaginary of 'control' over the sharing of personal data. In this chapter, I will expand this, by looking at the prospective role of citizens in this new system.

This chapter makes three interlinking arguments. First, it argues that the EUDI wallet begins to enact what I term a 'user-citizen' who is supposed to be digitally literate, entrepreneurial, and able to decide on the terms of their own datafication. I show that citizenship is envisioned in a way where citizens have to interact with the technology in order to participate in the (digital) society, thus 'acting' as users of the technology. As such, 'user' behaviour, such as consenting to the sharing of personal data, is being applied to citizen 'transactions', as this becomes part and parcel of gaining access to services. Therefore, the EUDI wallet is blurring the boundaries between users and citizens, and signifies a new role for citizens in their interactions with the state. Second, I argue that this is significant, because the credentialisation of identification means that the wallet will store high volumes of (high quality), 'verifiable' data, which can be used for both public and private services. Therefore, using the wallet requires a behavioural shift (becoming a 'user-citizen') on the side of citizens, where they manage these credentials, and are made responsible for making good data choices. This is important, because there is an insertion of market-like logics into the realm of identification: due to the wide scope of the wallet, the possibility of a new market arises. In this market, citizens can consent to exchanging their personal data for perks, such as discounts. Third, I argue that this could give rise to new inequalities, as not all citizens may have the time, resources and data literacy to manage their data. Therefore, if digital skills and access to

technology are not scaled alongside this development, it is important to question what is really on offer in the wallet.

To make these points, I first address the link between 'digital identity' and digital citizenship, showing that digital identity is seen as a prerequisite for participation in the digital society. I then turn to the new role that citizens are expected to take up in this system, arguing that this enacts a 'user-citizen.' I expand this further in the next section, which looks at the link between 'control' and 'empowerment'. This section also addresses the possibility of a new market, where citizens monetise their personal data, exchanging it for perks and benefits. Finally, I address the potential drawbacks of this new system, highlighting the potential new inequalities that could arise, as not all groups might have the digital literacy, financial resources, and time to use the wallet.

5.2. Digital identity and digital citizenship

The previous chapter looked at identity in the context of the internet, and mentioned some of the frictions related to implementing this in the context of (EU) states. This chapter will dive deeper into this, connecting the topic of digital identity to citizenship. As I mentioned, identification documents are inherently linked to citizenship as being 'legible' (Scott, 1998) to the state by means of a legal identification document, grants citizens access to rights, benefits, and responsibilities (Lyon, 2007). Therefore, identification is intimately tied to one of the classic dimensions of citizenship, which is social rights and participation in society (see e.g. Marshall, 1950; Joppke, 2007). However, looking at this in the digital realm, citizenship is also meant to give access to rights and benefits online, and as such, allow for participation in the digital sphere (Mossberger et al., 2007; Antenucci and Tomasello, 2023). It is important to note, however, that the opportunities for participation that digital technologies offer have become more complex due to the rise of datafication and the surveillance practices that come with it (Hintz, et al. 2018; Hintz, 2020). As Pangrazio and Sefton-Green (2021) point out, while the digital offers opportunities for engagement and participation, the 'opacity of digital infrastructures and the increasing reliance on algorithmic decision-making raises critical challenges to what it means to be an informed, engaged and active citizen.' Furthermore, while the digital can make citizens less dependent on their nation-state, it is also a means for states to extend their power over citizens (Pangrazio and Sefton-Green, 2021). Similarly, as Barassi (2019) notes, while the capturing of citizen data has been part and parcel of states monitoring their citizens, the extent to which this is possible today is unprecedented. Consequently, the construction and prediction of citizen subjects through data (see e.g. Cheney-Lippold, 2017; Fourcade and Healy, 2013; Fourcade, 2021) has the potential to reconfigure state-citizen relationships in profound ways (Barassi, 2019; Fourcade and Gordon, 2020). In other words, therefore, digital citizenship is complicated; as Hintz et al. (2018) observe, there is a tension between the option for participation that the internet offers citizens, and the potential for increased surveillance that it offers states.

SSI technology, and therefore the EUDI Wallet, occupy an interesting position in this debate: on the one hand, the technology is supposed to solve some of the problems associated with earlier identification systems, particularly in terms of control over personal data (see e.g. Hicks, 2020; Masiero, 2020). What is more, it aims to go beyond this, for it aims to offer citizens a means to control their personal data in all kinds of transactions, both offline and online, ranging from logging in to a social media platform to picking up a prescription (European Commission, 2024c). On the other hand, the EUDI Wallet will be a state-issued identification system that is supposed to be able to 'verify' citizens' identities with a very high degree of confidence. This means that it is also part of a longer history of identification by the state, where identification should be seen as a relationship infused with power in itself, as it is a means for states to produce 'uniqueness' so that citizens can be made 'legible' and differentiated from others (Brensinger and Eyal, 2021). As Caplan and Torpey (2001: 8) note in relation to older identity documents:

> 'The identity document purports to be a record of uniqueness, but also has to be an element in a classifying series that reduces individuality to a unit in a series, and that is thus simultaneously deindividualizing. This discloses the fundamental instability of the concept of the "individual" as such, and helps to explain the uneasy sense that we never fully own or control our identity, that the identity document carries a threat of expropriation at the same time as it claims to represent who we "are".'

In other words, as I also mentioned in the previous chapter, the very act of giving someone a 'unique' identity establishes a relationship characterised by power - where the state makes an individual part of a series. As such, the question whether individuals will be able to 'control' their digital identity and data - the main promise of SSI technology – becomes questionable. This means that there is an inherent tension between the want to give citizens more 'control' over their data and digital identities, and the traditional functions of state-issued identification, as it is a means for states to establish control over the citizenry (Lyon, 2008; Torpey, 2000).

In the interviews I conducted with the people working on the EUDI Wallet, it became clear that they mainly view the wallet as a means for citizens to participate in the digital society. Here, identification is seen as a means to acquire access to (digital) services. For this, a 'digital identity' is needed. While a digital identity is not the same as digital citizenship, the two are closely connected. As Sullivan (2018) describes, 'digital identity' is a relatively recent term, which was crystallised by the move of government services online. This move, she argues, 'elevated digital identity to a new level of commercial and legal significance because government schemes are usually necessarily based on the premise of one person: one digital identity' (Sullivan, 2018: 724). In other words, it is a means to establish uniqueness and 'fix' identities - which is a common feature across all identification schemes, as this makes it possible to 'verify' a person's identity. As Sullivan (2018: 725) points out, there are two steps to digital identity schemes: the authentication of an identity at the time of registration, so the establishment of a digital identity based on documents such as birth certificates and passports, and the verification of identity, which happens any time a transaction takes place. This goes

back to what I discussed in the previous chapter: any time a citizen releases (part of) a credential, their identity is verified. As different parts of people's lives are 'credentialised', the wallet stores an aggregated digital identity, consisting of various credentials.

Importantly, the verification of identities is also key to the link between digital identity and digital citizenship: the idea is that a citizen's identity needs to be verified in order to grant them access to services and benefits. As a result, the verification of a citizen's identity becomes a prerequisite for access to services, and thus participation in (digital) society. As Antonio, consultant to the European Commission on the topic of the EUDI Wallet, explains to me in an interview:

> 'Because if you look from a […] digital citizenship point of view, in order to enable all the citizens to take part of a digital society, performing payments, buying almost everything, you need to be identified, right. Your identity needs to be qualified…you need to be, I mean, at least in many, many countries those are based not on the common law but on civil law, you need to be identified, and you need to have that information in a quite certain way.'

In other words, this suggests that a 'unique' identity is necessary for participation in the digital society. For Antonio, digital citizenship also means that citizens should be able to do anything that they can currently do offline, digitally as well. As he puts it:

> 'Anything […] I can do in real life, I should be able to do also in the digital life. So this is for me, this is the main right, also part of my identity, so, reflecting my identity also in the digital.'

In other words, digital identity is seen as the cornerstone for access to (digital) services – and therefore allows citizens to perform digital citizenship. What is more, as Andreas, member of the eIDAS Expert Group, tells me, it will be mandatory for member states to provide citizens with a digital identity (also called 'eID') and a wallet:

> 'A key aspect of the eIDAS revision is that, from a voluntary exercise of the member states, it becomes a right for the citizen, because member states will have the obligation to issue both a notified eID and a EUDI wallet.'

This is a notable development because it shows that having a digital identity and wallet is taken very seriously by the EU Commission: it becomes a right for citizens. It is crucial to consider who will get to enjoy this right, and whether exercising this right will be possible for everyone. I will discuss this more elaborately in the third part of this chapter. For now, it is important to note that having a digital identity (and wallet) is seen as a prerequisite for digital participation. This also corresponds to how SSI proponents view the role of digital identity. As Christoph tells me in an interview:

> ‘Identity is a prerequisite and foundation for a lot of other things. So if you think about social networks or payment use cases or some online communities, or…different, I don't know, platforms or employment scenarios, […] there are lots and lots of things that that require digital identity as a basis. So, yes, it will…it's not just about logging in and about opening a bank account. It's really about a new kind of very ambitious digital environment and infrastructure that has trust and privacy and all these things built in.’

In other words, being able to ‘verify’ identities is seen as the basis for access to different kinds of services. Therefore, this goes back to the classic relationship between the citizen and the state: only when it has been ‘proven’ that a person is a citizen, they can enjoy the rights and privileges offered by the state (Lyon, 2007). At the same time, however, it is more complicated, as the EUDI Wallet is expanding the wallet beyond the state and public services alone; it will also include an array of private services. I will address this more elaborately in the next section of this chapter.

Another important factor that complicates the relationship between digital identity and digital citizenship is the fact that the EUDI Wallet is being developed at the European level. This is remarkable because matters of citizenship and identification are normally handled by the member states. Furthermore, it is particularly salient because European citizenship is a contested concept: not only legally, because it is derived from national citizenship, but also because European citizens generally feel less attachment to their European than to their national identity (Bauböck, 2007; 2014; Delanty, 2007). As I mentioned above, citizenship goes to the heart of the relationship between citizens and their state: they are issued by the state which recognises a person as a member; a citizen (Torpey, 2000; Lyon, 2007). Therefore, determining that relationship at the EU-level, would imply a significant change in state-citizen relationships. However, this is not the case: while the legislation and the technical specifications for the wallet are developed at the EU-level, member states will be responsible for issuing foundational identity credentials - the digital equivalent of legal identity documents - to citizens (De Rosa, 2024). As Matteo, who is a high-level civil servant in DG CNNCT (the directorate responsible for IT and communication technology in the EU), tells me, citizenship and digital identity were a bone of contention during the development process:

> ‘Identity was actually, I would say, at that moment in time [circa 2014, during the first version of the eIDAS[13] regulation] not even spoken as such, because we never spoke about identity then, but about identification/authentication, because, I mean, the identity has got to do with really the root of citizenship. And the member states, who are very sensitive in seeing something of this to be moved out from their responsibilities to something that can be harmonised or structured beyond what is indeed […] the type of inherent link which is established in each and every member state. And this is why […] eIDAS talks about identification/authentication. Identity is not defined in eIDAS, because it is related to the responsibility of the member states, and we focus on what matters in relation to the

[13] Electronic Identification and Trust Services. This is the legislation that establishes the European Digital Identity Wallet.

> objectives, and that is indeed the internal market, so a company to be able to establish themselves, to be established, or do businesses across Europe, or people, citizens, be able to have access to public services across Europe.'

In other words, there is an inherent friction between citizenship, allocated on the national level, and the European-wide digital identity format. This demonstrates another aspect of credentialisation: here, credentials play an important role, because 1.) the foundational identity credentials will be issued by the member states, and 2.) the possibility to selectively disclose information to 'prove' who you are, is seen as a means to get around this citizenship issue. Namely, Matteo explains that digital identities and credentials made it possible to circumvent the problem of issuing citizenship at the European level:

> 'In order to avoid the problem in the issue of what identity…what somehow makes the link between a person and a community. The way in which you are […] established as a Dutch citizen, the relation between you and your country, your state. The same is for mine. And of course, I mean, at the time it was very much like cleaning the table from having any sense of we are harmonising the way in which the identity of a European citizen is established. This has come. Why? Because I mean at the end of the day, what remains, is that okay, the citizen [Matteo's real name] or Isadora Dullaert…are indeed what counts, and […] the digital identity - not the identity - the *digital identity* is just, I would say, focusing on what proofs of you […] are relevant to the transaction. My age is my digital identity, if I would need to prove my age to buy tobacco online. Nothing else. Or my title, my residence, and I don't know, my age, may indeed […] what is the digital identity instantiation for me to have access to a certain service. But the identity, so the citizen identity, is something completely different, more sophisticated, is much more than properties, attributes, entitlements.'

In other words, different 'proofs' of identity make it possible to focus only on verifying whether someone is who they claim to be or are entitled to something. For example, individuals can choose to 'selectively disclose' the information on their ID credential that is necessary for a certain transaction, such as their name or date of birth (De Salve et al., 2022). This is important, because it shows that the process of credentialisation makes it possible to create digital identities, which in turn are necessary to participate in the digital society, as they allow citizens to 'prove' who they are. In that sense, it is a manifestation of processes of establishing 'uniqueness' which are part and parcel of identification (Caplan and Torpey, 2001). At the same time, focusing on 'proofs' is also a way around the European citizenship issue. For example, the legal identity credential will be only one of the 'proofs' – and one that needs to be issued by an EU member state. Therefore, even though the two are increasingly often conflated (Sperfeldt, 2021; Manby, 2020), there is a difference between identity in the sense of being part of a state - legal identity tied to citizenship - and digital identity. In short, the relationship between digital identity and (digital) citizenship is complex: while digital identities facilitate digital citizenship, as they make it possible for citizens to access services and thus participate

in the digital society, there is an important difference between 'digital identity' and identity associated with citizenship.

5.3. Enacting 'user-citizens'

The 'verification' of identities - which is key to accessing services – is, I argue, made possible through credentialisation: the credentials stored in the EUDI wallet can provide 'proof' about (different aspects of) a citizen's identity and entitlements. At the same time, credentialisation is also what sets the EUDI Wallet apart from existing digital identity schemes: it does not only store the digital equivalent of identity documents such as ID cards and passports, but can also include other credentials, such as supermarket loyalty cards or social security numbers (European Commission, 2024c), thereby turning different aspects of people's lives into 'verifiable' information. As such, it gives access to a wide range of services, both public and private ones, and both offline and online.

Sullivan (2018) already predicted that digital identities created for government services would eventually be used for the private sector as well. As she puts it: '[w]hat this means is that the digital identity required for government transactions effectively becomes the individual's digital identity for transactions generally, and that identity becomes the primary means by which an individual is recognized and can enter into transactions in the digital age' (Sullivan, 2018: 276). However, while the EUDI Wallet does, as I discussed in the previous chapter, make it possible to use credentials across contexts (for example, the ID credential can be used for private transactions as well), it also goes beyond state-issued identity credentials alone. Namely, as it can store all kinds of credentials, the wallet brings together previously separate identification systems and social institutions, ranging from the state, to universities, to banks, to the health sector. I argue that state-issued identification is changing, as the EUDI Wallet collapses these institutions. Therefore, identification is not only 'done' by the state anymore; rather, as I argued in the previous chapter, it increasingly involves shifting assemblages of different public and private actors, that are all involved in identification processes.

Importantly, this new system also presupposes a new way for citizens to interact with services. The EUDI Wallet does not just involve the introduction of a new technology; it also requires a new role for citizens, as they will have to 'perform' within these systems (Fourcade, 2021; Schou and Hjelholt, 2018). While researchers have pointed to collapsing roles of citizens before, such as 'consumer citizens,' where consumer experiences increasingly shape civic participation (Scamell, 2000; Porter, 2020), I argue that the EUDI Wallet blurs the boundaries between 'users' and citizens through its very design. Because of this, I argue, the EUDI Wallet enacts a specific user (see e.g. Woolgar, 1990; Akrich, 1992; Oudshoorn and Pinch, 2003), who is at the same time a citizen: a user-citizen. I argue that the blurring of the boundaries between users and citizens can in part be attributed to the fact that an identity model that was originally developed for the internet, is being applied in the context of the state. Namely, as I will show,

some of the 'user behaviours', such as consenting to the sharing of personal data, is being applied to citizen 'transactions', as this becomes part and parcel of gaining access to services. Furthermore, as I mentioned in the previous section, digital citizenship is envisioned in a way where citizens have to interact with the technology in order to participate in the (digital) society, thus 'acting' as users of the technology. Key to this, is that the credentialisation of identification implies a new way of engaging with transactions.

One part of this, is that digital ID wallets have different abilities than their physical counterparts. As Mark, 'thought leader' in the digital identity and banking sector, tells me, it is important to note that these wallets are 'intelligent':

> 'I make a big distinction in my writing now between the digitised identity, taking your passport, putting it on the web somewhere so we can use it, and a digital identity, so an identity that is created for the digital world, has very different characteristics. It's intelligent, your passport is not intelligent, your electronic passport will be intelligent, for example it might be able to talk to other electronic passports; your passports can't talk to other passports, you know. It might be able to verify them. If you show me your passport, I am not an international anti-piracy, anti-counterfeiting, anti-terrorist genius, I mean, how would I know if your passport is real or not. If you showed your electronic passport to my electronic passport, my electronic passport would know whether it was real or not. Because it's cryptography. You know, digital identities are connected, they can talk to other things, not just other digital identities. They can make decisions. If I look at your passport, your passport tells me everything about you. Your passport doesn't interrogate me, like your passport should be asking me "who are you?" Do you have permission to look for data?'

This means that identification processes will be different, as the way in which citizens will interact with them, will change. Therefore, Mark expands, people will need a new 'ceremony' for the way in which they interact with digital ID wallets:

> 'We don't have a ceremony; we don't know what to do about identity. So at the kind of technical level, we need to resolve that, so that I know when I'm being asked for my identity, I know when I'm asked some facts about me, some attributes, I can tell all that. And it can't be too complicated otherwise people won't do it, so we need some kind of simple sort of ceremony.'

This ceremony could take different forms, such as a place in a shop where people can tap their phone to prove their age, he suggests. The main point is, however, that the implementation of digital ID wallets will need to be accompanied by a new kind of (user) behaviour. I argue that the introduction of digital ID wallets in general (and the EUDI Wallet more specifically) is not just a technological change, it is accompanied by a behavioural shift because it requires people to interact with them in a new way. This is important, particularly because the EUDI Wallet will include so many different functions, services and institutions. As I will show below, this new 'user' behaviour includes ideas about the ways in which individuals should manage their

credentials, as they are supposed to be in control. Luke, developer of blockchain and SSI, suggests that a 'mental shift' is required:

> 'And that requires also a mental shift in thinking how we treat…how we deal with data, because also from my professional experience we noticed, we were trying to…we have a few projects around data science and we realised, "yeah it's really hard to make them work", because we […] have the data but it's really inconsistent, so we store…not "we" but […] like in general, people store the wrong data, type of data in the wrong column. And like you know all these kind of errors which they seem like "oh it's just a typo," but eventually, if you look into that it's like…it all goes down to partially, the fact that you're doing something you have always been doing in one way, and you don't want to adapt and change mentally, and do things differently, because that brings you out of your comfort zone, it requires some effort, you know.'

This suggests that people are used to doing things a certain way, and having to change the way they deal with data will require some time and effort, because they will have to adapt their behaviour. Peter, researcher for a public/private organisation focusing on SSI, makes a similar point, and thinks that the technology is 'only a small part of the solution.' The real change, he suggests, is the way we think about the sharing of data; this goes for individuals, but also for companies, that will have to get used to storing less data:

> 'We need to go from the old thinking, of "data is the new oil", to a different paradigm, where companies no longer store as much data as possible, but rather only store what they need in order to verify someone.'

As such, he thinks that 'technology is only 10% of the problem; it is all about daring to move forward.' This suggests, I argue, that the technology needs to be accompanied by a shift in behaviour; learning how to interact with these new identification systems. While digital ID wallets are new, changes in how users are supposed to interact with transactions have been examined in relation to payments. For example, Mützel (2021: 12) has theorised the 'payment experience'. She points out that, rather than being just an economic action, digital payments are increasingly being framed as experiences, where 'social and communicative interactions with a seller, the product, and potential future buyers moves to the centre stage' (Mützel, 2021: 12). In other words, a new kind of 'ceremony', to use the words of my interviewee Mark, has been created. In a similar vein, Swartz (2020: 4) has argued that digital payments are social: payment is increasingly framed as social media rather than only a financial service. Therefore, according to Swartz (2020), this new sociality points to a profound change in the way that payments work; it is much more than an economic transaction, it is an experience, as well as a tool of categorisation that assigns membership. When digital ID wallets are widely available, it will be important to consider this as well, given the importance of membership for citizenship (Joppke, 2007).

While payments are not the same as verifying identities, these new ways of interacting point to a similar trend: there is a new kind of thinking around transactions, which come with a different social role for the user. In the case of the EUDI Wallet, that user is also a citizen. As I described above, this citizen will need to shift their thinking and behaviour around data, as the EUDI Wallet will put them in 'control' of their credentials. The technological design of the wallet will make this possible, for it enables citizens to store different credentials and select which data they want to disclose. As such, the very design of the wallet says something about the expected 'user'. STS theorists focusing on technology users, have argued that users are 'configured' through the design of technologies: they are designed bearing a user with specific characteristics in mind (Woolgar, 1990; Akrich, 1992; Oudshoorn et al, 2003; Rose and Blume, 2003). Akrich (1992), for example, calls this a 'script', which specifies the role of the user and how they are supposed to interact with the technology. This means that, in a way, the technology shapes the prospective user, as it determines what the technology can do and how the user should interact with it.

In the case of the EUDI Wallet, the design enacts a user who is supposed to manage their credentials, deciding when they want to share them and with whom. This new 'user' behaviour is therefore intimately tied to the sociotechnical imaginary of 'control'. Crucially, these 'users' are citizens at the same time, and being able to interact with the technology also determines whether they can successfully participate in the digital society, thus performing their digital citizenship. I argue that the EUDI Wallet introduces a particular view of the citizen as a user of technology: a 'user-citizen'. I conceptualise the term 'user-citizen' as follows: 1.) the technological model (SSI technology) is taken from the internet and has been developed for 'users' rather than for citizens, and 2.) citizenship is envisioned in a way where citizens have to interact with the technology in order to participate in the (digital) society, thereby acting as users of the technology. 3.) user behaviour, such as consenting to the sharing of personal data, is therefore being applied to citizen 'transactions', as this becomes an integral part of gaining access to services. As I will discuss further below, it is important to examine this development critically, as not everyone can be expected to have the digital literacy, time, or financial resources to make these data decisions.

Before diving deeper into this expected behaviour of the user-citizen, however, it is important to acknowledge that scholars have argued that users often change technologies as well. As Oudshoorn and Pinch (2003: 2) suggest, for example, users can 'consume, modify, domesticate, design, reconfigure and resist technologies.' This means that users can, for example, use technology in a different way than envisioned, or not use it at all. As the EUDI Wallet is not publicly available yet, it is unfortunately not possible to explore how user-citizens might use and change the technology. As I will describe in the concluding chapter, this will be an important avenue for future research. At this moment, it is possible to look at the user-citizen that is envisioned through the design of the EUDI Wallet. This is important, because it speaks to the changes that the people working on the wallet hope to bring about, which includes a new social role for citizens.

5.4. Empowering citizens?

> *'If implemented well, this is going to change everything. If not, a few tech companies will rule the market'* (Panellist, Identity Fair, November 2022).

The future role of user-citizens is closely related to the sociotechnical imaginary of 'control' that I described in the previous chapter. Namely, more 'control' to individuals is meant to establish a new relationship between the individual and powerful actors, such as states and companies (Giannapoulou, 2023). In this new environment, user-citizens are expected to manage their credentials, making responsible decisions about the sharing of their data. The arrival of the EUDI wallet is not only the implementation of a new technology; citizens themselves are expected to transform as well (see e.g. Schou and Hjelholt, 2018). As I will show, this shift in 'control' is often described as empowering for citizens. However, while there could be empowering potential for some, it is also important to critically examine the implications of this shift, because credentials will contain 'high quality', verifiable data about various aspects of people's lives. This opens up the possibility to profile citizens with a new degree of accuracy. This is particularly important because this shift in 'control' is happening in a context where there are many 'data hungry' actors (Meijas and Couldry, 2019), and storing as much data as possible has become the norm (Fourcade and Healy, 2024). Therefore, as I will show, the possibility of a new market, where citizens more explicitly consent to the sharing of their data in exchange for financial perks, emerges. This means, I argue, that user-citizens are expected to be entrepreneurial actors who are able to make smart data-choices.

The discursive relationship between 'control' and 'empowerment' becomes clear in various communications around the EUDI Wallet. For example, in a written statement about the EUDI Wallet, Romana Jerković, rapporteur on this file, remarks:

> 'With the European Digital Identity Framework, we want the EU to become the first global region with a governance framework for trusted digital identities. The Digital Wallet will become a reliable, all-in-one identity gateway that puts citizens in full control of their own data and gives them the freedom to decide exactly what information to share, with whom, and when. From social, financial, medical, and professional data, to contacts and much more, it will make it possible to store personal credentials within a single digital ID. Digital identity is no longer just a nice-to-have feature, but a new driver of civic engagement and social empowerment and a tool for an inclusive digital Europe' (European Parliament, 2023).

This shows the relationship between 'control' and 'empowerment' in relation to the intended scale and scope of the project. It is important to note that this focus on (control over) personal data in different areas is remarkable, as this is a state-issued identification system. As such, this identification system goes beyond traditional functions of creating administrative data to make citizens 'legible' to the state (Lyon, 2007; Scott: 1998), and is more closely related to newer

conceptions of datafied citizens, where citizens are (in part) constructed through their data traces (Hintz et al, 2018; Barassi, 2019). The fact that the EUDI Wallet is bringing this together, and also aims to provide a solution for the exploitation of a wider range of data, is new. This shows another facet of changing identification practices, where ('control' over) data comes to play a more important role.

The relationship between 'control' and 'empowerment' was a recurring theme in the responses of my respondents. For example, Aidan, researcher for the EU on the topic of SSI, tells me in an interview:

> 'I think it's going to revolutionise Europe, and really enable to move to - if the proposal to amend the eIDAS regulation is voted in in its current form and it's not watered down[14] - I think it's really going to enable us to move to a single European digital market and empower citizens to really… You know, it'll make GDPR not a bad thing, but an empowering thing, so it's not going to be like "oh, shit, we need to deal with that," but it's going to be like "oh, great, because of this I control my own data!"'

This shows again that the underlying hope is that controlling data will empower citizens. Furthermore, in linking the GDPR to the EUDI Wallet, Aidan signals the protection of personal data and the importance of consent, which, he believes, will be more manageable with the wallet, as citizens will make a more active choice about the sharing of their data. It should be noted, however, that the GDPR has been criticised for its effectiveness; personal data is still being collected and sold (Burgess, 2022), and the GDPR is not often reinforced (Access now, 2023; The Irish Council on Civil Liberties, 2023). In addition to these procedural concerns, there has also been a more general ongoing debate about informed consent mechanisms in the digital sphere, and whether consent is meaningful if people do not read or do not understand the terms they are agreeing to (Barocas and Nissenbaum, 2014; Joergesen, 2014; Custers, 2016). I will address these concerns more extensively in the next section of this chapter.

For now, it is important to stress that the empowerment narrative is echoed by interviewees working more narrowly on SSI technology. For example, Jack, SSI consultant, thinks:

> 'It's absolutely empowering because of these […] fundamental things that…it's data about me, that I control, that I can choose to use when I choose to use it, with whom I choose to use it, and nobody else can use it on my behalf without me knowing, without me being part of that sort of discussion.'

As these quotes show, the concept of empowerment is often linked to the ability to exercise choice and control over personal data. This, I argue, should be seen in light of the thinking where 'data' touches on the very idea of knowledge and what we can know. Nearly ten years ago, Van Dijck (2014) suggested that we were entering a new paradigm of what she termed

[14] This interview was conducted at a time when the legislation had not yet been passed.

'dataism'. According to her, the turn towards data collection and analysis on an unprecedented scale has ontological and epistemological implications, because it changes the idea of what we can know and how we can act on that knowledge. More specifically, dataism assumes a relationship between data and people, which forms the basis for the prediction of future behaviour (Van Dijck, 2014). Importantly, as Fourcade and Gordon (2021: 80-81) observe, also states embrace this worldview, applying a 'dataist philosophy of governing', which is built on the idea that 'society consists of data flows.' Therefore, the very emergence of datafication (Cukier and Schönberger, 2013; Meijas and Couldry, 2019), where everything can be turned into data, has led to different ways of interpreting the social world. Therefore, while the EUDI Wallet is attempting to redirect the control over data, it simultaneously consolidates the idea that there is an inherent link between data and people, as it solidifies which types of data belong to whom. Namely, in the form of credentials, data is made 'verifiable', and is thus seen as 'proof' that a person is who they claim to be.

It is important to be critical of this status that is given to data; as critical data scholars remind us, data is 'never raw but always cooked to some recipe' (Kitchin, 2021: 5). In other words, data is not something neutral, that is sitting out there waiting to be harvested, but should rather be seen as something that is actively produced - and the end product reflects decisions made by people (Kitchin, 2021; Iliadis and Russo, 2016). Or, as Sadowski (2019: 2) puts it: that 'see[ing] the world in a way that asserts "everything is data" does not just *reveal* or *reflect* the world […] [but] *order* and *construct* the world' [emphasis in original]. Therefore, data exerts power, as it says something about how the world is constructed and interpreted, and who is doing this interpreting (Iliadis and Russo, 2016).

What is more, the ubiquity of 'data' has also led to its commodification: the 'surveillance capitalism' (Zuboff, 2019) which, as I mentioned, SSI technology is supposed to counter. Data presents an important economic incentive and opportunity: for example, Birch, Cochrane and Ward (2021) argue that Big Tech companies have transformed personal digital data into a new 'asset class', where personal data has been framed as a 'critical political-economic resource of the future' (Birch, Cochrane and Ward, 2021: 2). Assetisation, the process of transforming a resource into an asset, i.e. capitalised property (Birch and Muniesa, 2020; Birch, Cochrane and Ward, 2021), makes it possible to see personal data as a source of revenue. This, they argue, is done through a process of 'techcraft', where personal data has to be made legible and measurable (Birch, Cochrane and Ward, 2021). Furthermore, much of the current digital economy is based on the premise that individuals can access a service for free, but effectively pay with their data (Zuboff, 2019; Sadowski, 2019; Fourcade and Kluttz, 2020). SSI technology is supposed to mitigate this: as individuals will have to consent to the sharing of their data, it is supposed to prevent entities (such as online platforms, but also states) from simply taking data. As Christoph explains to me in an interview:

> 'To avoid this surveillance capitalism, so that that I can log into websites with my wallet instead of with my Facebook account. Right? A lot of people, a lot of websites where they say "log in with Facebook", and you log in with Facebook with a lot of websites. And if,

> instead of that, I log in with my digital wallet, and that's much more privacy preserving. And that's great. Yeah, that so that's definitely part of the idea why this whole concept of self-sovereign identity and decentralised identity was started a few years ago, to help improve the situation.'

However, as Olivia, another SSI expert, points out, it is difficult to do this right, because people are very used to getting everything for 'free':

> 'I have spent many years with many companies resisting the temptation to offer an enhanced digital identity service to some users that enable them to, instead of having a free service, have a paid-for service, but have additional privacy controls. But as consumers we're doped up on the idea that we should have everything for nothing. Think about the compromises you make on your personal privacy for utility, think about how much you use G-docs and Google for searching and all the other free applications – they're only "free" because…free in terms of the money you spend, because you're sharing lots of data that they can then sell, effectively. So there's an imbalance there, you know. The reason you have to resist that temptation is because if privacy is only accessible for those who've got money to pay, then that drives further inequalities…but it's really a structural problem in the market as opposed to with digital identity.'

This highlights that a problem arises from the fact that people are now used to having access to free services, which raises the question of how to remedy the data harvesting problem without asking people to pay. As Fourcade and Kluttz (2020) show, there are some projects that aim to compensate people for either their data or their labour. However, they suggest that, ironically, this 'liberation from free services often relies upon users being enrolled into new systems of payment', as this only creates a new market (Fourcade and Kluttz, 2020: 11). Importantly, the EUDI Wallet could facilitate a similar situation, where data can be exchanged for benefits like discounts, thereby inserting market-logics into processes of identification. This is important, precisely because credentials contain 'high quality', verifiable data. Because of its 'verifiability', this data is valuable. I discussed this topic with Max, another SSI expert, whom I asked whether it would be possible for companies such as Facebook to ask people to share more data, in exchange for benefits. He answered:

> 'Yes, of course, in practice that's something which is happening already, and we will also see that happening in the future. However, it's still it's my decision, right. And in the end, it's about practical usage, and in the day-to-day business, or day-to-day use cases, right, and the idea and the hope which we have is that we can provide the same level of convenience […] to the users of the wallet, with way higher privacy and control. And then, of course if they want to share additional data to get some benefits and perks whatsoever, offered by company, they're free to do so, but they don't have to, right, and that's kind of the additional control aspect which we would like to introduce in order to make the individual more sovereign about what data they share, and not, for example, just click "accept all cookies".'

Therefore, importantly, while 'empowering' citizens by shifting 'control' to them, this simultaneously creates the possibility of a new market, where citizens exchange their personal data for financial perks. Therefore, SSI technology and, by extension, the EUDI Wallet may not radically subvert the system where data is commodified, but rather contribute to a new market where personal data is traded for perks. Aidan also fantasised about the future and the financial opportunities:

> 'I create my own ID, I have data points relating to me, I can choose who sees what data points, who sees what attributes, who gets what data, and enables me to monetise data or not monetise it, share or not share. It really puts the user back in control of their own data. Or, for the first time!'

Therefore, 'empowerment' is not just about choice to share or not share data, it could also create new market structures, where citizens exchange their data for money or other perks. As such, this data may become a form of capitalised property as well (Birch, Cochrane and Ward, 2021). The difference is, however, that not (only) companies or data brokers are in charge of monetising data; but rather citizens themselves. Because of this, I argue that user-citizens are expected to be entrepreneurial, and able to make smart data-choices. They will need to decide which data they are willing to share, and whether they want to try and exchange it for perks and benefits. Therefore, they will effectively have to decide on the terms of their own datafication and commodification of their personal data.

As I will suggest in the next part of this chapter, this is not without risk: not everybody can be expected to have the time and resources to manage their credentials, which could lead to exploitation of vulnerable groups. This is particularly serious because credentials contain 'high quality' data. In other words, while 'control' can be empowering and positive, it could also be detrimental for populations who are not as digitally literate or do not have the time and resources to make these decisions.

However, before turning to this, it is important to note that in the case of the EUDI Wallet, there are limitations to the amount of data service providers (so-called 'relying parties') are allowed to ask for, as well as to the kind of data citizens can refuse to share. In some cases, there are legal requirements about the necessary data. For example, banks are required to perform Know Your Customer (KYC) and Anti Money Laundering (AML) checks, which obliges them to request data to verify identities, and prove that they are operating above board (GDPREU, 2022). In a similar vein, government-led public services, such as tax agencies or social subsidy agencies, are also likely to need a base level of personal data to be able to perform a service. On the flip side, relying parties are, in accordance with the GDPR, only supposed to ask for the data they need for a particular transaction (Regulation (EU) 2014/83). Importantly, however, they can ask for more than what is essential, as long as citizens consent to it. For this, several of my interviewees explain, relying parties will need to make explicit that sharing additional data is optional. Marta, who works for a tech consultancy, explained to me that data minimisation will be an important aspect of the EUDI Wallet:

> ‘One of the most important parts of the regulation will be around data minimisation […] We expect to see guardrails in place that will require service providers to only ask the minimum amount of data required to provide a service. If they want to ask anything else then […] it will need to be very clear to me as a consumer what is actually required to access the services, and what is the extra information that the provider would like to have. But I can simply refuse to share it, so that is quite empowering.’

In other words, relying parties will need to be very explicit about which data they need, and which data would be supplementary. The user-citizen is then expected to make an informed decision. As a follow up question, I asked Marta whether this would mean that companies would still be allowed to ask for more, in exchange for benefits. She answered:

> ‘I mean, you cannot forbid these things, right, it is businesses’ right to ask these things and to provide those personalised offers. But that's where the empowerment comes from. You know, I have a choice, and I know what I'm getting in return, and that's a very, very interesting example, because that can potentially create… instead of businesses trying to track some cookies that are not great, gather some metadata that is not always reliable, and try to second-guess how we can do some personalised marketing, they would be able, as you said, to actually ask individual directly: “Hey, would you mind please sharing these additional preferences, so these bits of data with us, we will give you some discount in return, and for us it will help to do better marketing campaigns, right?”’

This indicates that empowerment is not only tied to personal choice and control; there is an implicit suggestion that enhanced control can be used to benefit financially as well. I argue that ‘empowerment’, then, also refers to the ability of citizens to assert themselves through their choices about the commodification of their personal data. This produces a view of the user-citizen as an economically savvy subject; an entrepreneurial citizen who can pick and choose what to share, and capitalise on financial opportunities. This user-citizen is empowered to say ‘no’, when they do not want to share additional data, which presupposes that they have the time and resources to think about data choices. Therefore, the EUDI Wallet has some neoliberal qualities, as citizens are seen as entrepreneurial actors who are responsible for their own success (Brown, 2016). Matteo, whom I cited in the beginning of this chapter, also spoke about the circumstances under which asking for more data would be allowed.

> ‘Isadora: so, hypothetically speaking, if Facebook were to ask for more data than is absolutely needed, would that be allowed?
>
> Matteo: They can. They have to justify. They have to say the finality; they can't hide behind, you know… […] Why do they need to know the name of my mother? Why do they need to have my telephone number? So they have to justify. And then I decide. “Yes, I mean for the purpose, yes, I agree”, but then they are responsible for the acquisition with the finality. So if they give the telephone number…to a relying party for the purpose of, I would say, security, I should not be receiving communication via the telephone number for

> instance. So the engagement will be based on the declared finality, which is not generically security. You see what I mean?'

In other words, it will be possible for relying parties to ask for more data than strictly necessary, as long as they tell the user-citizen what it will be used for. It is important to note that it is not only people working in the private sector, who see the potential of the exchange of data for perks. Frederico, one of the members of the eIDAS Expert Group, discusses this topic as well. Using me as an example, he tells me:

> '[Imagine] Isadora doesn't trust the relying party, but Isadora trusts eIDAS, that's a federation, a system, an infrastructure. And well, Isadora's wallet will ask to the trusted third party "do you know cinema.org?", and the trusted third party will give you the proof. "Yeah, I know it…it is complying", and […] it only can ask to you, this predefined set of things. If it will ask more than those, well, it's up to you…if you are willing, decide to share. Because you control. […] Well, the relying party may exploit the process with some benefits, like, if you will share your email […] I can give you a coupon, and for sure that will work. But the most important is the willingness, the will of the user, is that drives this process.'

This shows again the emphasis that is placed on the 'user': they are expected to make this decision, as they are in control. In this example, Frederico refers to the fact that there will be a registry of trusted relying parties that are known to the system, which means that the wallet can tell wallet users whether a particular party has been through the registration process and can be trusted (De Rosa, 2024). This is expected to minimise rogue actors trying to exploit citizens. At the same time, relying parties can ask for more data in exchange for a benefit, such as a coupon.

By obliging relying parties to register, the EU has chosen to insert a level of control and protection, as not just any party can join and ask citizens for their data. This speaks to the difference between 'pure' SSI technology and the EUDI Wallet; in its original formulation, SSI would not introduce a layer of additional protections, as the technology is supposed to make individuals 'self-sovereign': they are solely in control of this decision. However, in the context of EU states, there is a question around the responsibility of states, and whether citizens need to be protected. This question is significant, as the EUDI Wallet will be able to store all kinds of sensitive information, ranging from passport information to health records. As Andreas, another eIDAS Expert Group member, tells me, this was a bone of contention during the development of the technical specifications:

> 'There are, let's say, from a from a bird's perspective there may be two streams. Stream one is: if it is based on user consent, why not? That would be an approach where the followers of those of that approach would say, "well, who is the government or the issuer of a wallet to explain me as a citizen, what I want to share - it's my data - with whom?" So that would be the approach, "as long as there is consent, it's my choice, and if I want to share my complete health record with Google, why shouldn't I?" On the other hand, there

> are streams saying, "well, for some data there may be state responsibility, as private sector or gatekeepers, or the Big Techs may even exercise some pressure in terms of social pressure, that…to consent." So that's for some categories of data, let's take extreme examples like a stigmatizing information, in particular from the health sector.'

This shows the tension between full 'control' and the responsibility that states have vis-à-vis their citizens: to what extent is full control desirable, and how to mitigate the potential abuse of the system by Big Tech companies, are important questions related to larger power dynamics, and the extent to which we can really expect the EUDI Wallet to subvert these. In its 'purest' form, SSI technology would be in line with the first stream of thought, as this would make citizens completely 'sovereign' over their data. However, in the context of the EU, this raises more questions, which pertain to the duty of states to protect their citizens. This shows an important difference between users of the internet and citizens of a state.

When this interview was conducted (December 2022), it was not yet clear what the final legislation would look like. At the time of writing, the legislative text has been finalised (European Council, 2024), and includes protections for citizens. It states that relying parties that want to use the EUDI Wallet will have to register, and will have to declare their intended use of the wallet, as well as the types of data they intend to request. Furthermore, there are safeguards for special categories of data (defined under the GDPR), such as health data, that are supposed to guarantee the lawful processing of these types of data (Regulation (EU) 2014/83). The registration process, therefore, will most likely make it difficult for relying parties to request special categories of data. However, practice will show whether this will indeed be adhered to. In addition, other, less protected data, such as email addresses (mentioned in the example above) can more easily be exchanged for monetary benefits. As such, this has the potential to bring about a market where citizens more explicitly share data in exchange for benefits such as discounts.

5.5. The 'ideal' digital user-citizen

> *The session about the EUDI Wallet was packed. A group of developers working on the technical specifications of the wallet answered questions. 'Trust', the role of governments, the level of assurance with which persons can be 'verified' were all popular topics. One of the main questions was, however, whether "verifiers can only ask about certain claims" (whether service providers can only ask for specific and limited data). "There are discussions about that", the main consultant to the EU Commission on this topic answered. "But in my opinion", he continued, "the wallet is not the policeman of the GDPR".'* (Radical Identity Meet-up, Switzerland, June 2023).

As I have argued above, the EUDI Wallet is beginning to craft an independent, entrepreneurial, tech-savvy 'user-citizen'. This is happening in a context where the EUDI Wallet is – through the

process of credentialisation- bringing together different social institutions and social roles. It is important to see the user-citizen in this context, as the scope of the wallet makes the question whether citizens will be able to perform in these systems more pressing. What is more, the EUDI Wallet is not only a means to control personal data; it is linked to access to essential services, and therefore social rights and participation in society. Crucially, therefore, if digital literacy, skills, and access to technology, are not scaled in conjunction with this, it is essential to question what the wallet really has to offer.

While being able to make choices about the release of personal data can be empowering, it also places more responsibility on citizens. Not everyone might have the digital skills, time or financial resources to engage with this system. In other words, it is questionable whether it will be more inclusive to everyone. For example, Fourcade (2021: 8) has observed in the context of the digital rankings and measuring systems (ranging from physical fitness to credit scores), that the consequence of these systems is that people are not supposed to merely strive to be included into these systems, but are expected to *perform* well in them too. As such, she argues that 'the move toward financial and digital inclusiveness is producing newly actionable social divisions, social duties and forms of capital that shape people's life trajectories in multiple ways' (Fourcade, 2021: 5). This 'performance' aspect brings out a crucial point, which is that it is increasingly the responsibility of individuals to make the 'right' choices on how to engage with digital systems. Consequently, there is a limit to the access and increased inclusivity that digital technology can provide, as gaining access to the digital system is only the first step.

I argue that the EUDI Wallet presents a rather individualistic conception of citizenship, where citizens are responsible for themselves and encouraged to 'control' their own data and access to services. This ties in with recent trends in data rights: for example, legal scholar Salomé Viljoen (2021) has looked at what she terms 'individualistic remedies' to data rights. She argues that data-governance law that aims to give individuals more control over their data, be it by giving them a more control over 'the terms of their datafication' or wanting to have individuals benefit financially from the data they generate, fail to recognise a crucial point: the relational aspect of data. The core argument that Viljoen (2021: 4) makes, is that data collection practices by powerful tech companies are not interested in deriving information about specific individuals, but rather in generating 'population-level insights regarding how data subjects relate to others.' These insights can be applied to all persons that fall in a particular group, which shares some of the same characteristics. Writing in the context of the United States, she contends that most data reform proposals see the effects that the data economy has on a population-level as a consequence of eroded individual data rights. Therefore, she argues, the 'individualist remedies' which new legislation proposes, will not address the harms that occur on the population level. In other words, according to her, legislation should move past the focus on individual rights and control, and towards a collective, institutional approach to data governance (Viljoen, 2021: 4-5). Crucially, she points out that 'individualist theories of informational interests result in legal proposals that advance a range of new rights and duties with respect to information, but practically fall back on

individuals to adjudicate between legitimate and illegitimate information production' (Viljoen, 2021: 8). Therefore, putting individuals in charge of controlling 'their' data, risks making them responsible for making the right data-choices as well as the harms that could arise from it. Similarly, as Hintz (2022: 96) points out in regard to comparable individualistic approaches to data management, there is a risk that these policies '[transfer] a societal problem to the realm of individual lifestyle changes.' In other words, while the data economy and the harms it generates are a societal issue, solutions are often sought at the level of the individual.

The EUDI Wallet runs this risk as well: making data-choices such an integral part of the EUDI Wallet introduces the risk that not everyone might be able to perform equally well in this system, thereby creating a situation where some citizens are more successful in guaranteeing their privacy, generating benefits off their data, and accessing services than others. This individualistic approach suggests the influence of neoliberal logics (Schinkel and Van Houdt, 2010), where citizens are 'responsibilised' (Brown, 2016: 9) for their own success. Crucially, while the EUDI Wallet could be empowering for some tech and data-savvy citizens, it is plausible to assume that not everybody possesses the data literacy and resources to make these decisions. This is particularly important because the EUDI Wallet is not only a means to control data; it grants access to different kinds of services that are necessary to participate in the (digital) society.

Therefore, it is essential to consider who this wallet is for. Oudshoorn et al. (2004; 2016) argue that technologies are often developed with particular user representations in mind. However, they point out, these often fail to include users from various gender and racial backgrounds, as well as differences in skills and interests among users. As a result, there is a risk that new technologies are presented as empowering for everybody, but are really only developed with one group of users in mind. As more and more aspects of society are being digitised, scholarship on the digital divide has shown that differences in social, cultural, and material resources lead to digital inequalities (Van Dijk, 2020; Kaharevic and Skill, 2021). Van Dijk (2020: 85) shows, for example, that the digital divide 'tends to reflect and reinforce existing social inequality.' Similarly, Hargittai (2018) finds that people's socioeconomic status, as well as age, gender, disability and ethnicity influence the way in which they access and experience technology. Therefore, when a particular 'user' is 'expected', there is a risk that any other groups that fall outside of this vision, will be excluded. This exclusion can occur across different dimensions, relating, for example, to both access to technology as well as digital skills. These are sometimes called the first (material access to internet and technology), second (internet-related skills and usage) and third (who benefits most from this access) level digital divide (Van Deursen and Van Dijk, 2019).

A concrete issue, related to the first level digital divide, is the hardware (the phones) that is required for the EUDI Wallet. Antonio tells me that a particular type of hardware is needed to meet the safety requirements ('level of assurance high') for sensitive data:

> 'That requires the hardware ready, so the phones…the smartphones to be ready to do that, and or a remote architecture for that, and this is not yet there. […] What I want to

> say is that the market needs also to be ready for that, and we are not there. So it is not just about the regulation and the member states, and so on and so forth, but also the market is not - most probably because of this level of assurance high – they are not ready to...but they are getting there. The private sector is really excited about this approach.'

In other words, this means that that citizens will need a new type of smartphone to be able to use the wallet. As not everybody may be able to afford a new phone when the market is ready, this can create a situation where financially precarious groups cannot use the EUDI Wallet, which means that these groups are excluded from accessing the digital services that it provides. This has the potential to reinforce existing citizenship hierarchies (Castles, 2005), and even create new ones, where citizens with lower incomes do not have the same access to services as higher income groups.

It is important to note, however, that the legislation states that the EUDI Wallet is not mandatory and is supposed to be non-discriminatory, meaning that citizens should be granted access to the same services if they choose not to use the wallet (Regulation (EU) 2014/83). Therefore, the legislation works to guarantee the same access to services for all. However, at the same time, there is still a risk that the EUDI Wallet will become the de facto new infrastructure, and alternatives will be harder to gain access to. For example, a similar transition occurred in the banking space, where individuals can technically still go to the bank, but 'offline' banking has become harder as many local branches have disappeared and it sometimes incurs additional costs (Chakravarty, 2006). Peter, for example, is not convinced that there will be equal alternatives. He tells me:

> 'There is a pretty heavy nudge to digital processes; it doesn't make much sense to say "it won't be mandatory," because people will be pushed into it anyway.'

In other words, there is a risk that it will be hard to 'escape' using the EUDI Wallet as it might become the primary way to easily access services. For this reason, it is important to consider issues related to the second and third level digital divide as well, and address the topic of digital and data literacy. As debates on consent on the internet have shown, the fact that people consent to the sharing of their personal data, does not always mean that they understand the terms and conditions. For example, as Hintz (2022: 95) points out in relation to the GDPR, the idea of the 'informed user' is not as clear-cut as it seems. While more individual control over data can give individuals the tools to manage their own data preferences, the impact this will have may be limited if individuals do not have the knowledge and skills to use these tools. Similarly, Brunton and Nissenbaum (2015: 3) observe an 'information asymmetry', where 'data about us are collected in circumstances we may not understand, for purposes we may not understand, and are used in ways we may not understand,' while Edwards and Veale (2017) point out in the context of consent on the internet, that the burden of privacy is completely placed on the individual. Furthermore, Draper and Turow (2019: 1825) note that even if users have some control over their data, they often feel 'digital resignation': even though they are unhappy with extensive consumer surveillance practices, they feel that it is inescapable. In light

of these studies then, it is important to be critical of the 'empowering' potential that the consent mechanism in the EUDI Wallets really holds.

This is particularly if digital skills are not scaled alongside the implementation of the wallet: while it may be empowering for people who are very informed about data practices, it is unlikely that everybody will possess the necessary data skills. Namely, as scholars working on data literacy have demonstrated, there is an important difference between knowing how to use digital tools on a technical level, and engaging with them in a critical way (Pangrazio, 2016; Pangrazio and Selwyn, 2019; D'Ignazio, 2016). As Pangrazio (2016: 165) argues, the difference between 'technical mastery' and 'critical mindsets' is crucial: if we acknowledge that digital technology is more than a tool, and part of a complex social-technical system, people require to be able to think about digital technology and data reflexively. In other words, if this critical reflexivity is not present or scaled, it is questionable whether the EUDI Wallet will indeed have the empowering potential that it claims to have. Therefore, tasking citizens who do not have the required data literacy with the responsibility to distinguish between 'legitimate and illegitimate information production' (Viljoen, 2021: 8) could lead to digital inequalities. This is especially important because the wallet is not just a tool for data management, it also gives access to essential services.

Eurostat (2022) statistics show that within the EU, there are significant differences between the digital skills across member states. For example, while The Netherlands, Finland and Ireland score high on 'basic digital skills', with 79% of the population for the first two and 70% for the latter, other countries, such as Bulgaria, Romania and Poland score lower, with 28%, 31% and 43% of the population respectively (Eurostat, 2022). Overall, the data shows that 54% of the European population has basic digital literacy skills (Eurostat, 2022). This is significant, for it means that nearly half of the population does not possess these skills. What is more, some marginalised communities, such as the Roma people, score still lower in terms of digital skills (Dira, 2023). Therefore, there is a risk that inequalities and hierarchies in terms will emerge, where the data literate and financially stable will be able to enjoy the privileges of the wallet, whereas less data literate groups are more vulnerable to data exploitation and may find it harder to gain access to services.

What is more, in addition to differences between citizens from different EU states, the EUDI Wallet risks (re)producing differences and hierarchies among non-EU citizens as well. This is not only in terms of digital skills, also in terms of who is included in the wallet: while official residents are entitled to access to the wallet, the legislation does not account for refugees and migrants who are in the EU 'illegally' or still awaiting their status (Schoemaker et al., 2023). In other words, the EUDI Wallet might also have differential impacts on non-citizen groups, such as 'alien' residents, (undocumented) migrants and refugees, for these groups are not considered in the design. Consequently, it is unclear whether these groups will have access to the same services. What is more, it is also uncertain who is responsible, as there are no overarching European rules on identification mechanisms for (undocumented) migrants and asylum seekers. A recent report by the Organization for Migration (IOM) (2023) suggests that identification mechanisms for migrants, refugees and asylum seekers are primarily organised

by member states, which means that there is differential access to e-government services across the EU. What is more, while the report does not extensively consider the EUDI Wallet, it does suggest that there is scope for extending the system to migrants, where the process of issuing credentials needs to be contemplated (IOM, 2023). Importantly, however, this means that, as it stands, the EUDI Wallet excludes these groups, and could further entrench differential treatment and barriers to access.

In sum, there is a risk that a substantial part of the population will not be able to use the EUDI Wallet in the way that it is envisioned. These differences have the potential to play out both at the individual level, as not all citizens might be able to afford a new phone or have the data literacy to use the EUDI Wallet, as well as the country level: as there are significant differences in data literacy across states, the wallet might create new hierarchies in terms of data literacy, privacy and access, where citizens in less digitised societies will be at a higher risk of data exploitation and not being able to access essential services. Finally, the fact that groups such as alien residents, (undocumented) migrants and asylum seekers are not included, could pose significant barriers for these groups, and reinforce differential access.

5.6. Conclusion

This chapter interrogated the new role that citizens are supposed to take up in the EUDI Wallet. It first showed the connection between digital identity and digital citizenship: I find that digital identity is seen as a means to grant access to services, and thus as a key element for participation in the digital society. This ties in with older processes of identification, as 'proving' who someone is, is seen as a prerequisite to membership and access to rights and privileges. At the same time, the EUDI Wallet also extends traditional state-issued identification mechanisms, as the process of credentialisation brings different aspects of people's lives together in one wallet. This, I argued, also means that citizens are expected to take up a new role, as they have to manage these credentials. As such, a 'user-citizen' emerges, blurring the boundaries between users and citizens. These blurring boundaries could in part be attributed to the fact that SSI was originally an internet identity model, designed for users. Suddenly, 'user' behaviour, such as consenting to the sharing of personal data, is being applied to citizen 'transactions', as this becomes part and parcel of gaining access to services. This, I showed, is directly related to the sociotechnical imaginary of 'control', where more control over personal data is seen as 'empowering'. As citizens will have to manage a wide range of credentials, containing high quality, 'verifiable' data, they are expected to be tech-savvy, entrepreneurial, and able to decide on the terms of their own datafication. This is particularly important because there is an insertion of market-like logics into the realm of identification: due to the wide scope of the wallet, the possibility of a new market, where citizens can consent to exchanging their personal data for perks, such as discounts, arises. While this may be empowering for some, there is a risk that not everybody will have the resources, time, or digital literacy to make decisions about the sharing of their personal data. Therefore, if data literacy, skills and abilities are not 'scaled' alongside these developments, it is important to question

what is really on offer in the wallet. Ultimately, there is a risk that new hierarchies between groups with varying degrees of data literacy, skills and access to legal documentation will emerge. In sum, therefore, this chapter helped show that the shift to wallet-based identification systems is more than just a technological change; it includes a societal change as well, with a new role for citizens.

Chapter 6. The politics of standards: how global power battles are reflected in tiny technicalities

> 'As momentum increases to digitise all physical credentials, standards are solidifying making interoperability more likely (though not guaranteed!). It's still quite messy at the moment, but things are getting better and I hope the "religious fervour" of one protocol over another dies down soon' (Tobin, 2023).

6.1. Introduction

According to Bigo et al. (2019: 4), it is essential to look beyond 'political struggles over data production and its deployments,' and explore 'how data is generative of new forms of power relations and politics at different and interconnected scales.' In other words, it is important to interrogate the world behind data production as well. In the previous chapters, I argued that credentialisation changes identification practices, collapsing various social institutions and social roles. In doing so, I addressed the changes in power and 'control' over data that the EUDI Wallet aims to bring about. In this chapter, I extend this, by looking at power dynamics on different (and interconnected) scales: I zoom in on the global power struggles over the design of digital ID wallets. In particular, I investigate the 'technical standards', the requirements and specifications that are supposed to make sure that 'products are fit for their purpose' (National Science Board, 2018: 1). I do so because standards show how 'the big and the small' (De Goede, 2016: 362) are connected: global power battles are reflected in tiny technical standards.

By applying a *transversal perspective*, it becomes possible to look at the power of different actors (the EU Commission, technical experts, the SSI community, Big Tech companies) on different scales (Nogueira, 2017; Basaran and Guild, 2017), and begin to sketch out this space, showing that these power dynamics are not straightforward. I therefore argue that sites of power around (the development of) identification systems are shifting, as different actors have 'different power' (Avelino, 2021). Namely, the EU has the 'transformative' power to regulate, while Big Tech companies have the 'innovative' power to quickly develop new technologies (Avelino, 2021). As I will argue, actors like states and Big Tech companies sometimes compete, and sometimes work together. As such, on top of the shifting assemblages that are involved due to credentialisation – as the EUDI Wallet will give access to many different services - this chapter addresses another way in which power dynamics around identification have become more diffuse. Therefore, I argue that power over identification systems does not reside exclusively with states, but rather flows in various directions. This is significant, as identification was traditionally within the purview of the state.

First, I show how the development of the EUDI Wallet is closely linked to the Covid-19 pandemic. This state of emergency gave rise to a need for more and quickly developed technology, which resulted in a competition between the EU and Big Tech companies over technical standards. I then show how this is related to the involvement of technical experts in

the development of the EUDI Wallet, as they are meant to develop the technical specifications for the wallet in an accelerated fashion. This means that the legal and technical process are happening in parallel, giving technical experts indirect influence over the legislation. I then turn to the so-called 'wallet wars', showing that as Big Tech companies sometimes compete with states, and sometimes work together with them. In the final section I expand on this theme by focusing in on the standardisation of credentials, showing that this reflects larger power battles.

6.2. The Covid-19 pandemic as catalyst for digital (identity) technology

As I have argued throughout this dissertation, identification was traditionally 'done' by the state, but is now changing in a multitude of ways. One envisioned change is that SSI technology is meant to subvert power relations between state and companies on the one hand, and citizens on the other. However, it is crucial to address the power dynamics below the surface as well, surrounding the design of the wallet. This shows, I argue, that there are shifting assemblages of actors involved in the design of digital ID wallets, which sometimes work together, and sometimes compete with one another. In this section, I address the relationship between the development of EUDI Wallet and the Covid-19 pandemic. This is necessary, because it shows that the way in which the EUDI Wallet came about is heavily influenced by the power struggles between the EU and Big Tech companies- commonly understood to comprise of Apple, Amazon, Microsoft, Alphabet/Google and Facebook/Meta (Birch and Bronson, 2022) - surrounding Covid-related apps, such as contact tracing-apps.

Before the Covid-19 pandemic, researchers had already noted that tech companies were moving more and more into the realm of public services, to the extent that global private (tech) companies can increasingly be seen as 'social actors', delivering public goods (Brühl and Hofferberth, 2013; Magalhães and Couldry, 2021). The pandemic accelerated this development: because most work and social interaction had to be moved online, individuals found themselves increasingly reliant on digital infrastructure, which was – due to their rapid implementation - sometimes not fit for purpose (Bodó and Janssen, 2022). For states, this was challenging too, for they suddenly had to adapt to the digital world as well, something that not all states were equally prepared for. In the field of digital identity, scholars have argued that the pandemic has served as a legitimation tool for the rapid implementation of digital identity systems world-wide (Masiero, 2020; Martin, 2021). Martin (2021: 105) goes as far to suggest that it has 'provided advocates of digital identity systems with a new crisis through which to promote and legitimize identification systems.' The EUDI Wallet fits into this trend: the legitimation of the project as well as the fact that it was supposed to be rolled out very quickly can in part be attributed to the pandemic.

This can be traced back to new systems that were specifically designed in response to the pandemic: Covid contact-tracing apps and vaccination passport apps. The main concern around these apps was that they could help states engage in (ever-expanding) surveillance

practices, as they involved a scaling up of data collection (Sharon, 2021). However, as Sharon (2021: 46) notes, '[i]n an interesting twist, the tech giants came to be portrayed as greater champions of privacy than some European governments,' as privacy experts were unexpectedly excited about Google and Apple's contact tracing API. As such, Google and Apple suddenly became responsible for the delivery of an important public service in times of crisis. According to Sharon (2021), this should be seen as part of a larger trend, where tech companies are encroaching on different spheres of life, such as medicine and politics. Others have noted these trends as well: for example, building on Naomi Klein's (2020) often-cited article on the free rein that some Big Tech companies were given by governments during the pandemic, Hendrikse et al (2022) point to the fact that Big Tech representatives were invited to the White House, Downing Street and Brussels, to discuss the rapid digitalisation of society. This all raises questions about the legitimacy of technology companies, as they gain what has been called a 'state-like position' (Broeders and Taylor, 2017: 315) in terms of power, while they are not subject to the same level of accountability.

First proposed in 2021, the EUDI Wallet was proposed at the height of the pandemic (Proposal for amending Regulation (EU) No 910/2014, 2021). While the concept of SSI had been around for several years, it only started to gain more traction in the European Union at this time. Matteo, high-level civil servant for the EU, thinks that the EUDI Wallet was ultimately pushed forward by the pandemic:

> 'I think that Covid boosted the interest, of course, I mean, you can imagine also that the focus on digital services and the need to have, say, safeguards for the use of the digital data, not only in the public administration, but also in private sector, became also very important.'

Later in the interview, he specifies that the pandemic also instilled the idea that having a digital identity system is necessary for the continuation of society:

> 'Also in terms of ensuring that there is continuity of […] society is not only, I would say, more easily and more convenient way of engaging, it's really […] an opportunity for society to keep going, and also, if we can, to be so close to each other.'

While this goes back to the relationship between digital identity and participation, which I addressed in the previous chapter, it also shows that the EUDI Wallet is a product of its time and was well-positioned to capitalise on developments in the Covid-19 pandemic, as this reinforced the need for the digitisation of society. What is more, the accelerated fashion in which the EUDI Wallet was proposed and developed is likely influenced by the struggle over Covid-related technologies mentioned above. Charlie, the director of a European digital civil rights organisation that is critical of the EUDI Wallet project, spoke about the competition over technical standards for digital ID wallets between the EU and Big Tech companies in an interview:

> 'European lawmakers feel an urgency to be first, and not let Google or Apple decide what the wallet standards will be. The pandemic has shown them that on the question of exposure notification, so Covid-tracking, they have waited too long, and it was the smartphone operating system vendors that decided how this is done. With the Covid-certificate, they actually managed to be first, and so they feel like, "okay, we can be standard-setters, and the European law is better than companies deciding unilaterally how these important platforms should work." And the mobile driver's license ISO standard is already law in some US countries, and so it would be another reason why there is an urgency in their eyes to not be late to the party, basically.'

This suggests that the EU felt pressured to develop the standards for the EUDI quickly, because Big Tech companies had shown during the pandemic that they could take over the delivery of these services. In their research on the EUDI Wallet, Weigl et al. (2022: 78) also find that the Covid-19 pandemic was an accelerating force, as it enabled 'digital identity and electronic signatures to show their usefulness for the continuity of fundamental services of society', and the possibility to 'deal with public authorities remotely.' Another reason for acceleration that Weigl et al. (2022: 78) find is the pressure from large platforms:

> 'In particular the "huge pressure" from large platforms […] offering identification and authentication services to EU citizens for data exploitation purposes was confirmed as a large threat resulting in the importance and urgency for governments to act quickly and strategically […] The Council Conclusions on Shaping Europe's Digital Future, published in June 2020, further acknowledged the power of large online platform companies as gatekeepers in the digital economy to draw vast amounts of data […] A clear need was stressed to establish limitations that would "prevent these big entities from scooping out the identity data that would be available in [digital] wallets".'

This is particularly important, because digital ID wallet will include many different kinds of credentials. As such, acting quickly to be 'first' became important, for if the EU would wait too long, other, commercial initiatives might take over identification services.

The technical standards are important, because they determine (in part) how the technology will work and what it will be able to do. A technical standard is 'a document that provides requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose' (National Science Board, 2018: 1). Or, as the International Organisation for Standardization (ISO) (n.d.) describes it, standards are 'the distilled wisdom of people with expertise in their subject matter and who know the needs of the organizations they represent – people such as manufacturers, sellers, buyers, customers, trade associations, users or regulators.' However, while 'distilled wisdom' sounds positive, standards are not neutral: as Bowker and Star (2000: 49) point out, 'standards and classifications, however dry and formal on the surfaces, are suffused with traces of social and political work.'

One way in which this social and political work becomes visible is through the de facto competition between the EU, a political body, and Big Tech companies, which reveals the

immense power that some Big Tech companies hold. As the quotes above show, the EU is vulnerable to the speed with which Big Tech companies can develop technical standards and technologies. This is important, because it demonstrates shifting sites of power in regard to (the development of) identification systems, which was traditionally only within the purview of states. Looking at this from a *transversal* perspective, where power is not necessarily only tied to nation-states, but different kinds of actors such as local authorities, international organisations, experts, and corporations, are included as well, and these actors are operating at different scales (see e.g. Nogueira, 2017; Basaran and Guild, 2017), shows these power dynamics around identification in a different light. Namely, it is not self-evident that state-like bodies like the EU fully control identification systems anymore, as corporate actors like Big Tech companies have a vested interest in expanding into the realm of identification, as well as the power and resources to be a force to be reckoned with. At the same time, while it might be harder for the EU to develop technologies and standards; it does have the power to develop legislation. In terms of power, therefore, I argue that the EU and Big Tech companies have 'different power' (Avelino, 2021; Avelino and Rotmans, 2009). This does not necessarily mean that one controls the other, but rather that they are mobilising power in a different way. What the case of Covid-related apps shows, is that Google and Apple had what Avelino (2017) terms 'innovative power', which is the power to create new resources. The EU, on the other hand, can mobilise its power in different ways, for example through the creation of a new legal framework - 'transformative power' (Avelino, 2017) - which it is doing through the establishment of the eIDAS Regulation, which brings the EUDI Wallet into existence.

It is important to note the connection between the 'big and the small' (De Goede, 2016; MacKenzie, 2005) here: the politics around the development and adoption of technical standards are related to global power struggles over the (development of) digital technology. Namely, this competition between the EU and Big Tech ties in with larger objectives of digital or technological sovereignty (which I also mentioned in chapter 4), where the EU is attempting to reign in the power of Big Tech (Madiega, 2021). This objective also clearly comes out in the case of the EUDI Wallet, as one of its goals is to provide an alternative to commercial digital ID wallets (Weigl et al., 2022). Or, as Peter puts it:

> 'We have become too dependent on American Big Tech. They know a lot about you and me, and we don't want that anymore. We want a European answer to that. This is one of the driving forces that is part of this [the EUDI Wallet], and is very present within the European Union.'

The concept of 'digital sovereignty' has gained traction quite recently (Hummel et al., Glasze et al., 2023), and, as scholars have shown, can refer to different situations (Couture and Topin, 2019). It is different from self-sovereign identity in the sense that this revolves around the 'sovereignty' of a state (or in this case, the EU), from companies and other states in relation to technology, rather than individuals being in 'control' of their own data. However, the

sentiment behind it is similar, as both concepts are concerned with power that can be exercised through technology and data.

In the case of the EU, digital sovereignty does not only refer to becoming 'sovereign' from (American) Big Tech companies; it objective also signals a competition with other global powers, mainly China and the US, in regard to technology (Broeders et al., 2023; Rühling, 2020). Technical standards should be seen as one part of this struggle. For example, Glasze et al. (2023: 921) suggest, 'digital sovereignty' has recently been used 'to legitimise strategies for enforcing technological and/or regulatory standards with a potentially global impact.' Similarly, Rühlig (2020: 5) notes that technical standards 'have been a driving engine behind globalisation' for decades, with the competition becoming fiercer over the past years. In recent years, he suggests, technical standards may become an integral part of a global power competition over technology (Rühlig, 2020. As such, '[t]echnical standardisation has never been non-political […]. Technical standardisation has been a particularly discrete form of exercising political power since its inherent political core remained largely overlooked' (Rühling, 2020: 7). Therefore, the power to set technological standards should not be underestimated, as standards are not neutral. Rather, there are values that are inscribed in these standards. This also means that the stakes are high, as this involves ideas about how society should be. In what follows, I will argue that the development of SSI and the EUDI Wallet and the standards that they use, should be seen against the backdrop of larger power struggles, where the EU and Big Tech companies sometimes compete and sometimes collaborate.

6.3. Experts and expertise

> *'"It's a digital identity revolution", a Dutch government representative exclaimed during his presentation. He told his audience that "all possibilities that exist in the physical realm, will extend to the digital realm in the future." At the moment, he pointed out, the European Digital Identity Wallet is still under development. However, "what is really new," he continued, is that "the policy process and implementation process are running in parallel".'* (Digital Identification Conference, The Netherlands, June 2023).

Unlike the contact tracing app, the technical specifications for the EUDI Wallet are not being developed by Big Tech companies, but rather by the so-called 'eIDAS Expert Group'[15], which consists of representatives (who are usually technologists) from every EU member state[16]. While this group does not develop technical standards itself, it does pick the standards that will be used for the EUDI Wallet, which, as I will show, is important, as the EUDI wallet is sometimes seen as a potential 'blueprint' for digital ID wallets across the world (Flanagan, 2023; Tobin, 2022). The involvement of the Expert Group is necessary because the EUDI Wallet is more than only new legislation; it also involves a technological object. As such, this group

[15] eIDAS refers to the legislation: Electronic Identification, Authentication and Trust Services.
[16] Based on interview data with members of the eIDAS Expert Group.

lays out the specifications in the so-called 'Architecture Reference Framework' (ARF) and the eIDAS Toolbox. As I mentioned, all EU member states are responsible for certifying wallets – which means that there will in practice be various wallets. However, all wallets will need to adhere to the technical specifications in the ARF.

What is remarkable about this process, however, is that the legislative process and the process of designing the technical specifications are happening in parallel, and there is a 'feedback loop' between them. This is likely related to the ambition to develop the EUDI Wallet very quickly, which, in turn, is necessary to be able to compete with Big Tech companies. However, this also raises another set of questions of power and legitimacy, as this 'feedback loop' demonstrates a far-reaching influence of technical experts over the creation and governance of this identification system.

Researchers have theorised the rise of 'the coding elite' (Burrell and Fourcade, 2021), the 'tech elite' (Brockmann et al., 2021), but also 'affluent tech workers' (Dorschel, 2020) to conceptualise the growing influence of technical experts. For example, Burrell and Fourcade (2021) suggest that the coding elite has gained more autonomy and independence, as their technical skills and knowledge are valuable in an increasingly digitised society. However, as these concepts are mostly developed with reference to Silicon Valley, they are not directly applicable to the eIDAS Expert Group. Möllers (2021: 113) looks more specifically at the growing influence of technical experts in statecraft, and argues that '[n]ationalizing information infrastructure and placing statecraft into the hands of scientists and engineers might indicate an emerging form of "techno-nationalism"—a combination of nationalist and technocratic tendencies.' This, she argues, is based on the desire to reclaim 'digital territory', by building digital infrastructure locally, rather than relying on, for example, Big Tech companies. However, she points out, this also means that governments increasingly rely on technological and scientific expertise, 'shifting tasks of government into the domain of computer scientists and network engineers' (Möllers, 2021: 112). Therefore, the materiality of the technology is important to achieving digital sovereignty.

I argue that the eIDAS Expert Group is also a group of technical experts that is carrying out government tasks. This is particularly because the legislation and the technical specification development process of the EUDI Wallet are happening in parallel. At the Identity & Technology Forum, SSI practitioners praised the EU Commission for taking this approach. One of them pointed out that 'things are not like in the '80s anymore', where legislation is made, and technologists have to figure out a way to make the technology. Instead, 'there is a feedback loop' between the legislation and the technical specification design process. They pointed out that 'the effort to do this is huge', which, the practitioners infer, 'shows how important this is for the Commission.'[17]

The members of the Expert Group whom I interviewed confirmed that this is not normally the approach that is taken. I interviewed four members, and when I asked them

[17] Identity & Technology Forum, Germany, May 2023.

whether this parallel process was something that happened more often, three of them answered that they had never seen this before. However, Marco, one of the Experts, pointed out that the only time this had happened was with the creation of the so-called 'green pass', the digital Covid-vaccine app, or 'Covid passport', which aimed to help European citizens travel between member states (Parker, 2021). This shows another connection between the pandemic and the EUDI Wallet: a new way of creating public interest technology, where speed is of the essence.

When I asked the Experts about the 'feedback loop' between the legislation and technical specifications, most were reluctant to talk about it, pointing out that the Commission puts forward the requirements and that they are simply finding the best way to translate the requirements into technological specifications. Others, however, do admit that there is some back and forth between the technical specifications and the legislation. As Antonio, the consultant reporting to the Commission about the Expert Group, describes his role in an interview:

> 'What I do is trying to translate the technical problems for the legals and trying to help them understand and find a better solution and negotiating all the all the different things in the discussion with the Parliament and discussion with the Member States or in the Council.'

In other words, policymakers do understandably not always have the background to understand the details of the technical part of the EUDI Wallet. However, as the legislation and the technical process are happening at the same time, this also means that there is the possibility for technology and legislation to mutually influence each other. Therefore, as this legislation revolves around the creation of a technology, this suggests that technical expertise is becoming more important and influential in the political realm. This also suggests shifting sites of power in contemporary statecraft, where the increased participation of technical experts is needed to establish digital policy (see e.g. Möller, 2021; Sharon, 2021).

In this case, creating a digital ID wallet brings technological experts much closer to the sphere of policymaking. This is significant, because this revolves around a technological object that could potentially be used by millions of citizens, and impacts how they access services. Moreover, particularly because this type of technology is very new, the number of people who work on it is limited. Schoemaker et al. (2023: 7) have argued, for example, that 'decentralized digital identity models still exhibit certain features of centralization, namely a reliance on what is currently a relatively small number of SSI technology providers and expertise.' It is therefore important to question the legitimacy of power that this group gains, as the EUDI Wallet relies quite heavily on a small group of not elected or politically accountable technical experts. As policymakers may not be familiar with all technical details, this puts technologists in a key position in the creation of the EUDI Wallet. Charlie is also worried about this, and tells me:

> 'Normally, a law-making process in Europe lasts between one and a half and four years, and then you have a final law, that's published, and then you go to implementation. And

> usually then, after you do guidelines that might specify minor details and implementation things. And, so it's also here. So we have a law, it might be done in 2023, I'd say first half of the year. And then come to delegated acts which take another six to twelve months, and only then do you know what is decided? What is the specification? And you should only then start developing things. But here it's the other way around. Here it's like a parallel process, and the lawmakers are totally redrafting the whole thing. At the same time technologists are already sitting there and saying "hmm, how could we actually do that? Is there any protocol for this? Where is this global standard for mobile driving licenses? Does this fit at all?"'

Consequently, as he sees it, the legislation is very dependent on what the Expert Group decides. He continues by expressing that he is primarily concerned because:

> 'You always have people with deep pockets and usually very good government contacts, that are the vendors of existing electronic identity systems in those countries. Or companies like Thales, which is like the French Palantir. Huge data programme. And they are powerful voices in this debate. They always say, like "Don't worry, we have the solution, it's product A: on our shelf, you know. We've already done it". So they basically try to sell what they already have in their pockets, in terms of software that they've already produced. And that is just the wrong way to do it.'

Therefore, the power structures around the EUDI Wallet are not straightforward: as this involves the creation of a technological object, different actors, each with their own interests, are necessarily involved. This includes, for example, companies that are trying to influence the development of the EUDI Wallet behind the scenes, as well as experts, who may also have their own agendas based on their companies' or member states' interests. What is more, this arguably impacts the way in which power and statecraft are exercised; it puts states in a position where they can regulate, yet not be completely independent from the tech sector, as they are dependent on technical experts and perhaps the sector writ large to develop the necessary technology for a digital society. In other words, therefore, this is beginning to sketch out a change in how digital identification, as well as contemporary digital statecraft is brought about: with the (rapid) digitisation of society come new assemblages, including policy makers, technologists, and private companies. More generally, it also shows how power in relation to digital technology can be complicated and sometimes even paradoxical; yet different actors somehow also work together (see also Collier, 2024).

6.4. The Wallet Wars

While a shifting site of power in itself, the development of the EUDI Wallet is not happening in a vacuum: there is a larger, global shift to digital ID wallets as well (Schoemaker et al., 2023). Importantly, while the EU is trying to regulate Big Tech companies, these companies are still entering the digital ID wallet space elsewhere, which has ramifications for the EUDI Wallet. This is especially important to note in light of what Hicks (2023) has called the 'geopolitical

shaping of digital ID.' While she writes about this with a focus on Asia, it does conceptualise the way in which states and corporate actors 'compete to shape digital ID systems, surfacing underlying intentions' (Hicks, 2023: 216). Similarly, Lyon (2010) has argued that large corporations have been competing over the procurement of contracts to produce digital IDs for various countries, which means these systems are becoming increasingly similar. However, as I will show, 'the wallet wars' are not just a competition between corporate actors; it is also between Big Tech companies and state-like actors like the EU. This is significant, because it means that political bodies are de facto competing with corporations over identification, which was traditionally within the purview of states. At the same time, I argue that this power battle is not straightforward, as they do not oppose each other all the time: sometimes states and Big Tech companies align and cooperate, and sometimes they compete. As such, I argue that power dynamics of digital ID wallets are multi-layered and complex, and include shifting assemblages.

Key examples of other digital ID wallets are Google and Apple Pay, which started off as payment wallets, but are now expanding into the digital identification space. Importantly, they have entered into partnerships with several states in the US, thereby becoming part of the public digital identification infrastructure (Weatherbed, 2023; Perala and Counter, 2023). For example, in the summer of 2023, Google and the state Maryland announced a partnership which will allow residents to store their state ID and mobile driver's license in the Google Wallet (Weatherbed, 2023). Similarly, Apple partnered with the state of Arizona: residents are now able to store their state ID as well as their mobile driver's license (Peters, 2022). Both companies are working on expanding these programmes, and Apple's upgraded wallet is now available in four states (Perala and Counter, 2023). In addition to incorporating driver's licenses, Google is looking to digitise other existing cards, such as library cards and health insurance cards (Weatherbed, 2013). This is not only happening in the US; UK citizens and residents will likely be able to save their National Insurance Number to their Google Wallet soon (Weatherbed, 2023). While these are just a few examples, they show that the digital ID wallet space is moving fast. Importantly, credentialisation is key to this development: these wallets are also utilising credentials as a format to store personal data. As Tobin (2023, n.p.), a prominent SSI figure, writes in a blogpost:

> 'It seems like everyone wants to provide their users with a digital wallet, and credentials to go in it. eIDAS is the main continent-spanning government initiative in town. Microsoft are going big on their Entra suite and adding wallets & credentials to apps like LinkedIn. Apple and Google are busy credentialising their operating system wallets, opening them up to more credential types (though still with high spiky walls around their gardens, especially Apple). Identity providers are pivoting their models to handle "reusable identity" in the form of wallets and credentials.'

In other words, even though, according to Tobin (2023: n.p.), the EUDI Wallet is the 'main continent-spanning government initiative in town,' credentialisation is a wider trend than

something that is happening in the EU alone. This is at the same time, I argue, also the reason that the 'wallet wars', which I will describe below, are so significant: as the credentialisation of identification means that different social institutions and social roles are collapsed into one wallet, the entity that designs the (standards for) the wallet that will be widely used, holds significant power. This is important, because the social conditions which shape a technology matter - they impact the way a technology functions and what its impact on the social world is (MacKenzie and Wajcman, 1998).

Therefore, a key reason that the 'wallet wars' emerged, is that digital ID wallets are still in the development phase. As such, it is still possible to determine its direction, and influence or even dominate the global digital ID wallet market. As Sophie, a prominent SSI expert, explains to me in an interview:

> 'Wallet wars are really…well, the reason there is a quote unquote "war" is because there's different protocols. Different protocols work differently. Therefore, the software that is your wallet, it needs to work differently for each of those different protocols, and be able to sort of speak different languages, as it were. So it's a language fight: "what's our language going to be?" Now, if we don't share a language, then we can't communicate, right?'

In other words, the development of these different 'languages' matters, as this will allow to create a system where wallets can communicate with each other, as well as with service providers (relying parties). What is more, during the industry events that I attended, SSI developers often expressed the wish for digital ID wallets to become interoperable on a global scale[18]. In this sense, the ability to 'scale' was seen as almost synonymous with success, following, what Pfotenhauer et al. (2022) have termed the 'logic of scalability.' This makes it clearer what is at stake in the wallet wars: designing the specifications that underpin a system that could potentially be scaled globally will bestow significant power on the entity that designs this future.

In a *Forbes* article which gained traction in the digital ID community, digital identity and Fintech thought leader David Birch (2023) writes about the 'wallet wars' in the world of payments. His point is, though, that the 'wallet wars' are not about payment, but about digital identity. As digital ID wallets are on the rise, due to 'a combination of consumer demand, regulatory mandates (such as eIDAS in Europe) and the trend toward digital identity wallet issuance by global governments' (Birch, 2023: n.p.), he argues that the digital identity ecosystem (rather than payments) is where the real competition is. This is important, because it shows the emphasis that is put on digital identity as a connector of different systems and services. This is again because of 'proving' and 'verifiability'; the thinking is that completely digital transactions (in the broad sense of the word: payments, but also digital access to public services) will be possible when it has been 'verified' that someone is who they claim to be. In other words,

[18] Identity & Technology Forum, Germany, May 2023; Radical Identity Meet-up, Switzerland, June 2023.

digital identity and identification are thought to be key to a completely new ecosystem and way of accessing services.

In a blogpost, digital identity expert Antti Kettunen (2023: n.p.) identifies three main groups participating in the 'wallet wars': Big Tech platform giants, that 'are extending their platform capabilities,' the public sector 'like the European Union and its member states are revising their digital identity approach with legislation and national wallet service,' and independent wallet providers.

Kettunen (2023: n.p.) calls Apple Pay the 'gateway drug' to an integrated wallet ecosystem. This means that Apple will likely follow its familiar strategy of 'ecosystem lock-in', where the users of Apple products can link services together, which makes it easier to use for them, and a great business opportunity for Apple. In his words: '[l]et's be clear: Apple is developing the Apple Wallet as a loyalty ecosystem, and its goal is to provide a master loyalty app experience through wallet including points, pay-with-points, promotions, customer service messaging, geofencing and more' (Kettunen, 2023: n.p.). This means that Apple's wallet could become much more than just a wallet where credentials are stored: transactions could be monetised, and the wallet turned into 'media' (Kettunen, 2023). In other words, it could become something more closely resembling a platform than a physical wallet.

In competition with this type of wallets, are wallets issued by states, the EUDI Wallet being the most sophisticated example of this (Kettunen, 2023). As I mentioned, the EU took the approach of designing legal and technical specifications that a wallet needs to comply with, which are based on SSI principles. Member states can then certify wallets that are in line with these specifications. As such, these wallets will be more regulated, and the private sector will have less freedom to design them. However, these wallets will also include a wide range of credentials and use-cases, which, as I argue, makes them more than only a wallet for identification: the fact that they could also be used to pay, save train tickets, or rent a car, suggests that they will collapse different social institutions and social roles.

The third group that Kettunen (2023) identifies, independent wallet providers, is a mix of different organisations that are developing wallets. The issue with these is that they often do not have a specific use-case yet, but companies developing these could potentially work for private and commercial actors to develop custom-made wallet for specific projects (Kettunen, 2023).

As such, the 'wallet wars' refer to a global competition over the design of digital ID wallets. It is striking that identification has become a site of struggle, because states have traditionally had the monopoly over identification (Torpey, 2000; Caplan and Torpey, 2001; Lyon, 2007). I argue that the competition described above could, in part, be seen as related to the credentialisation of identification: because new digital ID wallets aim to bring together previously separate aspects of people's lives, different functions, and different services, there is more overlap between formerly distinct mechanisms of identification. Namely, with the EUDI Wallet, the EU is expanding identification processes beyond the sphere of the state alone, and aims to include private services, as well as identification on the internet. Wallets developed by,

for example, Apple, have been able to do some of these things, such as storing tickets and making online payments, for longer (Tkacz, 2019). At the same time, as I have shown above, companies like Apple and Google are also trying to enter the space of state-issued identification, as they aim to make it possible to store credentials like ID cards and driver's licenses in their wallets. Therefore, the expansion into different types of credentials and identification comes from 'both sides': the EU is trying to include private services, while Big Tech companies are trying to include traditional citizenship documents.

However, this power struggle is complex. Shifting alliances are difficult to frame in relation to traditional accounts of power, which are often more focused on the way in which power is exercised within the state (see e.g. Bachrach and Baratz; Lukes, 2004). However, following Avelino (2021), I argue that the EU and Big Tech companies have 'different power.' Avelino's (2021) work allows me to conceptualise these new power dynamics, as she conceptualises an account of power where power does not necessarily rest with one actor (like a state or the EU) which has power over another actor, or where one actor has more power than another. Instead, actors surrounding a particular issue can have 'different power' (Avelino, 2021: 434), which means that they mobilise different types of resources. Crucially, Avelino (2021: 434) proposes that the '"power-to-change/create-something-new" is a qualitatively different phenomenon from "power-to-reproduce-the-existing".' Following Avelino's (2021) typology, therefore, I argue that Big Tech companies yield significant 'innovative power', because they have the capacity to create new technologies, such as standards. They can do this significantly faster than the EU, which has many more political and legal hoops to jump through. What is more, as I showed earlier in this chapter, this even leads to the new involvement of technical experts. The EU, in turn, does have 'transformative power' because it is able to develop (re)new(ed) structures and institutions (Avelino, 2021: 434), such as the legal framework (eIDAS) that brings the EUDI Wallet into existence and makes it an official identification system. Clearly, Big Tech companies do not have such power, and the only way in which they can incorporate state-issues identification documents, is by cooperating with states.

However, to complicate this even further, there is a way in which wallets developed by Big Tech companies could become certified in the EU. As I mentioned, there will not be just one EUDI Wallet: rather, there will be a set of legal and technical specifications that wallets will need to comply with. It is then up to member states to certify wallets. Therefore, it is in theory possible for member states to certify Apple or Google Wallets, as long as they fulfil all requirements. As Carl, a digital identity expert who plays an important role in the large-scale pilots for the EUDI Wallet, puts it:

> 'The eIDAS says the issuing of the wallet…it's issued by the member state or on behalf of member state, or it's a private wallet certified by a member state. We do not think about the member state certifying the Apple wallet. Against the requirements given by European standards, the eIDAS toolbox. Yes, and then we have an Apple wallet, which is an EU digital

> wallet, which has to be accepted, by every member state, also by GAFA[19], also by a critical infrastructure. This is not excluded. And then the member state currently can decide if they provide their wallet only for their citizens or for any other citizen of a European member state. And now think a little bit… we have a member state which certifies an Apple wallet and gives the possibility for any European citizen just to get this wallet. Any other questions concerning privacy?'

This is ironic, because the EU is trying to regain control through regulation, and limit the power of Big Tech companies in this space. At the same time, however, this is hard to control completely, as these companies could decide to create a wallet that adheres to the specifications. Therefore, the EU is on the one hand competing with Big Tech, as there is a race over who develops and adopts the specifications and standards that will be widely used, and, on the other hand, could also cooperate with them so long as Big Tech companies comply with the legislation. As such, there is a continuous back and forth, where power does not clearly reside with the one or the other; instead, the power dynamics are complex. Applying a *transversal perspective* to the politics of Big Tech, Monsees et al. (2023: 6-7) argue that:

> '[t]he politics of Big Tech is simultaneously embedded in, opposed to, and split from traditional political power. On the one hand, the practices of Big Tech work transversally by cutting across and unsettling political, institutional, and legal boundaries. On the other, these practices remain strongly linked to territorially bounded political and judicial institutions and boundaries.'

This helps elucidate the complicated power structures around the EUDI Wallet that I mentioned above; rather than seeing power as something that resides either with the one or the other actor, the power of Big Tech companies could be seen as 'different' from the power of the EU, as it works transversally. Employing this perspective helps to conceptualise the shifting assemblages of power, in which Big Tech companies are sometimes working together with states, sometimes competing with them and sometimes something in between. This ultimately reshapes what identification looks like, as the EU as well as Big Tech companies are expanding into different spaces, turning identification into something that is not just controlled by states anymore. I will explore these shifting power dynamics further below, by focusing on the example of technical standards for credentials.

6.5. The politics of standards

> *'Standards', 'interoperability', 'seamlessness', 'scalable trust' are the issues that came up in nearly every presentation. The current design challenge, as was pointed out many times, is to make different wallet systems interoperable: only then it will be possible to have a wallet that can be used around the world. The key thing to*

[19] An acronym for Google, Apple, Facebook, Amazon.

> *make this happen is standardising components of the technology. This development is in full force right now, as the technology is being created and implemented at the same time. As was remarked during one panel featuring leading figures in SSI-world: 'we are at that moment now that we're showing the power of standards by implementing'. Or, as another prominent standards developer put it in her call to action: 'implement, implement, implement!'* (Identity & Technology Forum, Germany, May 2023)

To illustrate the complicated power dynamics described above, I will show that this battle happens on different scales. In this section, I zoom in on one competition below the surface of the 'wallet wars': the development of technical standards, with a focus on the development of standards for credentials. I do so because I have argued throughout this dissertation that credentialisation lies at the core of changing identification mechanisms.

As I briefly mentioned above, standards are the foundation for different 'languages' (protocols). They are necessary to 'scale' technology, and make it interoperable, because it allows different devices to communicate with each other. As such, they are an important topic of conversation and contestation in this stage of the development of digital wallets, as defining standards and the question of who does the designing, will in part determine the course of this technology. Bowker and Star (2000: 44), who have written extensively on systems of classification, argue that there are 'practical politics' around the development of standards, because 'whatever appears as universal or indeed standard, is the result of negotiations, organizational process, and conflict.' Therefore, even though standards are (nearly) invisible once they have been implemented, they are in fact the outcome of both struggle and cooperation. Or as Bowker and Star (2000: 49) put it, 'standards and classifications, however dry and formal on the surfaces, are suffused with traces of social and political work.' These politics matter, because standards and classifications shape the social and moral order (Bowker and Star, 2000). What is more, as Timmermans and Epstein (2010: 70), who call for a sociology of standardisation, point out; standards are inextricably connected to globalisation, as they 'help regulate and calibrate social life by rendering the modern world equivalent across cultures, time, and geography.' The example of the standardisation of credentials, which I will discuss below, shows the social and political work behind the scenes as well as the global dimensions of the struggle over standards, as it connects the competition around standards to the larger struggles between states and Big Tech companies described above. As such, while standards might seem quite technical and insignificant in some ways, looking at them allows to connect the 'big and the small' (De Goede, 2017: 356), where small technicalities are connected to global politics (Mattli and Büthe, 2003).

In the space of digital ID wallets, some standards have already been developed, while others are still a bone of contention. As I mentioned above, SSI practioners emphasise the importance of standards because it allows wallets to be interoperable and, therefore, to scale globally. In an interview, Christoph compares the interoperability of digital identity to web browsers:

> 'No matter where I am in the world, I can use my web browser to access any website and anywhere else in the world, at least in theory. Of course, there's some firewalls and censorship, and so on, but that's the original intention of the Internet to be globally connected. And it should be the same way with digital identity, right? […] That's the responsibility of the technical standards, and to make sure that it's not…that we don't end up with some isolated ecosystems that are disconnected, and that don't work with each other, because as a human being […] I should also be able to take who I am with me wherever I go, and whatever I do, I'm still the same person.'

This shows that the development of common standards is considered to be important, because it allows different systems to connect and 'talk' to each other. Accordingly, it is related to the 'language fight' that I mentioned in the previous section, as different wallets will need to speak the same language to be able to communicate.

Credentials are one key aspect of digital ID wallets that needs to be standardised – and while these are a small technical component, they are also a site of big power struggles. The hopes pinned onto credentials to change society were palpable at the industry events I attended. As was in promised in one presentation at the Identity & Technology Forum[20] by developers working on credentials 'the world of credentials will happen.' However, as this world is still under development, and credentials are currently being standardised, they also pointed out that 'we're right at the early exciting days, and we don't know yet whose ideas will win the day.' It is important to point out that these industry events are not only attended by people from the original SSI community, but also by vendors selling 'identity solutions', government representatives and companies that are looking for identity solutions to improve their online services. As these different actors interact, concepts are reshaped as well. While the concept of 'credentials' comes from the world of SSI, it is being adopted - or as some would argue, appropriated - by other actors as well. As one presenter, member of the original SSI community, pointed out at that same conference, 'everyone is doing credentials now'. As she continued, some of those do not align with how the SSI community has them in mind: 'even companies that were very against adopting VCs are now doing it. They just call it something else. They are credentials, but not decentralised.' This shows, therefore, that credentialisation also comes with competition, power struggles and appropriation.

In particular, SSI practitioners often showed disgruntlement about Apple's attempts to influence the standardisation of verifiable credentials. At the Radical Identity Meet-up[21], one presenter mentioned that Apple is currently trying to exercise influence through one of the standard setting bodies, OpenID. When I spoke to the presenter[22], they told me that there is currently a 'Apple vs Google vs Microsoft vs others battle going on.' Apple's approach is particularly harmful, according to this SSI practitioner, because they are trying to 'impose' their

[20] Identity & Technology Forum, Germany, May 2023.
[21] Radical Identity Meet-up, Switzerland, June 2023.
[22] When I explained that I wanted to include the battle around standards in my PhD dissertation, they were happy to participate, as they perceived it as an important and political issue.

standard for verifiable credentials – the so-called 'MDL standard' - through the mobile driver's license. Because Apple is working with ISO (International Organization for Standardization), which is one of the main standard-setting bodies, the company is able to gain considerable influence. In the United States, the presenter explained, this has led to a complicated situation, because some states, like California, are going against this, while other states are working with Apple. The main problem that the SSI community sees, is that Apple's/ISO's MDL standard is not an open standard, which means that no one knows how it is made. The problem, according to them, is that 'Apple is easy to use. And if Apple implements MDL, then it will design the standards of our world.'

Not wanting Big Tech to 'design the standards of our world' is something that is brought up more often during these events. At the Identity & Technology Forum[23], practitioners often urge participants to contribute to standardisation, pointing out that 'we don't want Big Tech giants to win', urging practitioners to 'implement' and test standards sooner rather than later. In particular the MDL standard was often perceived to be dangerous. This view was also held by Sophie, who tells me:

> 'MDL is a terrible standard built by a secretive standards body with really just the card cartel and government interest at the table, no citizen input, no visibility, so you can't see what they're doing as they do it. You can't even see the spec when it's done. But you want to roll out a digital identity program to people with a format that they can't even read. And you want citizen trust in it?'

The fact that the SSI community is so passionate about this can be traced back to their original goal: creating an 'identity layer' for the internet, which would mean that individuals would control their own data and identity and not be dependent on powerful actors like platforms to be identified anymore. Therefore, the fact that those same Big Tech players are now also moving into this space, is a reason for concern for the SSI community, for if Big Tech does manage to define the standards and protocols that will be widely used, it would go against the very core of the SSI community's ambitions. As such, it is not only a technical fight: it is directly related to questions about the social and moral order (Bowker and Star, 2000) that is imposed through these standards, as the way in which this is done corresponds to very different views of how the social world should be. Namely, the SSI community is trying to implement their idea of a power shift towards individuals, whereas Apple is more likely to follow its own business logics. The EU occupies an interesting position in this, as it aligns with the SSI community, while also having its own interests (which I will address below), showing that there are shifting assemblages in this space.

Just how complicated the world of standards is, became clear to me when Sophie allowed me to look at the list of existing ones. Sharing her screen during our interview on Zoom, she

[23] Identity & Technology Forum, Germany, May 2023.

showed me an excel file containing a list of different possible standards for credentials[24]. There are currently 19 different standards, she shows me as she scrolls through the list. She tells me that there are some different credential 'flavours', which each have their own core group. Companies will pick one that they will bring to market. She explains:

> 'You've got companies. So what's Microsoft gonna to do? Well, that has a huge impact […], you know…what's Google gonna do? What's Apple gonna do? What's Facebook gonna do? Right. So these really big actors in the tech world; what infrastructure are the infrastructure companies gonna sell? So IBM, Oracle, like the entities that have giant databases, the government, […] they're going to be like, "well, we can help you issue a blah blah blah". Well, what's the blah blah blah that they say they can issue, in what format? Governments themselves who pick vendors, who pick, "we want, in our ARF[25], we care about this format of credential, issued in this way." […] So it's really these large entities that are building stuff and […] where do they get their information from? Who do they decide is the right way? […] And then there's kind of sitting on the fence people who are like "it's too risky to pick anything, we'll wait until it settles out in the market." Well, that doesn't help the market decide, the market being where the wind blows.'

In other words, it is a complicated dance, that involves many different actors, such as states, companies, people developing the technology. Ultimately, as Sophie also points out, it is also a question of which information is chosen, and trusted, and who gets to make the decisions. As such, designing the standards is not the (only) problem; getting them to be adopted for large projects means that they will actually be used. Government representatives, for example, might not always be aware of the (subtle) differences between different standards, and the politics surrounding them. What is more, in case of the EU, even though it is trying to regulate Big Tech companies, it is difficult to not be influenced by these companies, as they have such 'innovative power' (Avelino, 2021), as, for example Apple paired up with ISO (one of the main standard-setting bodies) and, as such, as considerable influence over standards. Importantly, all standards are created in a specific context, and convey a specific idea about the future. As Sophie points out:

> 'There's little mini politics stories behind each one of these, and each one of them has different kind of backers with different amounts of power, and ultimately there are actual differences in the architectural ending.'

This shows again that the standards for credentials are not neutral, they are created in relation to different interests. In a follow-up interview, we spoke about this more. According to her, the groups that are working on standards also have varying degrees of openness, and different ideas about what the standard should do:

[24] It should be noted that credentials are not the only part of the technology that still need to be standardised. They are just one part of the puzzle.
[25] The Architecture Reference Framework, which contains the technical specifications for the EUDI Wallet.

> ‘Some [standard setting bodies] are more egalitarian than others, and some are super like closed, and you […] cannot get in them, no matter how hard you try. Different processes that they use for their internal group work. So there's like who can get in and […] there's what they do when they're inside, and then there's […] within that like who they care about, who are they writing the standard for? What's their imagined future when they're writing the standard? Like, somebody said, I actually think this is kind of brilliant, somebody said, like every organisation, has an official version of the future that they're all kind of working towards, like, they have different official versions of the future, all these groups, right? And then they come to market meaning there are products based on these specifications, and then there…the different specs with their different starting points and different constituencies, who got behind them to make them, are now fighting in in this…it's fighting in the sense that they're trying to get large entities with power to pick them.’

Accordingly, there are layers on layers of politics behind the development of standards. It is more than just a technical debate: this is underpinned by different world views and ideas - sociotechnical imaginaries (Jasanoff and Kim, 2015) - of what the future should look like. As such, the standard that is ultimately chosen and widely adopted, comes from a very specific point of view. Therefore, choosing standards and developing digital ID wallets is a complicated power struggle over the future.

The EU, and more specifically the eIDAS Expert Group, plays an important role in this, as the adoption of standards is key to their success (Timmermans and Epstein, 2010). Therefore, because the EUDI Wallet is such a large-scale project, which, is often suggested, could be the ‘blueprint’ for digital identity systems in different places (Tobin, 2022; Flanagan, 2023), the technical standards that are adopted in the Architecture Reference Framework matter as, as they could cause the market to go a particular way in terms of standards and protocols. In other words, while the EU does not design the standards for the EUDI Wallet itself, so does not have that kind of ‘innovative’ (Avelino, 2021) power, it does decide on a set of standards. As the EU does have the power to regulate, and thus the ‘transformative’ power (Avelino, 2021) to bring about new legislation which is developed in conjunction with the technical specifications for a digital ID wallet for 27 states, the standards that the eIDAS Expert Group will have a significant impact on what the digital ID wallet landscape will look like.

In other words, there is a strategic imperative in adopting technical standards, because if these standards do indeed become the global norm, other states will follow and create technology in a way that has the EU’s stamp of approval on it. Therefore, even though seeming technical details, the politics of standards link power struggles on different, interconnected scales.

6.6. Conclusion

This chapter sketched out the shifting sites of power in relation to the design of digital ID wallets. It first showed that the Covid-19 pandemic has significantly impacted the (perceived) need for the EUDI Wallet, as well as the accelerated fashion in which the wallet is being developed. In trying to keep up with the digital developments, states will increasingly need to rely on technical experts to develop the technological underpinnings. In the case of the EUDI Wallet, this also resulted in a parallel legal and technical process, with technical experts exceptionally close to the legislation, suggesting a growing influence in statecraft and, more specifically, digital policy. What is more, the credentialisation of identification raises the stakes for the so-called 'wallet wars', where different actors, including the EU and Big Tech companies compete over the design of digital ID wallets. This is significant, for it means that political bodies like the EU are de facto in competition with Big Tech companies over identification – which was traditionally within the purview of the state. What is more, I showed that there is an expansion into different types of identification documents and mechanisms from both sides: political bodies like the EU are trying to enter the online identification space, while Big Tech companies are trying to include traditional citizenship documents. As such, I argued that the complicated power dynamics are in part due to credentialisation, as digital ID wallets such as the EUDI Wallet are integrating different, previously separate functions. At the same time, I argued, it is not simply a matter of 'the state' against 'Big Tech', but power manifests itself in various ways. Namely, while Big Tech companies have the advantage of significant innovative power, state-like actors like the EU have the transformative power to develop legislation. Applying a *transversal* perspective therefore showed that there is simultaneous competition over and collaboration between states and Big Tech companies over digital ID wallets. What is more, these power battles are reflected in the small technicalities of technical standards, linking the 'small' to the 'big' (De Goede, 2017). Looking at the example of the standardisation of credentials, I showed how something small like a technical standard is tied to different political stories and competing views of the future. In sum, this chapter showed shifting sites of power in contemporary governance, as new actors, such as technical experts, but also Big Tech companies become more involved in the development of digital identification systems in changing assemblages. Linking this back to the sociotechnical imaginary of 'control', this is ironic, as a technology that aims to equalise power structures, has become part of a battle over power and monopolies. As such, on top of the move of an internet identity system to the sphere of the state, the new assemblages of (public and private) actors involved in the wallet due to credentialisation, and the new role for user-citizens, this shows yet another way in which identification is changing.

Chapter 7. Conclusion

This research set out to investigate the changing nature of state-issued identification practices. Looking at SSI technology and the EUDI Wallet, I explored the sociotechnical imaginaries underpinning SSI and investigated how this arrangement of imaginaries and technologies was translated into the context of (EU) states. In doing so, I asked how this technology shapes citizenship, and how digital ID wallets (re)produce existing or new power dynamics. Using technologies, citizens and power as theoretical lenses, the dissertation argued that the rise of digital ID wallets, and the EUDI Wallet in particular, signifies an important shift, for it changes how identification is 'done' and how citizens gain access to services. In particular, I have argued that the credentialisation of identification has given rise to 'user-citizens', who must be tech-savvy, entrepreneurial and are expected to decide (to a degree) on the terms of their own datafication, and that the emergence of the wallet produces new assemblages of actors, changing identification processes and the power structures surrounding it.

The three empirical chapters of the dissertation, address several aspects of the emergence of SSI and the EUDI wallet. Together, these tell the story of the wallet in different ways and on different scales: going from the technical, to the societal, to the international dimension of the wallet. Chapter 4 looked at the intimate relationship between sociotechnical imaginaries and the technical architecture of the wallet. I found that new assemblages are now involved in identification practices, and the translation of SSI to the EUDI wallet. The chapter showed how the sociotechnical imaginary that was developed for users of the internet, is now being applied to users of the state. In other words, this chapter tells the story of the EUDI Wallet on the level of the technology itself: it shows how technology is seen as a vehicle to implement a vision of a (better) future. This set the scene for chapter 5, which explored the new role that (digital) citizens will have to play in the wallet ecosystem. I found that different, previously separate identification systems are now linked together (e.g. online and offline systems, or public and private sector ones). This also changes what is expected of citizens: I therefore argued that user-citizens are seen as entrepreneurial and tech-savvy who have to decide on the extent of their own datafication. Therefore, this chapter addressed the emergence of the wallet on a societal level; assessing what implementing this technology means for citizens and the concept of citizenship. These technical and more societal oriented chapters provide the context for the international dimension of the wallet addressed in chapter 6. This chapter shows that identification, which was once something that was in the purview of the state and applied to the state's citizens, is now influenced by international power structures and actors. For example, I found that the so-called 'wallet wars', in which both states and (Big Tech) companies are involved, revolve around seemingly small things like technical standards (e.g. for credentials), but can have large ramifications. This, I argued, has led to simultaneous competition and collaboration between the EU and Big Tech companies. As such, this chapter showed new international interdependencies.

Ultimately, therefore, the three results chapters addressed different levels of the EUDI wallet: a technical, a societal and an international one. The chapters build on each other, showing the various contexts the wallet is embedded in, as well the actors that influencing the wallet on these different levels. Ultimately, these different contexts and actors shape the power structures around processes of identification.

Through these chapters, I developed the concept of 'credentialisation' as a frame to capture what wallet-based identification is shifting: it turns different aspects of people's lives into 'verifiable' information, works to make them machine readable, and collapses previously different social roles and social institutions into one technical system. Throughout the dissertation, I have discussed different aspects of credentialisation. I found that one important way in which the changing nature of state-issued identification becomes visible is through the expansion into different spheres, as the wallet is expanded to include public and private, online and offline services. It is particularly remarkable that the EUDI Wallet includes online identification, as this links older identification practices to new digital issues, notably surveillance capitalism (see Zuboff, 2019). While surveillance is one of the problems that is associated with digital identification systems (e.g. Lyon, 2010; Masiero and Shakti, 2020, Weitzberg et al., 2021), the fact that the EUDI Wallet explicitly tackles (online) data harvesting practices, is new. Also new, is the emphasis on 'control': the wallet is presented as 'empowering' for citizens, as it will give them more control over their personal data.

However, at the same time, the wallet attaches importance to 'verifying' identities. Looking at this in light of the history of identification, this is not unusual, as establishing 'uniqueness' and 'fixing' identities is part and parcel of identification (e.g. Martin and Whitley, 2013; Van Zoonen, 2013; Caplan and Torpey, 2001). However, the dissertation did show that the process of verifying identities is becoming more important for a wide array of situations. Credentials play an important role in this: they consist of 'high quality' data which is meant to 'prove' someone's identity. Therefore, the wallet occupies an interesting space, between 'control' and 'verification'. On the one hand, it is presented as something which will make things easier for citizens. On the other hand, however, because of the sheer scope of the project, and its concern with 'verifying' identities, the EUDI wallet may further consolidate a societal practice where verification is a prerequisite for access.

This is not the only tension: doing this research, I noticed several tensions and points of friction. I found that power structures are not straightforward and sometimes even paradoxical. I knew about SSI's promise to shift power structures before I started my fieldwork. However, by immersing myself in the spaces where the technology is discussed, and talking to the people who are working on it, I became aware of its complexity. For example, I could never have predicted there to be 'wallet wars', or the different futures that standard-setting bodies are working towards. It often turned out that things were not black and white, and that 'new' and 'old' often exist together. More generally, therefore, I noticed that it is possible to implement a technology infused with radical imaginaries for the future, but it often runs up against existing power structures. This does not mean that it is impossible to implement, or to

change something, but rather that the sites of power are complex and shifting. This research therefore shows that different modes of power appear to be emerging in the story of the wallet. These have to do with the technology itself (how technology is supposed to re-order power), and the ideological dimension (sociotechnical imaginaries) attached to that, which gave rise to the sociotechnical imaginary of 'control'. In addition, there is the notion of classic state power, as well as the transversal power of Big Tech. While distinct, these different modes of power do not just exist alongside each other; they also overlap and create friction.

Power through technology itself revolves around specific technological affordances and ways that aim to make a shift in 'control' possible through the very architecture of the technology. For example, decentralisation is seen as a means to distribute power through technology, and 'trust' is something that need to be established through cryptographic systems. Importantly, the technological architecture is intimately connected to the ideological dimension of the technology, notably crypto-anarchist and libertarian ideals.

Importantly, this dissertation showed that this also causes friction, as these ideologies are not traditionally reconcilable with a second mode of power; state power. For example, EU states still aim to retain power over the process of identification, which means that the technology needs to be adapted to the context of the state. On the one hand, there is a narrative around giving more power to citizens, which happens through 'control' over their personal data. On the other hand, the wallet should be seen in light of the long history of identification by states, which has been an exercise of state power. Therefore, there is an inherent tension between the sociotechnical imaginary of 'control', and 'control' as a classic function of the state, where the aim is to establish unique, 'legible' individuals, who are simultaneously part of a collective (Caplan and Torpey, 2001; Brensinger and Eyal, 2021). This means that the EUDI wallet can be both a means to give more control over data, but also to identify and verify citizens, using very precise, high-quality data to do so.

The final mode of power is a transversal one: looking at the rise of digital ID wallets at a global scale, other assemblages are revealed. I argued that also these power dynamics are not straightforward: on the one hand, the EU is trying to reign in Big Tech companies, on the other it is difficult to completely escape or limit their influence. What is more, in trying to develop the wallet in an accelerated fashion, technical experts gain more influence in the process, and indirectly over the legislation, raising questions over legitimacy. This means that more, also non-traditional actors are now involved in the (design of) identification systems. Accordingly, I argued that states and Big Tech have 'different' (Avelino, 2021) power (transformative and innovative power respectively), and that they sometimes compete, and sometimes collaborate. Looking at this through a transversal lens therefore makes it possible to reflect on the different scales of power as well: while the EU is developing its own wallet, for example, it is still being influenced by the standard-setting power of Big Tech companies like Apple.

Ultimately, therefore, different, and sometimes contradictory modes of power are starting to manifest themselves through the story of the EUDI wallet. These complex modes of power sometimes work together and sometimes cause friction. For example, this means that

sociotechnical imaginaries sometimes run up against political realities; that the technology cannot be fully implemented because states need to retain some power over identification processes; or that a technology that aims to equalise power structures can simultaneously be part of battles over power and monopolies.

This dissertation, however, showed a different side of 'control' as well. Namely, the control that citizens are promised over their personal data and digital identity is linked to the services they can access. User-citizens will likely run up against existing data exploitation practices: while the wallet puts them in 'control', 'empowering' them, this also means that they need to manage their credentials, making informed decisions about sharing them. This development is important because it is not only concerned with changes in 'control' over personal data, but also the way in which citizens access (essential) services. Furthermore, it crucial to consider the inequalities and hierarchies that could arise as a result of this new system, as it is unlikely that everybody will have the data literacy and (financial) resources to participate. While credentials are meant to limit the amount of data that need to be stored about someone, as they contain high quality, 'verifiable' data, it is questionable whether this will fully change the value that is attached to data. Namely, we still live in a world where data is often seen as a commodity, where the parties that request information have a vested interest in asking for more information that they actually need. Therefore, the market logics that already become visible, could also be a risk, for the data stored as credentials is 'verifiable', and therefore valuable. As such, I found that both states and citizens are confronted with managing 'control', albeit in different ways. However, the credentialisation of identification introduces another complicated layer of power structures: while the EUDI Wallet is a state-issued identification system, it aims to include many different services. As such, other assemblages of actors become necessarily involved in identification processes, as they depend on the wallet for verification and therefore, to grant them access to the service they offer. This also raises questions about the ubiquity of identification, as more and more services come to depend on (the same) identification system.

It also begs the question who is actually in 'control'. With an eye on the future, it will be important to look at who stands to gain from this system: citizens, states, (big) tech companies? Furthermore, it is important to go beyond the issue of 'control' and see the new approach to data sharing that the wallet offers in light of the way in which citizens can participate in the (digital) society. Namely, it raises questions around the distribution of responsibility: in increasingly datafied societies, how should the responsibility for data be distributed between state and citizens, and how can access to (digital) services be guaranteed? Furthermore, the wallet offers access to many different services, but will scale equal equality? Finally, it is essential to look at the potential ubiquity of identification (see also Epicenter Works, n.d.): while credentials, and the possibility to store them all in one place offer an 'easy' system, could it lead to a situation where we need to be 'verified' for everything we do? And for whom will it be easy to 'verify' their identity - and who will find this difficult to prove?

7.1. Contribution

The main contribution of this research lies in the fact that it is one of the first in-depth explorations into SSI technology and the EUDI Wallet. In building on extensive interviews, fieldwork at industry events and documents, this research goes beyond what the few existing studies (see e.g. Cheesman, 2020; Gstrein and Kochenov, 2020; Giannapoulou, 2023) have addressed and maps out the changes that implementing a wallet-based identification system engenders. In doing so, it has demonstrated the complexities around implementing an internet identity model in the context of the EU, the new role for citizens, and the changing power structures around identification processes. Therefore, this is one first studies to provides insights into this emerging technology, as well as a framework for future research on this topic. In particular, by developing the concept of 'credentialisation', the dissertation offers a lens through which the changes that digital ID wallets bring about can be captured and understood. Namely, the credential format and everything that brings with it – the collapse of social roles and institutions, a new way to identify and verify people, is what makes this digital identification system different from previous ones. Therefore, this research presents a new way of looking at digital identification: the existing literature can mainly be divided into studies that consider identification through the lens of surveillance (e.g. Amoore, 2006; Epstein, 2007; Lyon, 2007), and work that consider it in relation to development (e.g. Masiero and Bailur, 2021; Madianou, 2020; Madon and Schoemaker, 2021). This dissertation adds to the literature on digital identification by considering identification processes in relation to datafication and the ongoing collapse of different social institutions, notably the internet and the state. As such, it offers a new perspective, which shows that with credentials and digital ID wallets, digital identification is moving into a new phase.

In addition, the dissertation contributes to this literature by offering insights into the shifting sites of power that accompany the rise of digital ID wallets, and the EUDI Wallet in particular. By showing the different (and shifting) assemblages that are involved in identification practices, the dissertation adds to a growing literature that considers the influence of different actors in identification processes.

Finally, the dissertation adds to the literature on digital citizenship. Existing literature on digital citizenship has investigated the position of citizens in increasingly datafied societies, but has mainly paid attention to citizen's ability to perform citizenship (e.g. Isin and Ruppert, 2015; 2017; 2020) or has considered datafication in relation to profiling and prediction of behaviour (e.g. Fourcade, 2021; Fourcade and Healy, 2013; Broomfield and Reuter, 2022). This literature, has, however, hardly addressed the relationship between citizenship and identification. This dissertation considers datafication and the issue of 'control' over personal data in relation to identification processes, showing that it is linked to access to services and participation. Specifically, the dissertation argued that the credentialisation of identification gives rise to a 'user-citizen', as the boundary between 'users' and 'citizens' is being blurred: 'user behaviour',

notably consenting to the sharing of personal data, is shifted to citizen-related 'transactions', as it becomes an important component of accessing (essential) services. Therefore, it shows that there is more at stake than 'controlling' data, but that the ability to do so is also connected to a citizen's ability to participate in the (digital) society.

7.2. Limitations

The fact that digital ID wallets, and the EUDI Wallet in particular, are very new makes it an important topic to explore. At the same time, it is also the most important limitation: it means that I was only able to investigate it while it was still under development. It is therefore difficult to make definite claims about its societal implications: while it is possible to offer suggestions based on the data and the existing literature, some real-life impacts will need to be investigated when the wallet is widely available. At the same time, it is already possible to demonstrate ongoing shifts: for example, the very fact that the wallet will give access to so many services shows that this technology is different from previous digital identification systems. As such, it was also important to think about the way in which I presented this development: striking a balance between the techno-optimism and solutionism that characterises the run-up to many new technologies (and is often hard to live up to) (Morozov, 2013), and showing that something is indeed shifting.

A second, more general limitation pertains to the data collection process. As Watts (2019: 6) points out, '[…] the pen only moves so fast, you can only sit in one chair, not all the chairs in all the rooms.' For me, this was sometimes very literal: at the industry events I had to decide which presentations I wanted to attend (and which chair to sit in, for that matter), for there were usually several sessions running in parallel. In other words, therefore, this story is necessarily limited. In a similar vein, I selected the interviewees and asked some questions rather than others. In other words, all data were filtered through and interpreted by me, the researcher. By making the connections that emerged from the interview data, I prioritised some over others in a way that I believed was most relevant to the research. It is therefore important to acknowledge that I shaped the narrative presented here. Therefore, even though my arguments are grounded in my empirical findings, there are no guarantees that other researchers would interpret the data in exactly the same way.

These limitations become visible in different ways. The fact that the technology is still under development, affected the way in which I could research the potential impacts of the EUDI Wallet on citizens. As the wallet is not available to the public yet, I was not able to involve 'user-citizens' in my research. As some STS researchers have argued, technologies could be seen as 'co-constructed' with users, as they find ways to adapt, use and manipulate technologies (Oudshoorn and Pinch, 2004; Akrich, 1992). In my research, I was not able to include their experiences. However, as I have argued, looking at what kinds of users are envisioned at the development and design stage is useful, as it reveals the expectations of 'users' as well as the

changes that the people who are working on the wallet are aiming to establish, which includes a new social role for citizens.

In a similar vein, there are other processes that remain hidden as well. For example, I started to sketch out the shifting sites of power with regard to the design and standardisation of digital ID wallets, mostly paying attention to the EU and Big Tech companies. However, it would also be valuable to look at the smaller power battles in 'the weeds' – for example, as Sophie, a prominent SSI expert, pointed out, there are many different standard setting bodies, which all have their own politics and visions of the future. Similarly, while I demonstrated the role of the eIDAS Expert Group, I did not look at the internal politics and decision-making processes of this group. It should be noted, however, that it would be difficult to gain access to these processes as they are largely behind closed doors. However, in the case of access, it would be interesting to further complicate the power struggles in the design phase. Some STS approaches (e.g. looking at 'technological frames', see e.g. Lin and Silva, 2005) may emphasise the importance of looking at all actors involved in a specific design process (see e.g. Bijker, 1987) to demonstrate how decisions are made and different 'frames' eventually converge and stabilise (Orlikowski, 1992; Orlikowski and Gash, 1994). However, while this is a valuable approach, it was not my goal to explore decision-making processes in depth; rather, I was interested in presenting a more general argument that captures the connection between something small - like a technical standard - and global power battles, and explore what is shifting due to the arrival of digital ID wallets.

7.3. Future research

An important avenue for future research will be to investigate what the EUDI Wallet does in practice: for example, what does the promise of 'control' look like in practice, and can the EUDI Wallet live up to its promises and expectations? Therefore, as I noted above, one essential topic would be to engage with the users of the EUDI Wallet once it is widely available. This could include ways in which users co-shape the technology, for example, by using it in ways that might be different from what was initially expected. This could be explored in different places across the EU, as digital literacy skills and (financial) resources vary across the continent. As such, by involving the users of the wallet, future research could ask what works and what does not work, exploring facets of inclusion and exclusion across social groups. In addition to looking at different groups of citizens, future research could look more closely at groups who do not have access to the wallet. In particular, migrants and asylum seekers are excluded from the (initial) design of the wallet, it is important to investigate how this affects these groups, and whether the EUDI Wallet reinforces social stratification.

A second avenue for future research is the convergence of digital ID wallets and digital payment wallets. The very fact that it is called digital ID *wallet* already suggests a connection with money and finance. While I alluded to this convergence in chapter 6, more research is

needed to capture the collapse of these different worlds. In particular, the fact that Google and Apple are expanding their payment wallets to include all kinds of credentials is significant, and raises questions about the role of corporate actors in the distribution of (public) services. What is more, it is important to pay attention to the banking sector here as well, as some banks are currently exploring the possibility of moving into the digital identity sphere (see e.g. Mobey Forum, 2023). Relatedly, attention should be paid to different entities developing wallets, and the marketplace of wallets that is likely to emerge. 'Super apps' are interesting in this regard, as they are also on the rise and have the capacity to include digital ID documents as well. Lastly, it would be interesting to look at the 'ceremony' around identification. Existing research about the new sociality of digital money and payments (see e.g. Swartz, 2020) suggests new memberships, communities and experiences, and it is worth asking if digital identification lead to similar social experiences.

Finally, I believe that there is a space for (more explicit) normative research on this topic: digital ID wallets have the potential to change the way in which people interact with their state, with services, and with each other. They could make identification more ubiquitous than ever before; it is important to consider whether this changes society for the better.

Bibliography

Aas, K.F. (2006) '"The body does not lie": Identity, risk and trust in technoculture', *Crime, Media, Culture: An International Journal*, 2(2), pp. 143–158. doi: https://doi.org/10.1177/1741659006065401

Aas, K. F. (2011) 'Crimmigrant' bodies and bona fide travelers: Surveillance, citizenship and global governance', *Theoretical Criminology* 15(3): pp. 311-346. doi: https://doi.org/10.1177/1362480610396643

Access Now (2023) *Five years under the GDPR. Becoming an enforcement success*. Available at: https://www.accessnow.org/wp-content/uploads/2023/05/GDPR-5-Year-report-2023.pdf (Accessed: 17 May 2023).

Adam, B. and Groves, C. (2007) *Future Matters: Action, Knowledge, Ethics.* Leiden: Brill.

Agamben, G. (2008) 'No to political tattooing', *Communication and Critical/Cultural Studies*, 5(2), pp. 201-202. doi: 10.1080/14791420802027452.

Ajana, B. (2012) 'Biometric citizenship', *Citizenship Studies*, 16(7), pp. 851–870. doi: https://doi.org/10.1080/13621025.2012.669962

Ajana, B. (2013) *Governing through Biometrics: The Biopolitics of Identity*. London: Palgrave MacMillan.

Akrich, M. (1992) 'The de-scription of technical objects', in Bijker, W. and Law, J. (eds.) *Shaping technology/building society. studies in sociotechnical change*. Cambridge: MIT Press, pp. 205–224.

Akrich, M. (1995) 'User representations: practices, methods and sociology', in Rip, A, Misa, T.J. and Schot, J. (eds.), *Managing technology in society: the approach of constructive technology assessment*. London: Pinter Publishers, pp. 167–184.

Alexopoulos, C., *et al.* (2021) 'How blockchain technology changes government: a systematic analysis of applications', *International Journal of Public Administration in the Digital Age*, 8(1), pp. 1-20. doi http://doi.org/10.4018/IJPADA.20210101.oa10

Alfrey, L. and Twine, F.W. (2017) 'Gender-fluid geek girls: negotiating inequality regimes in the tech industry', *Gender & Society*, 31(1), pp. 28–50. doi: https://doi.org/10.1177/0891243216680590

Allen, C. (2016) *The path to self-sovereign identity*. Available at: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (Accessed: 25 July 2023).

Allen, J. (2011) 'Powerful assemblages?', *Area* 43(2), pp. 154-157.

Allen, J. and Cochrane, A. (2010) 'Assemblages of state power: topological shifts in the organization of government and politics', *Antipode*, 42(5), pp. 1071–1089. doi: https://doi.org/10.1111/j.1467-8330.2010.00794.x

Allison, A. *et al.* (2005) 'Digital identity matters', *Journal of the American Society for Information Science and Technology*, 56(4), pp. 364–372. doi: https://doi.org/10.1002/asi.20112

Amoore, L. (2003) 'Governing by identity', in Bennett, C.J. and Lyon, D. (eds.) *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*. New York: Routledge, pp. 21-36.

Amoore, L. (2006) 'Biometric borders: governing mobilities in the war on terror', *Political Geography*, 25(3), pp. 336-351. doi: doi:10.1016/j.polgeo.2006.02.001

Amoore, L. (2013) *The Politics of Possibility: Risk and Security Beyond Probability*. Durham: Duke University Press.

Amoore, L. and Hall, A. (2009) 'Taking people apart: digitised dissection and the body at the border', *Environment and Planning D: Society and Space*, 27(3), pp. 444–464. doi: https://doi.org/10.1068/d1208

Anaïs, S. (2012) 'Objects of security/objects of research: analyzing non-lethal weapons', in Salter, M., Mutlu, C. (eds.) *Research Methods in Critical Security Studies.* London: Routledge, pp. 432-440.

Anand, N. and Brass, I. (2021) 'Responsible innovation for digital identity systems', *Data & Policy*, 3, pp. 1-22. doi: https://doi.org/10.1017/dap.2021.35

Anderson, B. (2006) *Imagined Communities*. London: Verso.

Andrieu, J. (2016) *A technology free definition of self-sovereign identity*. Available at: https://github.com/WebOfTrustInfo/rwot3-sf/blob/master/topics-and-advance-readings/a-technology-free-definition-of-self-sovereign-identity.pdf (Accessed: 25 July 2023).

Antenucci, I. and Tomasello, F. (2023) 'Three shades of "urban-digital citizenship": borders, speculation, and logistics in Cape Town', *Citizenship Studies*, 27(2), pp. 247–270. Available at: https://doi.org/10.1080/13621025.2022.2073088.

AoIR (2012) 'Ethical Decision-Making and Internet Research: Recommendations from the AoIR Ethics Working Committee (Version 2.0)'. Available at: https://aoir.org/reports/ethics2.pdf (Accessed: 15 January 2024).

Aradau, C. (2020) 'Experimentality, surplus data and the politics of debilitation in borderzones', *Geopolitics*, pp. 1–21. doi: https://doi.org/10.1080/14650045.2020.1853103

Aradau, C. and Blanke, T. (2018) 'Governing others: Anomaly and the algorithmic subject of security', *European Journal of International Security*, 3(1), pp. 1–21. Available at: https://doi.org/10.1017/eis.2017.14

Atzori, M. (2017) 'Blockchain technology and decentralized governance: Is the state still necessary?', *Journal of Governance and Regulation*, 6(1), pp. 45–62. doi:10.22495/jgr_v6_i1_p5.

Avelino, F. (2021) 'Theories of power and social change. Power contestations and their implications for research on social change and innovation', *Journal of Political Power*, 14(3), pp. 425–448. doi: https://doi.org/10.1080/2158379X.2021.1875307

Avelino, F. *et al.* (2017) 'Game-changers and transformative social innovation', *Ecology and Society*, 22(4), n.p. doi: https://doi.org/10.5751/ES-09897-220441.

Avelino, F. *et al.* (2020) 'Translocal empowerment in transformative social innovation networks', *European Planning Studies*, 28(5), pp. 955–977. doi: https://doi.org/10.1080/09654313.2019.1578339

Avelino, F. and Rotmans, J. (2009) 'Power in transition: an interdisciplinary framework to study power in relation to structural change', *European Journal of Social Theory*, 12(4), pp. 543–569. doi: https://doi.org/10.1177/1368431009349830

Bachrach, P. and Baratz, M.S. (1962) 'Two faces of power', *American Political Science Review*, 56(4), pp. 947–952. doi: https://doi.org/10.2307/1952796

Bai, Y. *et al.* (2022) 'Decentralized and self-sovereign identity in the era of blockchain: a survey', *2022 IEEE International Conference on Blockchain (Blockchain)*, Espoo, Finland, 22-25 August, pp. 500–507. doi: https://doi.org/10.1109/Blockchain55522.2022.00077

Bambacht, J. and Pouwelse, J. (2022) 'Web3: a decentralized societal infrastructure for identity, trust, money, and data', *Cornell University*. Available at: https://arxiv.org/abs/2203.00398 (Accessed: 24 January 2023).

Baran, P. (1964). 'On distributed communications networks', *IEEE Transactions on Communications Systems*, 12(1), 1–9. doi: https://doi.org/10.1109/TCOM.1964.1088883

Barassi, V. (2019) 'Datafied citizens in the age of coerced digital participation', *Sociological Research Online*, 24(3), pp. 414–429. doi: https://doi.org/10.1177/1360780419857734

Barber, G. (2018) 'I sold my data for crypto. Here's how much I made', *Wired*, 17 December. Available at: https://www.wired.com/story/i-sold-my-data-for-crypto/ (Accessed: 6 December 2023).

Barocas, S., and Nissenbaum, H. (2014), 'Big data's end run around anonymity and consent', in Lane, J., *et al*. (eds), *Privacy, Big Data, and the Public Good: Frameworks for Engagement*. Cambridge University Press, Cambridge, pp. 44–75.

Basaran, T., *et al*. (2017) 'Transversal lines: an introduction', in Basaran, T., *et al*. (eds.) *International Political Sociology: Transversal Lines*. New York: Routledge, pp. 1-10.

Barasan, T. and Guild, E. (2017) 'Mobilities, ruptures, transitions', in Basaran, T., *et al*. (eds.) *International Political Sociology: Transversal Lines*. New York: Routledge, pp. 272-285.

Bauböck, R. (1994) *Transnational Citizenship: Membership and Rights in International Migration*. Aldershot: Edward Elgar Publishing.

Bauböck, R. (2007) 'Why European citizenship - normative approaches to supranational union', *Theoretical Inquiries in Law*, 8(2), pp. 453-488.

Bauböck, R. (2010) 'Studying citizenship constellations', *Journal of Ethnic and Migration Studies*, 36(5), pp. 847–859. doi: https://doi.org/10.1080/13691831003764375

Bauböck, R. (2014) 'The three levels of citizenship within the European Union', *German Law Journal* 15(5), pp. 751–763. doi: 10.1017/S207183220001912X

Bauböck, R. (2019) 'Genuine links and useful passports: evaluating strategic uses of citizenship', *Journal of Ethnic and Migration Studies*, 45(6), pp. 1015-1026. doi: 10.1080/1369183X.2018.1440495

Bauman, Z. *Identity: Conversations with Benedetto Vecchi*. Cambridge: Polity Press, 2004.

Becker, M. and Bodó, B. (2021) 'Trust in blockchain-based systems', *Internet Policy Review*, 10(2). doi: https://doi.org/10.14763/2021.2.1555

Beduschi, A. (2019) 'Digital identity: contemporary challenges for data protection, privacy and non-discrimination rights', *Big Data & Society*, 6(2), pp. 2-6. doi: https://doi.org/10.1177/2053951719855091

Beduschi, A. (2021) 'Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations', *Data & Policy*, 3, pp. 1-13. doi: https://doi.org/10.1017/dap.2021.15

Bekkers, V. (2009) 'Flexible information infrastructures in Dutch E-Government collaboration arrangements: experiences and policy implications', *Government Information Quarterly*, 26: pp. 60-68. doi: https://doi.org/10.1016/j.giq.2007.09.010

Beltramini, E. (2020) 'Against technocratic authoritarianism: a short intellectual history of the cypherpunk movement, *Internet Histories*. doi: https://doi.org/10.1080/24701475.2020.1731249

Bennet, C. J. and Lyon, D. (2008) *Playing the Identity Card. Surveillance, Security and Identification in Global Perspective*. London: Routledge.

Berkhout, F. (2006) 'Normative expectations in systems innovation', *Technology Analysis & Strategic Management*, 18(3–4), pp. 299–311. doi: https://doi.org/10.1080/09537320600777010

Bigo, D. (2011) 'Freedom and speed in enlarged borderzones' in Squire, V. (eds.) *The Contested Politics of Mobility*. Oxon: Routledge, pp. 31-50.

Bigo, D. (2017) 'International political sociology: rethinking the international through dynamics of power', in Basaran, T., *et al*. (eds.) *International Political Sociology: Transversal Lines*. New York: Routledge, pp. 24-48.

Bigo, D., Isin, E. and Ruppert, E. (2019) 'Data politics', in D., Isin, E. and Ruppert, E. (eds.) *Data Politics. Worlds, Subjects, Rights.* London: Routledge, pp. 1-18.

Bijker, W.E. (1987) 'The social construction of bakelite: toward a theory of invention', in Bijker, W.E., *et al*. (eds*.) The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: MIT Press, pp. 155-182.

Bijker, W.E. and Law, J. (1992) *Shaping Technology/Building Society*. Cambridge: MIT Press.

Birch, D.G.W. (2023) 'The wallet wars are not about money, they are about identity', *Forbes*, 1 February. Available at: https://www.forbes.com/sites/davidbirch/2023/02/01/the-wallet-wars-are-not-about-money-they-are-about-identity/ (Accessed: 22 September 2023).

Birch, K. (2020) 'Automated neoliberalism? The digital organisation of markets in technoscientific capitalism', *New Formations*, 100(100), pp. 10–27. doi: https://doi.org/10.3898/NewF:100-101.02.2020

Birch, K. and Bronson, K. (2022) 'Big Tech', *Science as Culture*, 31(1), pp. 1–14. doi: https://doi.org/10.1080/09505431.2022.2036118

Birch, K., Cochrane, D. and Ward, C. (2021) 'Data as asset? The measurement, governance, and valuation of digital personal data by Big Tech', *Big Data & Society*, 8(1), pp. 1-15. doi: https://doi.org/10.1177/20539517211017308

Birch, K. and Muniesa, F. (2020) *Assetization: Turning Things into Assets in Technoscientific Capitalism*. Cambridge, MA: MIT Press.

Bixby, P. (2022) *License to Travel. A Cultural History of the Passport.* Oakland, CA: University of California Press.

Bloemraad, I. (2018) 'Theorising the power of citizenship as claims-making', *Journal of Ethnic and Migration Studies*, 44(1), pp. 4–26. doi: https://doi.org/10.1080/1369183X.2018.1396108.

Bloemraad, I., Korteweg, A. and Yurdakul, G. (2008) 'Citizenship and immigration: multiculturalism, assimilation, and challenges to the nation-state', *Annual Review of Sociology*, 34(1), pp. 153–179. doi: https://doi.org/10.1146/annurev.soc.34.040507.134608

Bodó, B., Brekke, J.K. and Hoepman, J.-H. (2021) 'Decentralisation: a multidisciplinary perspective', Internet Policy Review, 10(2). doi: https://doi.org/10.14763/2021.2.1563

Boenig-Liptsin, M. and Hurlbut, J.B. (2016) 'Technologies of Transcendence at Singularity University', in Hurlbut, J.B. and Tirosh-Samuelson, H. (eds.) *Perfecting Human Futures*. Wiesbaden: Springer Fachmedien Wiesbaden, pp. 239–267.

Boix Alonso (2020) 'European Digital Identity Framework'. Available at: https://www.ecb.europa.eu/paym/groups/pdf/efip/Digital_identity_update.pdf (Accessed: 6 November 2023).

Borup, M. *et al.* (2006) 'The sociology of expectations in science and technology', *Technology Analysis & Strategic Management*, 18(3–4), pp. 285–298. doi: https://doi.org/10.1080/09537320600777002

Bosniak, L. (2001) 'Denationalizing citizenship', in Aleinikoff, A. and Klusmeyer, D. (eds.) *Citizenship today*. Washington: Brookings Institution Press, pp. 83-95.

Bouma, T. (2019) 'Self-Sovereign Identity: Shifting the Locus of Control', 2 March. Available at: https://trbouma.medium.com/self-sovereign-identity-shifting-the-locus-of-control-10da1c8757ad (Accessed: 27 July 2023).

Bowker, G. and Star, S.L. (2000) *Sorting Things Out: Classification and its Consequences.* Cambridge, MA: MIT Press.

boyd, d. (2011) 'Social network sites as networked publics: affordances, dynamics and implications', in Papacharissi, Z. (ed.) *A Networked Self: Identity, Community and Culture on Social Network Sites*. New York: Routledge, pp. 39-59.

boyd, d. (2012) 'The politics of "real names"', *Communications of the ACM,* 55(8), pp. 29–31. doi: https://doi.org/10.1145/2240236.2240247

Breckenridge, K. (2014) *Biometric State*. Cambridge: Cambridge University Press.

Brensinger, J. and Eyal, G. (2021) 'The sociology of personal identification', *Sociological Theory*, 39(4), pp. 265–292. doi: https://doi.org/10.1177/07352751211055771

Brockmann, H., Drews, W. and Torpey, J. (2021) 'A class for itself? On the worldviews of the new tech elite', PLOS ONE, 16(1), pp. 1-26. doi: https://doi.org/10.1371/journal.pone.0244071

Broeders, D., Cristiano, F. and Kaminska, M. (2023) 'In search of digital sovereignty and strategic autonomy: normative power Europe to the test of its geopolitical ambitions', *Journal of Common Market Studies*, pp. 1-20. doi: https://doi.org/10.1111/jcms.13462

Broeders, D. and Hampshire, J. (2013) 'Dreaming of seamless borders: ICTs and the pre-emptive governance of mobility in Europe', *Journal of Ethnic and Migration Studies*, 39(8), pp. 1201–1218. doi: https://doi.org/10.1080/1369183X.2013.787512

Broeders, D. and Taylor, L. (2017) 'Does great power come with great responsibility? The need to talk about corporate political responsibility', in Taddeo, M. and L. Floridi (eds.) *The Responsibilities of Online Service Providers*. Cham: Springer International Publishing, pp. 315–323.

Broomfield, H. and Reutter, L. (2022) 'In search of the citizen in the datafication of public administration', *Big Data & Society*, 9(1), pp. 1-14. doi: https://doi.org/10.1177/20539517221089302

Brown, W. (2016) 'Sacrificial citizenship: neoliberalism, human capital, and austerity politics, *Constellations*, 23(1), pp. 3–14. doi: https://doi.org/10.1111/1467-8675.12166

Brubaker, R. (1992) *Citizenship and Nationhood in France and Germany*. Cambridge: Harvard University Press.

Brubaker, R. and Cooper, F. (2000) 'Beyond "identity"', *Theory and Society* 29, pp. 1-47.

Brühl, T. and Hofferberth, M. (2013) 'Global companies as social actors: constructing private business in global governance', in Mikler, J. (ed.) *The Handbook of Global Companies*. London: Wiley, pp. 351–370. doi: https://doi.org/10.1002/9781118326152.ch21

Bruton, F. and Nissenbaum, H. (2015) *Obfuscation: A User's Guide for Privacy and Protest*. Cambridge, MA: MIT University Press.

Budnitsky, S. (2022) 'A relational approach to digital sovereignty: e-Estonia between Russia and the West', *International Journal of Communication* 16, pp. 1918–1939.

Burgess, M. (2022) 'Why the GDPR is failing', *Wired*, 23 May. Available at: https://www.wired.co.uk/article/gdpr-2022 (Accessed: 16 May 2023).

Burrell, J. and Fourcade, M. (2021) 'The society of algorithms', *Annual Review of Sociology*, 47(1), pp. 213–237. doi: https://doi.org/10.1146/annurev-soc-090820-020800

Buzan, B. and Waever, O. (2003) *Regions and Powers*. Cambridge: Cambridge University Press.

Calzada, I. (2023) 'Emerging digital citizenship regimes: pandemic, algorithmic, liquid, metropolitan, and stateless citizenships', *Citizenship Studies*, 27(2), pp. 160–188. doi: https://doi.org/10.1080/13621025.2021.2012312.

Cameron, K. (2005) *Laws of identity*. Available at: https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (Accessed: 15 February 2023).

Caplan, J. and Higgs, E. (2013) 'Afterword: the future of identification's past: reflections on the development of historical identification studies', in About, I., Brown, J., and Lonergan, G. (eds.) *Identification and Registration Practices in Transnational Perspective*. London: Palgrave Macmillan UK, pp. 302–308.

Caplan, J. and Torpey, J. (2001) 'Introduction', in Caplan, J. and Torpey, J. (eds.) *Documenting Individual Identity: The Development of State Practices in the Modern World*. Princeton: Princeton University Press, pp. 1-12.

Carnejo, C. and Johnson, S. (2019) 'Understanding blockchain. From medieval origins to modern applications', in Alman, S., and Hirsh, S. (eds.) *Blockchain*. Chicago: ALA Neal-Schuman, pp. 14-18.

Castles, S. (2005) 'Hierarchical citizenship in a world of unequal nation-states', *Political Science and Politics*, 38(4), pp. 689-692. doi: https://doi-org.ezproxy.is.ed.ac.uk/10.1017/S1049096505050353

Castles, S. (2005) 'Nation and empire: hierarchies of citizenship in the new global order', *International Politics*, 42(2), pp. 203–224. doi: https://doi.org/10.1057/palgrave.ip.8800107.

Castronova, E. and Fairfield, J. (2014) 'The digital wallet revolution', *New York Times*, 10 September. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3068296 (Accessed: 10 May, 2024).

Center for Human Rights & Global Justice (2022). *Paving a digital road to Hell? A primer on the role of the world bank and global networks in promoting digital ID*. Available at: https://chrgj.org/wp-content/uploads/2022/06/Report_Paving-a-Digital-Road-to-Hell.pdf (Accessed: 10 July 2023).

Chakravarty, S.P. (2006) 'Regional variation in banking services and social exclusion', *Regional Studies*, 40(4), pp. 415-428. doi: 10.1080/00343400600632747

Charmaz, K., (2006). *Constructing Grounded Theory: A Practical Guide Through Qualitative Analysis*. Thousand Oaks, CA: SAGE.

Charmaz, K. (2014) *Constructing Grounded Theory.* London: SAGE Publications.

Chaudhuri, B. and König, L. (2018) 'The Aadhaar scheme: a cornerstone of a new citizenship regime in India?', *Contemporary South Asia*, 26(2), pp. 127–142. doi: https://doi.org/10.1080/09584935.2017.1369934

Chaum, D. (1985) 'Security without identification: transaction systems to make big brother obsolete', *Communications of the ACM*, 28(10), pp. 1030–1044. doi: 10.1145/4372.4373

Cheesman, M. (2020) 'Self-Sovereignty for refugees? The contested horizons of digital identity', *Geopolitics*, pp. 1–26. doi: https://doi.org/10.1080/14650045.2020.1823836

Cheesman, M. and Slavin, A. (2021) 'Self-sovereign identity and forced migration: slippery terms and the refugee data apparatus' in Korkmaz, E. (ed.) *Digital identity, virtual borders and social media*. Cheltenham: Edward Elgar Publishing, pp. 10-32.

Cheney-Lippold, J. (2017). *We Are Data: Algorithms and the Making of Our Digital Selves*. New York: NYU Press.

Cheqd (n.d.) *Web 3.0 and digital identity*. Available at: https://cheqd.io/web-3.0-and-digital-identity (Accessed 24 January 2023).

Clarke, J. *et al*. (2014) *Disputing Citizenship*. Bristol: Policy Press.

Cloud Signature Consortium (n.d.) *New EU eIDAS Regulation a quantum leap for electronic identity*. Available at: https://cloudsignatureconsortium.org/new-eu-eidas-regulation-a-quantum-leap-for-electronic-identity/ (Accessed: 24 May 2023).

Cohen, J.E. (2018) 'The biopolitical public domain: the legal construction of the surveillance economy', *Philosophy & Technology*, 31(2), pp. 213–233. doi: https://doi.org/10.1007/s13347-017-0258-2

Collier, B. (2024) *Tor: From the Dark Web to the Future of Privacy*. Cambridge, MA: MIT University Press.

Collins, R. (2019) *The Credential Society*. New York: Columbia University Press.

Council of the European Union (2022) *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity - General approach*. Available at: https://data.consilium.europa.eu/doc/document/ST-14959-2022-INIT/en/pdf (Accessed: 9 February 2023).

Couture, S. and Toupin, S. (2019) 'What does the notion of "sovereignty" mean when referring to the digital?', *New Media & Society* 21(10), pp. 2305-2322. doi: https://doi.org/10.1177/1461444819865984

Croxton, D. (1999) 'The peace of Westphalia of 1648 and the origins of sovereignty', *The International History Review*, 21(3), pp. 569–591. doi: https://doi.org/10.1080/07075332.1999.9640869

Cucko, S. and Turkanovic, M. (2021) 'Decentralized and self-sovereign identity: systematic mapping study', *IEEE Access*, 9, pp. 139009–139027. doi: https://doi.org/10.1109/ACCESS.2021.3117588

Cukier, K. and Mayer-Schönberger, V. (2013) 'The rise of big data: how it's changing the way we think about the world', *Foreign Affairs* 92(3), pp. 28-40. doi: 10.1515/9781400865307-003

Culpepper, P.D. and Thelen, K. (2020) 'Are we all Amazon primed? Consumers and the politics of platform power', *Comparative Political Studies*, 53(2), pp. 288–318. doi: https://doi.org/10.1177/0010414019852687

Curran, J., Fenton, N., and Freedman, D. (2016) *Misunderstanding the internet*. London: Routledge.

Custers, B. (2016) 'Click here to consent forever: expiry dates for informed consent', *Big Data & Society*, 3(1), pp. 1-6. doi: https://doi.org/10.1177/2053951715624935

Dahl, R.A. (1957) 'The concept of power', *Behavioral Science*, 2(3), pp. 201–215. doi: https://doi.org/10.1002/bs.3830020303

Danaher, J. (2022) 'Techno-optimism: an analysis, an evaluation and a modest defence', *Philosophy & Technology*, 35(2), pp. 1-29. doi: https://doi.org/10.1007/s13347-022-00550-2

Dardy, C. (1998). *Identités de papiers*. Paris: L'Harmattan.

DC4EU (2023) *About DC4EU*. Available at: https://www.dc4eu.eu/project/ (Accessed: 13 December 2023).

De Filippi, P. (2018) 'Citizenship in the era of blockchain-based virtual nations', in Bauböck, R. (ed.) *Debating Transformations of National Citizenship*. New York: Springer, pp. 267-278.

De Filippi, P. and Loveluck, B. (2016) 'The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure', *Internet Policy Review*, 5(3), pp. 1-28. doi:10.14763/2016.3.427

De Filippi, P., Mannan, M. and Reijers, W. (2020) 'Blockchain as a confidence machine: the problem of trust & challenges of governance', *Technology in Society*, 62, pp. 1-14. doi: https://doi.org/10.1016/j.techsoc.2020.101284

De Goede, M. (2016) 'Afterword: transversal politics', in Guillaume, X. and Bilgin, P. (eds.) *Routledge Handbook of International Political Sociology*. London: Routledge, pp. 355-367.

De Rosa, P. (2024) *Architecture and Reference Framework*. Available at: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md (Accessed: 12 June 2024).

De Salve, A., *et al.* (2022) 'Selective Disclosure in Self-Sovereign Identity based on Hashed Values', *2022 IEEE Symposium on Computers and Communications (ISCC)*, Rhodes, Greece: IEEE, pp. 1–8. Available at: https://doi.org/10.1109/ISCC55528.2022.9913052.

Deibert, R.J. and Pauly, L.W. (2019) 'Mutual entanglement and complex sovereignty in cyberspace', in Bigo, D., Isin, E. and Ruppert, E. (eds.) *Data Politics: Worlds, Subjects, Rights*. London: Routledge, pp. 81-99.

Delanty, G. (2007)' European citizenship: a critical assessment', *Citizenship Studies*, 11(1), pp. 63-72. doi: 10.1080/13621020601099872

Deleuze, G., and Parnet, C. (1987) *Dialogues II*. New York: Columbia University Press.

Demchak, C.C., and Dombrowski, P. (2011) 'Rise of a cybered Westphalian Age', *Strategic Studies Quarterly* 5(1), pp. 32-61. doi: http://www.jstor.org/stable/26270509

Dencik, L. (2022) 'Data and capitalism', in Dencik, L., *et al.* (eds.) *Data Justice*. London: Sage Publications, pp. 13-23.

Dencik, L. *et al.* (2019) 'Exploring data justice: conceptions, applications and directions', *Information, Communication & Society*, 22(7), pp. 873–881. doi: https://doi.org/10.1080/1369118X.2019.1606268

D'Ignazio, C. (2017) 'Creative data literacy: bridging the gap between the data-haves and data-have nots', *Information Design Journal* 23(1), pp. 6-18. doi: 10.1075/idj.23.1.03dig

D'Ignazio, C. and Klein, L. (2020) *Data Feminism*. Cambridge, MA: MIT University Press.

Dijstelbloem, H. and Broeders, D. (2015) 'Border surveillance, mobility management and the shaping of non-publics in Europe', *European Journal of Social Theory*, 18(1), pp. 21–38. doi: https://doi.org/10.1177/1368431014534353

Dira (2023) 'Digital skills in the Roma community'. Available at: https://www.hdl.fi/wp-content/uploads/2023/03/DIRA_SurveyReport_final.pdf (Accessed: 17 July 2024).

Dorschel, R. (2022) 'Reconsidering digital labour: bringing tech workers into the debate', *New Technology, Work and Employment*, 37(2), pp. 288–307. doi: https://doi.org/10.1111/ntwe.12225

Drèze, J., *et al*. (2017), 'Aadhaar and food security in Jharkhand', *Economic & Political Weekly*, 52(50), pp. 50-60.

Eaton, B., Hedman, J. and Medaglia, R. (2018) 'Three different ways to skin a cat: financialization in the emergence of national e-ID solutions', *Journal of Information Technology*, 33(1), pp. 70–83. doi: https://doi.org/10.1057/s41265-017-0036-8

Edwards, L. and Veale, M. (2018) 'Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?', *IEEE Security & Privacy*, 16(3), pp. 46–54. Available at: https://doi.org/10.1109/MSP.2018.2701152.

Enisa (2018) *eIDAS: Overview on the implementation and uptake of Trust Services*. Available at: https://www.enisa.europa.eu/publications/eidas-overview-on-the-implementation-and-uptake-of-trust-services?v2=1 (Accessed: 18 May 2023).

Epicenter Works (n.d.) *eID & public infrastructure*. Available at: https://epicenter.works/en/thema/eid-digital-public-infrastructures#:~:text=With%20the%20creation%20of%20easy,opened%20to%20the%20private%20sector (Accessed: 14 August 2024).

Epstein, C. (2007) 'Guilty bodies, productive bodies, destructive bodies: crossing the biometric borders', *International Political Sociology*, 1(2), pp. 149-164.

European Central Bank (2023) *The digital euro*. Available at: https://www.ecb.europa.eu/paym/digital_euro/html/index.en.html (Accessed: 6 November 2023).

European Commission (2019) *Take control of your virtual identity*. Available at: https://commission.europa.eu/system/files/2019-10/virtual_idenitity_en.pdf (Accessed: 16 May 2023).

European Commission (2020) *A European strategy for data*. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066 (Accessed: 7 November 2023).

European Commission (2021) *Impact assessment report accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity*. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021SC0124 (Accessed: 13 August 2024).

European Commission (2021) *2030 Digital Compass: the European way for the digital decade*. Available at: https://op.europa.eu/en/publication-detail/-/publication/d4220021-8d20-11eb-b85c-01aa75ed71a1/language-en (Accessed: 24 September 2023).

European Commission (2022) *European Declaration on Digital Rights and Principles for the Digital Decade*. Available at: https://digital-strategy.ec.europa.eu/en/library/declaration-european-digital-rights-and-principles#Declaration (Accessed: 19 May 2023).

European Commission (2023) *A trusted and secure digital identity for all Europeans – Questions and Answers**. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2664 (Accessed: 6 November, 2023).

European Commission (2023b) *EU Digital identity: 4 projects launched to test EUDI Wallet*. Available at: https://digital-strategy.ec.europa.eu/en/news/eu-digital-identity-4-projects-launched-test-eudi-wallet (Accessed: 6 November 2023).

European Commission (2023c) *European Digital Identity Wallet pilot implementation*. Available at: https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation (Accessed: 23 May 2023).

European Commission (2023d) *Discover eIDAS.* Available at: https://digital-strategy.ec.europa.eu/en/policies/discover-eidas (Accessed: 22 May 2023).

European Commission (2023e) *Commission welcomes final agreement on EU Digital Identity Wallet*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_5651 (Accessed: 6 November 2023).

European Commission (2023f) *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 (Accessed: 22 July 2024).

European Commission (2024) *A digital ID and personal digital wallet for EU citizens, residents and businesses*. Available at: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home (Accessed: 13 August 2024).

European Commission (2024b) *EU Digital Identity Wallet toolbox process*. Available at: https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox (Accessed: 13 August 2024).

European Commission (2024c) *The many use cases of the EU Digital Wallet*. Available at: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/The+many+use+cases+of+the+EU+Digital+Identity+Wallet (Accessed: 22 April 2024).

European Commisison (2024d) *The security and privacy features of the EU digital identity wallet.* Available at: https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Security+and+Privacy (Accessed: 14 August 2204).

European Commission (2024e) *European Data Governance Act*. Available at: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act (Accessed: 19 May 2023).

European Commission (2024f) *Data Act*. Available at: https://digital-strategy.ec.europa.eu/en/policies/data-act (Accessed: 19 May 2023).

European Commission (n.d.) *European digital identity*. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en (Accessed: 9 February 2023).

European Commission (n.d.-b) *The Digital Services Act: ensuring a safe and accountable online environment*. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en (Accessed: 19 May 2023).

European Commission (n.d.-c) *The Digital Markets Act: ensuring fair and open digital markets*. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en (Accessed: 22 May 2023).

European Commission (n.d.-d) *Europe's digital decade: digital targets for 2023*. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (Accessed: 9 February 2023)

European Council (2022) *European digital identity (eID): Council makes headway towards EU digital wallet, a paradigm shift for digital identity in Europe*. Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/european-digital-identity-eid-council-adopts-its-position-on-a-new-regulation-for-a-digital-wallet-at-eu-level/ (Accessed: 9 February 2023).

European Council (2022b) *A digital future for Europe*. Available at: https://www.consilium.europa.eu/en/policies/a-digital-future-for-europe/ (Accessed 9 February 2023).

European Council (2024) *European digital identity (eID): Council adopts legal framework on a secure and trustworthy digital wallet for all Europeans*. Available at: https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts11-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/#:~:text=The%20European%20digital%20identity%20wallet&text=Under%20the%20new%20law%2C%20member,%2C%20qualifications%2C%20bank%20account (Accessed: 22 April 2024).

European Parliament (2023) *MEPs back plans for an EU-wide digital wallet*. Available at: https://www.europarl.europa.eu/news/pt/press-room/20230206IPR72110/meps-back-plans-for-an-eu-wide-digital-wallet (Accessed: 9 February 2023).

European Parliament (n.d.) *European Digital Identity Framework*. Available at: https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2021/0136(COD)&l=en (Accessed: 23 May 2023).

European Wallet Consortium (2023) *Project*. Available at: https://eudiwalletconsortium.org/project/ (Accessed: 6 November 2023).

Eurostat (2022) 'Individuals' level of digital skills (from 2021 onwards)'. Available at: https://ec.europa.eu/eurostat/cache/metadata/en/isoc_sk_dskl_i21_esmsip2.htm (Accessed: 6 December 2023).

EWC (2023) *User Journey*. Available at: https://eudiwalletconsortium.org/project/user-journey/ (Accessed: 13 December 2023).

Faustino, S. (2019) 'How metaphors matter: an ethnography of blockchain-based re-descriptions of the world', *Journal of Cultural Economy*, 12(6), pp. 478–490. doi: https://doi.org/10.1080/17530350.2019.1629330

Faustino, S., Faria, I. and Marques, R. (2022) 'The myths and legends of king Satoshi and the knights of blockchain', *Journal of Cultural Economy*, 15(1), pp. 67–80. doi: https://doi.org/10.1080/17530350.2021.1921830

Flanagan, H. (2023) *Government-issued digital credentials and the privacy landscape*. Available at: https://openid.net/wp-content/uploads/2023/08/Government-issued-Digital-Credentials-and-the-Privacy-Landscape-v1-1-final.pdf (Accessed: 16 October 2023).

Floridi, L. (2020) 'The fight for digital sovereignty: what it is, and why it matters, especially for the EU', *Philosopy & Technology*, 33, pp. 369–378. doi: https://doi.org/10.1007/s13347-020-00423-6

Flynn, D. (2009) 'Unease about strangers: leveraging anxiety as the basis for policy', in Noxolo, P. and Huymans, J. (eds) *Community, citizenship and the 'war on terror'*. Basingstoke: Palgrave Macmillan, pp. 154-172.

Follows, T. (2023) 'Apple vision pro signals another move into digital identity for Apple', *Forbes,* 15 June. Available at: https://www.forbes.com/sites/traceyfollows/2023/06/15/apple-vision-pro-signals-another-move-into-digital-identity-for-apple/ (Accessed: 15 July 2023).

Foucault, M. (1977) *Discipline and Punish: The Birth of the Prison*. New York, NY: Vintage Books.

Fourcade, M. (2021) 'Ordinal citizenship', *The British Journal of Sociology*, 72(2), pp. 154–173. doi: https://doi.org/10.1111/1468-4446.12839

Fourcade, M. and Gordon, J. (2020) 'Learning like a state: statecraft in the digital age', *Journal of Law and Political Economy* 1(1), pp. 78-108. doi: https://doi.org/10.5070/LP61150258

Fourcade, M. and Healy, K. (2013) 'Classification situations: life-chances in the neoliberal era', *Accounting, Organizations & Society* 38, pp. 559- 572. doi: http://dx.doi.org/10.1016/j.aos.2013.11.002

Fourcade, M. and Healy, K. (2016) 'Seeing like a market', *Socio-Economic Review*, pp. 9-29. doi: https://doi.org/10.1093/ser/mww033

Fourcade, M. and Healy, L. (2024) *The Ordinal Society*. Cambridge, MA: Harvard University Press.

Fourcade, M. and Kluttz, D.N. (2020) 'A Maussian bargain: accumulation by gift in the digital economy', *Big Data & Society*, 7(1), pp. 1-16. doi: https://doi.org/10.1177/2053951719897092

GDPREU (2022) *The impact of GDPR on KYC checks 2022- What you need to know?* Available at: https://www.gdpreu.org/impact-of-gdpr-on-kyc/ (Accessed: 7 December 2023).

Gelb, A. and Clark, J. (2013) *Identification for development: the biometrics revolution*. Center for Global Development Working Paper No. 315. Available at: http://dx.doi.org/10.2139/ssrn.2226594 (Accessed: 15 May 2024).

Giannopoulou, A. (2023) 'Digital identity infrastructures: a critical approach of self-sovereign identity', *Digital Society*, 2(2), pp. 1-18. doi: https://doi.org/10.1007/s44206-023-00049-z

Giannopoulou, A. and Wang, F. (2021) 'Self-sovereign identity', *Internet Policy Review* 10(2), pp. 1-10. doi: https://doi.org/10.14763/2021.2.1550

Glas, R., *et al*. (2019) *The Playful Citizen: Civic Engagement in a Mediatized Culture*. Amsterdam: Amsterdam University Press.

Glasze, G. et al. (2023) 'Contested spatialities of digital sovereignty', *Geopolitics*, 28(2), pp. 919–958. doi: https://doi.org/10.1080/14650045.2022.2050070

Glazer, B. G. and Strauss, A. L. (1967). *The Discovery of Grounded Theory*. London: Aldine Transaction.

Glouftsios, G. and Scheel, S. (2021) 'An inquiry into the digitisation of border and migration management: performativity, contestation and heterogeneous engineering', *Third World Quarterly*, 42(1), pp. 123–140. doi: https://doi.org/10.1080/01436597.2020.1807929

Glyn, M. (2005) *The Idea of a European Superstate: Public Justification and European Integration*. Princeton: Princeton University Press.

Goffman, E. (1963) *Stigma: Notes on the Management of Spoiled Identity*. New York, NY: Simon and Schuster.

Golumbia, D. (2016) *The Politics of Bitcoin: Software as Right-Wing Extremism*. Minneapolis: University of Minnesota Press.

Golumbia, D. (2018) 'Zealots of the blockchain: the true believers of the blockchain cult', *The Baffler*, 38, pp. 102-111. Available at: https://thebaffler.com/salvos/zealots-of-the-blockchain-golumbia (Accessed: 10 May 2024).

Grech, A., Sood, I. and Ariño, L. (2021) 'Blockchain, self-sovereign identity and digital credentials: promise versus praxis in education', *Frontiers in Blockchain*, 4, pp. 1-12. doi: https://doi.org/10.3389/fbloc.2021.616779

Grönlund, Å. (2010), "Electronic identity management in Sweden: governance of a market approach", *Identity in the Information Society*, 3(1), pp. 195 - 211. doi: 10.1007/s12394-010-0043-1

Gstrein, O.J. and Kochenov, D. (2020) 'Digital identity and distributed ledger technology: paving the way to a neo-feudal brave new world?', *Frontiers in Blockchain*, 3, pp. 1-8. doi: https://doi.org/10.3389/fbloc.2020.00010

Gstrein, O.J. and Kochenov, D.V. (2021) 'Blockchain and citizenship: uneasy bedfellows', in Pollicino, O. and De Gregorio, G. (eds.) *Blockchain and Public Law.* Cheltenham: Edward Elgar Publishing.

Guest, G., Namey, E. and Mitchell, M., (2013). *Collecting Qualitative Data: A Field Manual for Applied Research*. London: SAGE Publications, Ltd.

Haimson, O. L., and Hoffmann, A. L. (2016) 'Constructing and enforcing "authentic" identity online: Facebook, real names, and non-normative identities', *First Monday* 21(6). doi: https://doi.org/10.5210/fm.v21i6.6791

Halpin, H. (2020) 'A critique of immunity passports and W3C decentralized identifiers', *Security Standardisation Research: 6th International Conference,* London, UK, November 30 – December 1. doi: https://doi.org/10.1007/978-3-030-64357-7_7

Hardman, D. (2021) 'SSI architecture: the big picture', in Preukschat, A. and Reed, D. (eds.) *Self-Sovereign Identity*. Shelter Island: Manning, pp. 87-109.

Hargittai, E. (2018) 'The digital reproduction of digital inequality', in Grusby, D. and Szelényi, S (eds.) *The Inequality Reader: Contemporary and Foundational Readings in Race, Class, and Gender*. New York: Routledge, pp. 936-944.

Hayward, C. and Lukes, S. (2008) 'Nobody to shoot? Power, structure, and agency: a dialogue', *Journal of Power*, 1(1), pp. 5–20. doi: https://doi.org/10.1080/17540290801943364

Hearn, A. (2017) 'Verified: self-presentation, identity management, and selfhood in the age of big data', *Popular Communication*, 15(2), pp. 62–77. doi: https://doi.org/10.1080/15405702.2016.1269909

Heaton, J. (2022) '"*Pseudonyms Are Used Throughout": A Footnote, Unpacked', *Qualitative Inquiry*, 28(1), pp. 123–132. doi: https://doi.org/10.1177/10778004211048379

Hendrikse, R. *et al.* (2022) 'The Big Techification of everything', *Science as Culture*, 31(1), pp. 59–71. doi: https://doi.org/10.1080/09505431.2021.1984423

Herian, R. (2018) *Regulating Blockchain: Critical Perspectives in Law and Technology*. London: Routledge.

Hicks, J. (2020) 'Digital ID capitalism: how emerging economies are re-inventing digital capitalism', *Contemporary Politics*, pp. 1–21. doi: https://doi.org/10.1080/13569775.2020.1751377

Hicks, J. (2023) 'The geopolitical shaping of digital ID in Asia: ten years of digital Asia', *Asiascape: Digital Asia*, 10(1–2), pp. 208–225. doi: https://doi.org/10.1163/22142312-bja10048

Hindess, B. (2002) 'Neo-liberal citizenship', *Citizenship Studies*, 6(2), pp. 127–143. doi: https://doi.org/10.1080/13621020220142932

Hintz, A. (2020) 'Digital citizenship in the age of datafication', in Yates, S. J. and Rice, R. E. (eds.) *The Oxford Handbook of Digital Technology and Society*. Oxford: Oxford University Press, pp. 526-546.

Hintz, A. (2022) 'Data and citizenship', in Dencik, L., *et al.* (eds.) *Data Justice*. London: Sage, pp. 74-86.

Hintz, A. (2022) 'Data and policy', in Dencik, L., *et al.* (eds.) *Data Justice*. London: Sage, pp. 89-104.

Hintz, A., Dencik, L., and Wahl-Jorgensen, K. (2018) *Digital Citizenship in a Datafied Society*. London: Polity Press.

Hockenhull, M. and Cohn, M.L. (2021) 'Hot air and corporate sociotechnical imaginaries: performing and translating digital futures in the Danish tech scene', *New Media & Society*, 23(2), pp. 302–321. doi: https://doi.org/10.1177/1461444820929319

Hoff, J.V. and Hoff, F.V. (2010) 'The Danish eID case: twenty years of delay', *IDIS* 3, pp. 155–174. doi: https://doi.org/10.1007/s12394-010-0056-9

Hofman, D. et al. (2021) 'Blockchain governance: de facto (x)or designed?', in Lemieux, V.L. and Feng, C. (eds) *Building Decentralized Trust*. Cham: Springer International Publishing, pp. 21–33.

Howlett, M. (2022) 'Looking at the "field" through a Zoom lens: methodological reflections on conducting online research during a global pandemic', *Qualitative Research*, 22(3), pp. 387–402. doi: https://doi.org/10.1177/1468794120985691

Huang, B., Cadwell, P. and Sasamoto, R. (2023) 'Challenging ethical issues of online ethnography: reflections from researching in an online translator community', *The Translator* 29(2), pp. 157-174.

Hughes, E. (1993) *A cypherpunk's manifesto*. Available at: https://nakamotoinstitute.org/cypherpunk-manifesto/ (Accessed: 26 July 2023).

Hummel, P., *et al*. (2021) 'Data sovereignty: a review', in *Big Data & Society* 8(1), pp. 1-17. doi: https://doi.org/10.1177/2053951720982012

Huseby, D. (2020) 'A unified theory of decentralization', *Medium*, 31 July. Available at: https://medium.com/swlh/a-unified-theory-of-decentralization-151d6f39e38 (Accessed: 30 July 2023).

Hussain, S.O. (2020) 'Prefigurative post-politics as strategy: the case of government-led blockchain projects', *The Journal of The British Blockchain Association*, 3(1), pp. 1–11. doi: https://doi.org/10.31585/jbba-3-1-(2)2020

Husz, O. (2018) 'Bank identity: banks, ID cards, and the emergence of a financial identification society in Sweden', *Enterprise & Society*, 19(2), pp. 391–429. doi: https://doi.org/10.1017/eso.2017.43

Husz, O. (2021) 'Money cards and identity cards: *De-vicing* consumer credit in post-war Sweden', *Journal of Cultural Economy*, 14(2), pp. 139–158. doi: https://doi.org/10.1080/17530350.2020.1719868

Iliadis, A. and Russo, F. (2016) 'Critical data studies: an introduction', *Big Data & Society*, 3(2), pp. 1-7. doi: https://doi.org/10.1177/2053951716674238

Infominer and Young, K. (2021) 'The origins of the SSI community' in Preukschat, A. and Reed, D. (eds.) *Self-Sovereign Identity*. Shelter Island: Manning, pp. 310-322.

International Organization for Migration (2023) *Access to digital identity for people on the move in Europe*. Available at: https://publications.iom.int/ system/files/pdf/pub2023-075-r-access-to-digital-identity.pdf (Accessed: 19 August 2024).

Irish Council on Civil Liberties (2023) *5 years: GDPR's crisis point*. Available at: https://www.iccl.ie/digital-data/iccl-2023-gdpr-report/ (Accessed: 17 May 2023).

Ishmaev, G. (2021) 'Sovereignty, privacy, and ethics in blockchain-based identity management systems', *Ethics and Information Technology*, 23(3), pp. 239–252. doi: https://doi.org/10.1007/s10676-020-09563-x

Isin, E. and Ruppert, E. (2015) *Being Digital Citizens*. London: Rowman & Littlefield International.

Isin, E. and Ruppert, E. (2017) 'Citizen Snowden', *International Journal of Communication*, 11, pp. 843-857.

Isin, E. and Ruppert, E. (2020) *Being digital citizens.* 2nd edition. London: Rowman & Littlefield International.

Isin, E. and Turner, B. (2002) *Handbook of Citizenship Studies*. London: SAGE Publications.

ISO (n.d.) *Standards*. Available at: https://www.iso.org/standards.html (Accessed: 11 July 2024).

Jacobsen, K. (2012) 'Unique Identification: inclusion and surveillance in the Indian biometric assemblage', *Security Dialogue*, 43(5): pp. 457–74. doi: https://doi.org/10.1177/0967010612458336

Jarvis, C. (2021) 'Cypherpunk ideology: objectives, profiles, and influences (1992–1998)', *Internet Histories*, pp. 1–27. doi:10.1080/24701475.2021.1935547

Jasanoff, S. and Kim, S.-H. (2009) 'Containing the atom: sociotechnical imaginaries and nuclear power in the United States and South Korea', *Minerva*, 47(2), pp. 119–146. doi: https://doi.org/10.1007/s11024-009-9124-4.

Jasanoff, S. and Kim, S.-H. (2015) *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. University of Chicago Press.

Jia, L., Nieborg, D.B. and Poell, T. (2022) 'On super apps and app stores: digital media logics in China's app economy', *Media, Culture & Society*, 44(8), pp. 1437–1453. doi: https://doi.org/10.1177/01634437221128937

Joergensen, R.F. (2014) 'The unbearable lightness of user consent', *Internet Policy Review*, 3(4), pp. 1-14. doi: https://doi.org/10.14763/2014.4.330

Johnson Jeyakumar, I.H., Chadwick, D.W. and Kubach, M. (2022) 'A novel approach to establish trust in verifiable credential issuers in Self-sovereign identity ecosystems using TRAIN', *Open Identity Summit 2022*, Gesellschaft für Informatik, Bonn 7 July. doi:18.18420/OID2022-02

Joppke, C. (2007) 'Transformation of citizenship: status, rights, identity', *Citizenship Studies*, 11(1), pp. 37-48. doi: 10.1080/13621020601099831

Joppke, C. (2010) 'The inevitable lightening of citizenship', *The European Journal of Sociology*, 51(1), pp. 9-32. doi: 10.1017/S0003975610000019

Joppke, C. (2019) 'The instrumental turn of citizenship', *Journal of Ethnic and Migration Studies*, 45(6), pp. 858-878. doi: 10.1080/1369183X.2018.1440484

Kaasa, A. and Andriani, L. (2022) 'Determinants of institutional trust: the role of cultural context', *Journal of Institutional Economics*, 18(1), pp. 45–65. doi: https://doi.org/10.1017/S1744137421000199

Kaharevic, A. and Skill, K. (2021) 'Digital citizenship in a Swedish marginalised neighbourhood: different attitudes to and experiences of digital inclusion and eHealth', *eJournal of eDemocracy and Open Government*, 13(1). doi: https://doi.org/10.29379/jedem.v13i1.637

Kettunen, A. (2023) 'Wallet wars? It's the war of ecosystems!'. Available at: https://www.mydata.org/2023/04/27/wallet-wars-its-the-war-of-ecosystems/ (Accessed: 28 September 2023).

Khan, R. (2024) [LinkedIn Post]. Available at: https://www.linkedin.com/posts/ronny-khan-1b564377_walletadoption-groundbreakinglegislation-activity-7166146701743927298-79yb?utm_source=share&utm_medium=member_desktop (Accessed: 8 September 2023).

Khera, R. (2019). *Dissent on Aadhaar: Big data Meets Big Brother*. Haiderabad: Orient BlackSwan.

Kim, E.-S. (2018) 'Sociotechnical Imaginaries and the globalization of converging technology policy: technological developmentalism in South Korea', *Science as Culture*, 27(2), pp. 175–197. doi: https://doi.org/10.1080/09505431.2017.1354844

Kim, Y., *et al*. (2022) 'Social class—not income inequality—predicts social and institutional trust', *Social Psychological and Personality Science*, 13(1), pp. 186–198. doi: https://doi.org/10.1177/1948550621999272

Kitchin, H. A. (2003) 'The tri-council policy statement and research in cyberspace: research ethics, the internet, and revising a 'living document', *Journal of Academic Ethics* 1, pp. 397-418. doi: 10.1023/b:jaet.0000025671.83557.fa

Kitchin, R. (2021) *Data Lives: How Data Are Made and Shape Our World*. Bristol: Bristol University Press.

Klein, N. (2020) 'New screen deal: under cover of mass death, Andrew Cuomo calls in the billionaires to build a high-tech dystopia', *The Intercept*, 8 May. Accessible at: https://theintercept.com/2020/05/08/andrew-cuomo-eric-schmidt-coronavirus-tech-shock-doctrine/ (Accessed: 22 September 2023).

Kloppenburg, S. and van der Ploeg, I. (2020) 'Securing identities: biometric technologies and the enactment of human bodily differences', *Science as Culture*, 29(1), pp. 57–76. doi: https://doi.org/10.1080/09505431.2018.1519534

König, P.D. (2022) 'Fortress Europe 4.0? An analysis of EU data governance through the lens of the resource regime concept', *European Policy Analysis*, 8(4), pp. 484–504. doi: https://doi.org/10.1002/epa2.1160.

Kotka, T. et al (2015) *Estonian e-Residency: redefining the nation-state in the digital er.* University of Oxford, Cyberstudies Programme, Working Paper No. 3. Available at: https://www.ctga.ox.ac.uk/article/estonian-e-residency-redefining-nation-state-digital-era (Accessed: 5 April 2024).

Kozinetz, R. V. (2015). *Netnography*. London: SAGE.

Kulyk, O., Gerber, N., Hilt, A., and Volkamer, M. (2020) 'Has the GDPR hype affected users' reaction to cookie disclaimers?', *Journal of Cybersecurity*, 6(1), pp. 1-14. doi: https://doi.org/10.1093/cybsec/tyaa022

Kymlicka, W. (1995) *Multicultural Citizenship: A Liberal Theory of Minority Rights*. Oxford: Clarendon Press.

Kymlicka, W. and Norman, W. (1994) 'Return of the citizen: a survey of recent work on citizenship theory', *Ethics*, 104(2), pp. 352–381. doi: https://doi.org/10.1086/293605

Laatikainen, G. et al (2021), 'Towards a trustful digital world: exploring self-sovereign identity ecosystems'. *Pacific Asia Conference on Information Systems*, Dubai, 12-14 July. Available at: https://aisel.aisnet.org/pacis2021/19 (Accessed: 4 April 2024).

Lahman, M.K.E., Thomas, R. and Teman, E.D. (2023) 'A Good Name: Pseudonyms in Research', *Qualitative Inquiry*, 29(6), pp. 678–685. doi: https://doi.org/10.1177/10778004221134088

Latonero, M. (2019) 'Stop surveillance humanitarianism', *New York Times*, July 11. Available at: https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html (Accessed: 15 July 2023).

Lauer, J. (2020) 'Plastic surveillance: payment cards and the history of transactional data, 1888 to present', *Big Data & Society*, 7(1), pp. 1-14. doi: https://doi.org/10.1177/2053951720907632

Leese, M. (2014) 'The new profiling: algorithms, black boxes, and the failure of anti- discriminatory safeguards in the European Union', *Security Dialogue*, 45(5), pp. 494–511. doi: https://doi.org/10.1177/0967010614544204

Leese, M. (2016) 'Exploring the security/facilitation nexus: Foucault at the 'smart' border', *Global Society*, 30(3), pp. 412-429. doi: https://doi.org/10.1080/13600826.2016.1173016

Leese, M. (2022) 'Fixing State Vision: Interoperability, Biometrics, and Identity Management in the EU', *Geopolitics*, 27(1), pp. 113–133. doi: https://doi.org/10.1080/14650045.2020.1830764

Lemberg-Pedersen, M. and Haioty, E. (2020) 'Re-assembling the surveillable refugee body in the era of data-craving', *Citizenship Studies*, 24(5), pp. 607–624. doi: https://doi.org/10.1080/13621025.2020.1784641

Lemons, M.A. and Parzinger, M. (2007) 'Gender schemas: a cognitive explanation of discrimination of women in technology', *Journal of Business and Psychology*, 22(1), pp. 91–98. doi: https://doi.org/10.1007/s10869-007-9050-0

Liang, F. *et al*. (2018) 'Constructing a data-driven society: China's social credit system as a state surveillance infrastructure', *Policy & Internet*, 10(4), pp. 415–453. doi: https://doi.org/10.1002/poi3.183

Lin, A. and Silva, L. (2005) 'The social and political construction of technological frames', *European Journal of Information Systems*, 14(1), pp. 49–59. doi: https://doi.org/10.1057/palgrave.ejis.3000521

Lipps, J. and Schraff, D. (2021) 'Regional inequality and institutional trust in Europe', *European Journal of Political Research*, 60(4), pp. 892–913. doi: https://doi.org/10.1111/1475-6765.12430

Lips, M. (2010) 'Rethinking citizen – government relationships in the age of digital identity: Insights from research', *Information Polity*, 15(4), pp. 273–289. doi: https://doi.org/10.3233/IP-2010-0216

Lips, M. (2013) 'Reconstructing, attributing and fixating citizen identities in digital-era government', *Media, Culture & Society*, 35(1), pp. 61–70. doi: https://doi.org/10.1177/0163443712464559

Lofretto, D. (2012) 'Sovereign source authority', *The Moxy Tongue*, 28 June. Available at: https://www.moxytongue.com/2012/06/golden-jellybean.html (Accessed: 6 December 2023).

Longman, T. (2001) 'Identity cards, ethnic self-perception, and genocide in Rwanda' in Caplan, J. and Torpey, J. (eds.) *Documenting individual identity: The Development of State Practices in the Modern World*. Princeton: Princeton University Press, pp. 345-357.

Lopez-Claros, A., Dahl, A.L. and Groff, M. (2020) 'European Integration: Building Supranational Institutions', in *Global Governance and the Emergence of Global Institutions for the 21st Century*. Cambridge: Cambridge University Press, pp. 65–78.

Lyon, D. (2003) *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination.* London: Routledge.

Lyon, D. (2007) 'National ID Cards: Crime-Control, Citizenship and Social Sorting', *Policing*, 1(1), pp. 111–118. doi: https://doi.org/10.1093/police/pam015

Lyon D (2007b) *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Lyon, D. (2008) 'Biometrics, identification and surveillance', *Bioethics*, 22(9), pp. 499–508. 30. doi: 10.1111/j.1467-8519.2008.00697.x

Lyon, D. (2009) *Identifying citizens: ID cards as surveillance*. Cambridge: Polity Press.

Lyon, D. (2010) 'National IDs in a global world: surveillance, security and citizenship', *Case Western Reserve Journal of International Law*, 42(3), pp. 607-623.

Lyon, D. (2022) 'Surveillance', *Internet Policy Review* 11(4), pp. 2-19. doi: https://doi.org/10.14763/2022.4.1673.

Luhmann, N. (1979) *Trust and Power*. New York: John Wiley.

Lukes, S. (2004). *Power: A Radical View*. 2nd edition. London: Red Globe Press.

Lukkien, B., Bharosa, N. and De Reuver, M. (2023) 'Barriers for developing and launching digital identity wallets'. *Proceedings of the 24th Annual International Conference on Digital Government Research*. *DGO 2023: Digital government and solidarity*, Gdansk, 11-24 July, pp. 289–299. doi: https://doi.org/10.1145/3598469.3598501

Lupton, D. (2021) '"Not the real me": social imaginaries of personal data profiling', *Cultural Sociology*, 15(1), pp. 3–21. doi: https://doi.org/10.1177/1749975520939779

McCallum, S. (2023) 'Meta: Facebook owner fined €1.2bn for mishandling data', *BBC*, 23 May. Available at: https://www.bbc.co.uk/news/technology-65669839 (Accessed: 25 May 2023).

McConvey (2024) 'As eIDAS 2.0 takes effect, EU faces 'paradigm shift for digital identity in Europe', *Biometric Update*, 7 May. Available at: https://www.biometricupdate.com/202405/as-eidas-2-0-takes-effect-eu-faces-paradigm-shift-for-digital-identity-in-europe (Accessed: 23 July 2024).

McDade, M. (2023) 'The top 10 identity and access management solutions', *Expert Insights*, 6 February. Available at: https://expertinsights.com/insights/top-10-identity-and-access-management-solutions/ (Accessed: 17 January 2023).

MacDonald, A. (2023) 'Bhutan launches self-sovereign biometric digital ID, crown prince first to enroll', *Biometric update*, February 23. Available at: https://www.biometricupdate.com/202302/bhutan-launches-self-sovereign-biometric-digital-id-crown-prince-first-to-enroll (Accessed 21 July 2023).

MacKenzie, D. (2005) 'Opening the black boxes of global finance', *Review of International Political Economy*, 12(4), pp. 555–576. doi: https://doi.org/10.1080/09692290500240222

MacKenzie, D. and Spinardi, G. (1988) 'The shaping of nuclear weapon system technology: US fleet ballistic missile guidance and navigation: I: from Polaris to Poseidon', *Social Studies of Science*, 18(3), pp. 419–463. doi: https://doi.org/10.1177/030631288018003002

MacKenzie, D. A. and Wajcman, J. (1985) *The Social Shaping of Technology: How the Refrigerator Got its Hum*. Milton Keynes: Open University Press.

MacKenzie, D.A. and Wajcman, J. (1999) *The Social Shaping of Technology*. 2nd ed. Buckingham: Open University Press.

McNeil, M. *et al*. (2017) 'Conceptualizing imaginaries of science, technology, and society', in Felt, U. *et al*. (eds.) *The Handbook of Science and Technology Studies.* Cambridge: MIT Press, pp. 435-464.

Madianou, M. (2019) 'The biometric assemblage: surveillance, experimentation, profit, and the measuring of refugee bodies', *Television & New Media*, 20(6), pp. 581–599. doi: https://doi.org/10.1177/1527476419857682

Madianou, M. (2019b) 'Technocolonialism: digital innovation and data practices in the humanitarian response to refugee crises', *Social Media + Society*, 5(3), pp. 1-13. doi: https://doi.org/10.1177/2056305119863146

Madiega, T. (2020) 'Digital sovereignty for Europe'. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf (Accessed: 1 May, 2023).

Madon, S. and Schoemaker, E. (2021) 'Digital identity as a platform for improving refugee management', *Information Systems Journal*, 31(6), pp. 929–953. doi: https://doi.org/10.1111/isj.12353

Magalhães, J. C. and Couldry, C. (2021) 'Giving by taking away: big tech, data colonialism, and the reconfiguration of social good', *International Journal of Communication* 15, pp. 343–362.

Magnet, S.A. (2011) *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham: Duke University Press.

Malone, E.A. and Wright, D. (2018) '"To promote that demand": toward a history of the marketing white paper as a genre', *Journal of Business and Technical Communication,* 32(1), pp. 113–147. doi: https://doi.org/10.1177/1050651917729861

Manby, B. (2020) '"Legal Identity for All" and statelessness: opportunity and threat at the junction of public and private international law', *Statelessness and Citizenship Review* 2(2), 248–271. doi: https://doi.org/10.2139/ssrn.3783310

Manby, B. (2021) 'The sustainable development goals and "Legal Identity for All": "First, do no harm"', *World Development*, 139, pp. 248-271. doi: https://doi.org/10.1016/j.worlddev.2020.105343

Mann, M., (1986) 'The sources of social power Vol.1', in Haugaard, M. (ed.) *Power: A Reader*. Manchester: Manchester University Press, pp. 166–180.

Marshall, T. H. (1950) *Citizenship and Social Class*. Cambridge: Cambridge University Press.

Martin, A. (2021) 'Aadhaar in a box? Legitimizing digital identity in times of crisis', *Surveillance & Society* 19(1), pp. 104-108. doi: https://doi.org/10.24908/ss.v19i1.14547

Martin, A. *et al*. (2023) 'Digitisation and sovereignty in humanitarian space: technologies, territories and tensions', *Geopolitics*, 28:3, pp. 1362-1397. doi: 10.1080/14650045.2022.2047468

Martin, A. and Taylor, L. (2021) 'Exclusion and inclusion in identification: regulation, displacement and data justice', *Information Technology for Development*, 27(1), pp. 50–66. doi: https://doi.org/10.1080/02681102.2020.1811943

Martin, A.K. and Whitley, E.A. (2013) 'Fixing identity? Biometrics and the tensions of material practices', *Media, Culture & Society*, 35(1), pp. 52–60. doi: https://doi.org/10.1177/0163443712464558

Martin, C. (2023) 'The Wallet Wars', *Continuum Loop*, 2 February. Accessible at: https://www.continuumloop.com/wallet-wars/ (Accessed 3 October 2023).

Masiero, S. (2020) 'COVID-19: What does it mean for digital social protection?', *Big Data & Society*, 7(2), p. 205395172097899. doi: https://doi.org/10.1177/2053951720978995

Masiero, S. (2023) 'Digital identity as platform-mediated surveillance', *Big Data & Society* 10(1), pp. 1-5. doi: https://doi.org/10.1177/20539517221135176.

Masiero, S. and Arvidsson, V. (2021) 'Degenerative outcomes of digital identity platforms for development', *Information Systems Journal*, 31(6), pp. 903–928. doi: https://doi.org/10.1111/isj.12351

Masiero, S. and Bailur, S. (2021) 'Digital identity for development: the quest for justice and a research agenda', *Information Technology for Development*, 27(1), pp. 1–12. doi: https://doi.org/10.1080/02681102.2021.1859669

Masiero, S. and Shakthi, S. (2020) 'Grappling with Aadhaar: biometrics, social identity and the Indian state', *South Asia Multidisciplinary Academic Journal* (23), pp. 1-11. doi: https://doi.org/10.4000/samaj.6279

Mattli, W. and Büthe, T. (2003) 'Setting international standards: technological rationality or primacy of power?', *World Politics*, 56(1), pp. 1–42. doi: https://doi.org/10.1353/wp.2004.0006
Mavelli, L. (2022) *Neoliberal citizenship*. Oxford: Oxford University Press.

May, T. C. (1988) *The crypto anarchist manifesto*. Available at: https://nakamotoinstitute.org/crypto-anarchist-manifesto/ (Accessed 26 January 2023).

Medaglia, R. *et al*. (2022) 'Mechanisms of power inscription into IT governance: lessons from two national digital identity systems', *Information Systems Journal*, 32(2), pp. 242–277. doi: https://doi.org/10.1111/isj.12325

Melgaço, L. and Monaghan, J. *Protests in the Information Age*. London: Routledge.

Meijas, U.A. and Couldry, N. (2019) 'Datafication', *Internet Policy Review* 8(4), pp. 1-10. doi: https://doi.org/10.14763/2019.4.1428

Michael, M (2000) 'Futures of the present: from performativity to prehension', in Brown, N. and Rappert, B. (eds.) *Contested Futures*. London: Routledge.

Mobey Forum (2023) 'Mobey Forum: Now is the time for banks to secure role in digital identity'. Accessible at: https://mobeyforum.org/mobey-forum-now-is-the-time-for-banks-to-secure-role-in-digital-identity/ (Accessed: 26 September 2023).

Möllers, N. (2021) 'Making digital territory: cybersecurity, techno-nationalism, and the moral boundaries of the state', *Science, Technology, & Human Values,* 46(1), pp. 112–138. doi: https://doi.org/10.1177/0162243920904436

Monsees, L. et al (2023) 'Transversal politics of big tech', *International Political Sociology*, 17(1), pp. 1-23. doi: https://doi.org/10.1093/ips/olac020

Morozov, E. (2013) *To Save Everything, Click Here*. London: Penguin.

Morris, J.W. and Murray S. (2018) *Appified: Culture in the Age of Apps*. Ann Arbor, MI: University of Michigan Press.

Mossberger, K., Tolbert, C. J. and McNeal, R. S. (2007) *Digital Citizenship: The Internet, Society and Participation*. Cambridge, MA: MIT University Press.

Moxy Tongue (2023) 'The Moxy Tongue'. Available at: https://www.moxytongue.com/ (Accessed: 2 August 2023).

Mühle, A. (2023) 'One to bind them: binding verifiable credentials to user attributes', *International Conference on Security and Cryptography*, Lisbon, 10-12 July, pp. 345-352. doi: DOI10.5220/0012057900003555

Mühle, A. *et al.* (2018) 'A survey on essential components of a self-sovereign identity', *Computer Science Review*, 30, pp. 80–86. doi: https://doi.org/10.1016/j.cosrev.2018.10.002

Mukta, R. *et al.* (2020) 'Blockchain-based verifiable credential sharing with selective disclosure', in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Guangzhou, China, 29 December – 1 January 2023, pp. 959–966. doi: 10.1109/TrustCom50675.2020.00128

Müller, B. (2004) '(Dis)qualified bodies: securitization, citizenship and 'identity management', *Citizenship Studies*, 8(3), pp. 279-294. doi: https://doi.org/10.1080/1362102042000257005

Müller, B. (2010) 'Unsafe at any speed? Borders, mobility and 'safe citizenship'', *Citizenship Studies*, 14(1), pp. 75-88. doi: https://doi.org/10.1080/13621020903466381

Müller, M. and Schurr, C. (2016) 'Assemblage thinking and actor-network theory: conjunctions, disjunctions, cross-fertilisations', *Transactions of the Institute of British Geographers*, 41(3), pp. 217–229. doi: https://doi.org/10.1111/tran.12117

Mützel, S. (2021) 'Unlocking the payment experience: Future imaginaries in the case of digital payments', *New Media & Society*, 23(2), pp. 284–301. doi: https://doi.org/10.1177/1461444820929317

Nader, L. (2018) *Contrarian Anthropology: The Unwritten Rules of Academia*. New York: Berghahn Books.

Naik, N. and Jenkins, P. (2020) 'Self-sovereign identity specifications: govern your identity through your digital wallet using blockchain technology', in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, Oxford: 3-6 August, pp. 90–95. doi: https://doi.org/10.1109/MobileCloud48802.2020.00021

Nair, V. (2019) 'Governing India in cybertime: biometric IDs, start-ups and the temporalised state', *South Asia: Journal of South Asian Studies*, 42(3), pp. 519–536. doi: https://doi.org/10.1080/00856401.2019.1598122

Nakomoto, S. (2008) *Bitcoin: a peer-to-peer electronic cash system*. Available at: https://bitcoin.org/en/bitcoin-paper (Accessed: 26 July 2023).

National Science Board (2018) 'Technical Standards, Invention, Innovation, and Economic Growth'. Available at: https://www.nsf.gov/statistics/2018/nsb20181/assets/1178/technical-standards-invention-innovation-and-economic-growth.pdf (Accessed: 11 July 2024).

Nguyen, L.T.V. *et al.* (2020) 'Collective empowerment in online communities: conceptualization, scale refinement, and validation', *Journal of Marketing Theory and Practice*, 28(3), pp. 301–317. doi: https://doi.org/10.1080/10696679.2020.1758568

Niklas, J. and Dencik, L. (2021) 'What rights matter? Examining the place of social rights in the EU's artificial intelligence policy debate', *Internet Policy Review*, 10(3). doi: https://doi.org/10.14763/2021.3.1579

NOBID Consortium (2024) 'The NOBID Project'. Available: https://www.nobidconsortium.com/our-proposal/ (Accessed: 13 May 2024).

Nogueira, J. P. (2017) 'Global governance and the politics of inequality: problematizing controversies in the field of international development', in Basaran, T., *et al*. (eds.) *International Political Sociology: Transversal Lines*. New York: Routledge, pp. 165-184.

Noiriel, G. (2001) 'The Identification of the Citizen: The Birth of Republican Civil Status in France', in Caplan, J. and Torpey, J. (eds.) *Documenting individual identity: The Development of State Practices in the Modern World*. Princeton: Princeton University Press, pp. 28-48.

Norris, T. (2023) 'Educational futures after COVID-19: big tech and pandemic profiteering versus education for democracy', *Policy Futures in Education* 21(1), pp. 34-57. doi: https://doi.org/10.1177/14782103221080265

Noxolo, P. and Huymans, J. (2009) 'Introduction: community, citizenship, and the 'War on Terror': security and insecurity', in Noxolo, P. and Huymans, J. (eds.) *Community, Citizenship and the 'War on Terror'*. Basingstoke: Palgrave Macmillan, pp. 1-10.

Nyqvist,A., Høyer Leivestad, H. and Tunestad, H.(2017) 'Individuals and industries: large-Scale professional gatherings as ethnographic fields', in Høyer Leivestad, H. and Nyqvist, A. (eds.) *Ethnographies of Conferences and Trade Fairs*. Cham: Springer International Publishing.

Nyst C., *et al*. (2016) *Digital identity: issue analysis: executive summary*. Available at: https://chyp.com/wp-content/uploads/2020/06/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf (Accessed: 10 June 2024).

O'Donnel, D. (2021) 'Digital wallets and digital agents' in Preukschat, A. and Reed, D. (eds.) *Self-Sovereign Identity*. Shelter Island: Manning, pp. 189-219.

OECD (2018) 'Case study – India'. Available at: https://www.oecd.org/gov/innovative-government/India-case-study-UAE-report-2018.pdf (Accessed: 6 February 2024).

Orgad, L. (2018) 'Cloud communities: the dawn of global citizenship?', in Bauböck, R. (ed.) *Debating Transformations of National Citizenship*. New York: Springer, pp. 251-260.

Orlikowski, W. J. (1992) 'The duality of technology: rethinking the concept of technology in organizations', *Organization Science*, *3*(3), pp. 398–427.

Orlikowski, W.J. and Gash, D.C. (1994) 'Technological frames: making sense of information technology in organizations', *ACM Transactions on Information Systems*, 12(2), pp. 174–207. doi: https://doi.org/10.1145/196734.196745

Oudshoorn, N., Neven, L. and Stienstra, M. (2016) 'How diversity gets lost: age and gender in design practices of information and communication technologies', *Journal of Women & Aging*, 28(2), pp. 170–185. doi: https://doi.org/10.1080/08952841.2015.1013834

Oudshoorn, N., Pinch, T. (2003) *How Users Matter: The Co-Construction of Users and Technology*. Cambridge, MA: MIT Press.

Oudshoorn, N., Rommes, E. and Stienstra, M. (2004) 'Configuring the user as everybody: gender and design cultures in information and communication technologies', *Science, Technology, & Human Values*, 29(1), pp. 30–63. doi: https://doi.org/10.1177/0162243903259190

Paasonen, S. (2011) 'Revisiting cyberfeminism', *Communications*, 36(3). doi: https://doi.org/10.1515/comm.2011.017.

Palm, E. (2016) 'Conflicting interests in the development of a harmonized EU e- passport', *Journal of Borderlands Studies*, 31(2), pp. 203-218. doi: 10.1080/08865655.2016.1181982

Palmer, S. (2021) 'Digital green pass, vaccine passport, EUDCC: What is it and who can use it?', *Euronews* June 9. Available at: https://www.euronews.com/travel/2021/06/09/digital-green-pass-vaccine-passport-eudcc-a-guide-to-post-pandemic-travel-documents (Accessed: 22 August).

Paloque-Bergès, C. and Schafer, V. (2019) 'Arpanet', *Internet Histories* 3(1), pp. 1-14. doi: https://doi.org/10.1080/24701475.2018.1560921.

Pangrazio, L. (2016) 'Reconceptualising critical data literacy', *Discourse: Studies in the Cultural Politics of Education* 37(2), pp. 163-174. doi: http://dx.doi.org/10.1080/01596306.2014.942836

Pangrazio, L. and Sefton-Green, J. (2021) 'Digital rights, digital citizenship and digital literacy: what's the difference?', *Journal of New Approaches in Educational Research*, 10(1), pp. 15-27. doi: https://doi.org/10.7821/naer.2021.1.616

Pangrazio, L. and Selwyn, N. (2019) '"Personal data literacies": a critical literacies approach to enhancing understandings of personal digital data', *New Media & Society*, 21(2), pp. 419–437. doi: https://doi.org/10.1177/1461444818799523

Pansardi, P. (2012) '*Power to* and *power over*: two distinct concepts of power?', *Journal of Political Power*, 5(1), pp. 73–89. doi: https://doi.org/10.1080/2158379X.2012.658278

Park, A., *et al*. (2022) 'Interoperability: our exciting and terrifying Web3 future', *Business Horizons* 66(4), pp. 1-25. doi: https://doi.org/10.1016/j.bushor.2022.10.005

Pelizza, A. (2019) 'Processing alterity, enacting Europe: migrant registration and identification as co-construction of individuals and polities', *Science, Technology, & Human Values*, 45(2), pp. 262–288. doi: https://doi.org/10.1177/0162243919827927

Pelizza, A. (2021) 'Identification as translation: the art of choosing the right spokespersons at the securitized border', *Social Studies of Science*, 51(4), pp. 487–511. doi: https://doi.org/10.1177/0306312720983932

Perala, A. and Counter, P. (2023) 'Apple mobile driver's license arrives in Georgia', *Mobile ID World*, May 19. Available at: https://mobileidworld.com/apple-mobile-drivers-license-arrives-in-georgia/ (Accessed: 26 September 2023).

Peters, J. (2022) 'Arizona is the first state to put its driver's license and state ID in Apple's Wallet', *The Verge*, March 23. Available at: https://www.theverge.com/2022/3/23/22992745/apple-wallet-license-arizona-colorado-hawaii-real-id (Accessed: 26 September 2023).

Pfotenhauer, S. et al. (2022) 'The politics of scaling', *Social Studies of Science*, 52(1), pp. 3–34. doi: https://doi.org/10.1177/03063127211048945

Pinch, T.J. and Bijker, W.E. (1984) 'The social construction of facts and artefacts: or how the sociology of science and the sociology of technology might benefit each other', *Social Studies of Science*, 14(3), pp. 399–441. doi: https://doi.org/10.1177/030631284014003004

Plantin, J.-C., *et al*. (2018) 'Infrastructure studies meet platform studies in the age of Google and Facebook', *New Media & Society*, 20(1), 293-310. doi: https://doi.org/10.1177/1461444816661553

Pohle, J. and Thiel, T. (2020) 'Digital sovereignty', *Internet Policy Review* 9(4), pp. 2-19. doi: https://doi.org/10.14763/2020.4.1532

Potential (2024) 'Building the future of digital identity in Europe'. Available at: https://www.digital-identity-wallet.eu/ (Accessed: 13 May 2024).

Potential (2024b) '140+ public and private partners'. Available at: https://www.digital-identity-wallet.eu/partners (Accessed: 13 May 2024).

Porter, E. (2020) *The Consumer Citizen*. Oxford University Press.

Preukschat, A. and Reed, D. (2021) 'Why the internet is missing an identity layer – and why SSI can finally provide one', in Preukschat, A., and Reed, D. (eds.) *Self-Sovereign* Identity. Shelter Island: Manning Publications Co., pp. 1-19.

Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (2021). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2021%3A281%3AFIN (Accessed: 4 December 2023).

Rapley, T. and Rees, G. (2018). 'Collecting documents as data', in (ed. Flick, U.) *The SAGE Handbook of Qualitative Data* Collection. London: SAGE Publications Ltd. pp. 378-391

Ratcliff C., Martinello, and Litos, V. (2022) 'Digital Agenda for Europe'. Available at: https://www.europarl.europa.eu/erpl-app-public/factsheets/pdf/en/FTU_2.4.3.pdf (Accessed: 19 May 2023).

Reed, D. (2021) 'SSI governance frameworks' in Preukschat, A. and Reed, D. (eds.) *Self-Sovereign Identity*. Shelter Island: Manning, pp. 248-274.

Reed, D., Joosten, R. and Van Deventer, O. (2021) 'The basic building blocks of SSI' in Preukschat, A. and Reed, D. (eds.) *Self-Sovereign Identity*. Shelter Island: Manning, pp. 21-38.

Reed, D. and Sabadello, M. (2021) 'Decentralized identifiers', in Preukschat, A. and Reed, D. (eds.) *Self-Sovereign Identity*. Shelter Island: Manning, pp, 157-186.
Reed, I.A. (2013) 'Power: relational, discursive, and performative dimensions', *Sociological Theory* 31(3), pp. 193-218. Available at: DOI: 10.1177/0735275113501792

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), *Official Journal* L 119, p. 1–88.

Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (2024) *Official Journal* L, 1-56.

Reijers, W., O'Brolcháin, F. and Haynes, P. (2016) 'Governance in blockchain technologies & social contract theories', *Ledger*, 1, pp. 134–151. doi: 10.5195/ledger.2016.62

Rist, O. (2021) 'The best identity management solutions for 2023', *PC Mag*, 18 November. Available at: https://uk.pcmag.com/migrated-46739-onlinecloud-backup-services/71363/the-best-identity-management-solutions-for-2020 (Accessed: 17 January 2023).

Roberts, H. et al. (2021) 'Safeguarding European values with digital sovereignty: an analysis of statements and policies', *Internet Policy Review*, 10(3). doi: https://doi.org/10.14763/2021.3.1575

Røvik, R. (2023) 'Kick-off for NOBID and large scale piloting of the EU digital wallet'. Available at: https://www.nobidconsortium.com/kick-off-for-nobid-and-large-scale-piloting-of-the-eu-digital-wallet/ (Accessed: 7 November 2023).

Rühlig, T.N. (2020) 'Technical standardisation, China and the future international order. A European Perspective'. Available at: https://eu.boell.org/sites/default/files/2020-03/HBS-Techn%20Stand-A4%20web-030320.pdf (Accessed: 2 October 2023).

Ruppert, E. (2018) 'Sociotechnical Imaginaries of Different Data Futures: An Experiment in Citizen Data'. *3e Van Doornlezing*, Rotterdam, Netherlands, 14 July. Available at: https://www.eur.nl/sites/corporate/files/2018-06/3e%20van%20doornlezing%20evelyn%20ruppert.pdf (Accessed: 2 May 2024).

Rygiel, K. (2011) 'Governing borderzones of mobility through e-borders: the politics of embodied mobility', in Squire, V. (ed.) *The Contested Politics of Mobility*. Oxon: Routledge, pp. 143- 168.

Sadowski, J. (2019) 'When data is capital: Datafication, accumulation, and extraction', *Big Data & Society*, 6(1), pp. 1-12. doi: https://doi.org/10.1177/2053951718820549

Sadowski, J. (2020) 'The internet of landlords: digital platforms and new mechanisms of rentier capitalism', *Antipode*, 52(2), pp. 562–580. doi: https://doi.org/10.1111/anti.12595

Sadowski, J. and Beegle, K. (2023) 'Expansive and extractive networks of Web3', *Big Data & Society*, 10(1), pp. 1-14. doi: https://doi.org/10.1177/20539517231159629

Salter, M. (2004) 'Passports, mobility and security: how smart can the border be?', *International Studies Perspectives*, 5(1), pp. 71-91. doi: https://doi.org/10.1111/j.1528-3577.2004.00158.x

Sassen, S. (2006) *Territory, Authority, Rights. From Medieval to Global Assemblages*. Princeton: Princeton University Press.

Scammell, M. (2000) 'The Internet and Civic Engagement: The Age of the Citizen-Consumer', *Political Communication*, 17(4), pp. 351–355. Available at: https://doi.org/10.1080/10584600050178951.

Schinkel, W. and Van Houdt, F. (2010) 'The double helix of cultural assimilationism and neo-liberalism: citizenship in contemporary governmentality', *The British Journal of Sociology*, 61(4), pp. 696–715. Available at: https://doi.org/10.1111/j.1468-4446.2010.01337.x.

Schmidt, D. C. (2018) 'Google data collection'. Available on: https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf (accessed 15 February 2023).

Schneier, B. (2019) 'There's no good reason to trust blockchain technology', *Wired*, 6 February. Available at: https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/ (Accessed: 29 July 2013).

Schoemaker, E., *et al*. (2021) 'Identity at the margins: data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda', *Information Technology for Development*, 27(1), pp. 13–36. doi: https://doi.org/10.1080/02681102.2020.1785826

Schoemaker, E., Martin, A. and Weitzberg, K. (2023) 'Digital identity and inclusion: tracing technological transitions', *Georgetown Journal of International Affairs*, 24(1), pp. 36–45. doi: https://doi.org/10.1353/gia.2023.a897699

Scott, J.C. (2020) *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed.* New Haven: Yale University Press.

Scott, M. (2019) 'What's driving Europe's new aggressive stance on tech', *Politico*, 27 October. Available at: https://www.politico.eu/article/europe-digital-technological-sovereignty-facebook-google-amazon-ursula-von-der-leyen/ (Accessed: 2 October 2023).

Seaver, N. (2017) 'Algorithms as culture: some tactics for the ethnography of algorithmic systems', *Big Data & Society*, 4(2), pp. 1-12. doi: https://doi.org/10.1177/2053951717738104

Sedlmeir, J. *et al.* (2021) 'Digital Identities and verifiable credentials', *Business & Information Systems Engineering*, 63(5), pp. 603–613. doi: https://doi.org/10.1007/s12599-021-00722-y

Semenzin, S. (2020) *Blockchain & Data Justice. The political culture of technology*. Ph.D. Thesis. University of Milan and University of Turin, Italy. Available at: https://iris.unito.it/bitstream/2318/1849682/1/Semenzin_PhD%20thesis.pdf (Accessed: 2 February 2023).

Semenzin, S., Rozas, D. and Hassan, S. (2022) 'Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia', *Policy and Society*, 41(3), pp. 386–401. doi: https://doi.org/10.1093/polsoc/puac014

Sengoopta, C. (2003) *Imprint of the Raj: How Fingerprinting Was Born in Colonial India*. London: Palgrave Macmillan.

Sharon, T. (2021) 'Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers', *Ethics and Information Technology*, 23(S1), pp. 45–57. doi: https://doi.org/10.1007/s10676-020-09547-x

Shaw, J. (2018) 'EU citizenship: still a fundamental status?', in Bauböck, R. (ed.) *Debating Transformations of National Citizenship*. New York: Springer, pp. 1-20.

Siegelberg, M. (2020) *Statelessness: A Modern History*. Cambridge MA: Harvard University Press.

Singh, R. (2019) 'Give Me a Database and I Will Raise the Nation-state.*" Journal of South Asian Studies*, 42(3):501–18. doi: https://doi.org/10.1080/00856401.2019.1602810

Skinner, Q. (2010) 'The sovereign state: a genealogy', in Hent, K. (ed.) *Sovereignty in Fragments*. Cambridge: Cambridge University Press.

Smith, B., Loddo, O.G. and Lorini, G. (2020) 'On Credentials', *Journal of Social Ontology*, 6(1), pp. 47–67. doi: https://doi.org/10.1515/jso-2019-0034

Sovrin (2018) *What is self-sovereign identity?* Available at: https://sovrin.org/faq/what-is-self-sovereign-identity/ (Accessed: 15 January 2023).

Soysal, Y.N. (2012) 'Citizenship, immigration, and the European social project: rights and obligations of individuality', *The British Journal of Sociology*, 63(1), pp. 1–21. doi: https://doi.org/10.1111/j.1468-4446.2011.01404.x

Sparke, M. (2004) 'Passports into credit Cards: on the borders and spaces of neoliberal citizenship', in Joel Migdal (ed.) *Boundaries and Belonging*. Cambridge: Cambridge University Press, pp. 251 - 283.

Sparke, M. (2006) 'A neoliberal nexus: economy, security and the biopolitics of citizenship on the border', *Political Geography*, 25(2), pp. 151-180. doi: https://doi.org/10.1016/j.polgeo.2005.10.002

Sperfeldt, C. (2021) 'Legal identity in the sustainable development agenda: actors, perspectives and trends in an emerging field of research', *The International Journal of Human Rights*, pp. 1–22. doi: https://doi.org/10.1080/13642987.2021.1913409

Sporny, M. *et al*. (2022) *Decentralized Identifiers (DIDs) v1.0. Core architecture, data model, and representations*. Available at: https://www.w3.org/TR/did-core/#dfn-did-documents (Accessed 6 February 2023).

Srnicek, N. (2016) *Platform Capitalism*. London: Wiley.

Statista (2024) 'Digital identity solution market revenue worldwide from 2020 to 2028'. Available at: https://www.statista.com/statistics/1263580/worldwide-digital-identity-solution-market-revenue/ (Accessed: 10 May 2024).

Steinberg, M., Mukherjee, R. and Punathambekar, A. (2022) 'Media power in digital Asia: Super apps and megacorps', *Media, Culture & Society*, 44(8), pp. 1405–1419. doi: https://doi.org/10.1177/01634437221127805

Stevens, R. (2022) 'What is Web3? Understanding what Web3 is…and isn't', *Coinbase*, 19 August. Available at: https://www.coindesk.com/learn/what-is-web-3-and-why-is-everyone-talking-about-it/ (Accessed: 20 January 2023).

Stokkink, Q. and Pouwelse, J. (2018) 'Deployment of a blockchain-based self-sovereign identity', *IEEE International Conference on Blockchain*, Halifax, Canada, 30 July – 3 August. doi: https://doi.org/10.48550/arXiv.1806.01926

Storeng K. T. and De Bengy Puyvallée A (2021) 'The smartphone pandemic: how big tech and public health authorities partner in the digital response to Covid-19', *Global Public Health* 16(8-9), pp. 1482-1498. doi: 10.1080/17441692.2021.1882530

Sullivan, C. (2018) 'Digital identity – from emergent legal concept to new reality', *Computer Law & Security Review*, 34(4), pp. 723–731. doi: https://doi.org/10.1016/j.clsr.2018.05.015

Sullivan, C. and Burger, E. (2019) 'Blockchain, digital Identity, e-government', in Treiblmaier, H. and R. Beck (eds.) *Business Transformation through Blockchain*. Cham: Springer International Publishing, pp. 233–258.

Sümer, B. and Schroeders, J. (2021) 'The new digital identity regulation proposal and the EU data protection regime'. Available at: https://www.law.kuleuven.be/citip/blog/the-new-digital-identity-regulation-proposal/ (Accessed: 24 May 2022).

Swartz, L. (2017) 'Blockchain dreams: imagining techno-economic alternatives after Bitcoin', in Castells, M. (ed.) *Another Economy is Possible: Culture and Economy in a Time of Crisis*. London: Polity Press, pp. 82-105.

Swartz, L. (2018) 'What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology', *Cultural Studies*, 32(4), pp. 623–650. doi: https://doi.org/10.1080/09502386.2017.1416420

Swartz, L. (2020). *New Money: How Payments Became Social Media*. New Haven: Yale University Press.

Sztompka, P. (1999) *Trust. A Sociological Theory*. Cambridge: Cambridge University Press.

Tammpuu, P. and Masso, A. (2019) 'Transnational digital identity as an instrument for global digital citizenship: the case of Estonia's e-residency', *Information Systems Frontiers*, 21(3), pp. 621–634. doi: https://doi.org/10.1007/s10796-019-09908-y

Taylor, L. (2017) 'What is data justice? The case for connecting digital rights and freedoms globally', *Big Data & Society*, 4(2), p. 205395171773633. doi: https://doi.org/10.1177/2053951717736335

Timmermans, S. and Epstein, S. (2010) 'A world of standards but not a standard world: toward a sociology of standards and standardization', *Annual Review of Sociology*, 36(1), pp. 69–89. doi: https://doi.org/10.1146/annurev.soc.012809.102629

Timmermans, S. and Tavory, I. (2012) 'Theory Construction in Qualitative Research: From Grounded Theory to Abductive Analysis', Sociological Theory, 30(3), pp. 167–186. Available at: https://doi.org/10.1177/0735275112457914.

Tkacz, N. (2019) 'Money's new abstractions: Apple Pay and the economy of experience', *Distinktion: Journal of Social Theory*, 20(3), pp. 264–283. doi: https://doi.org/10.1080/1600910X.2019.1653348

Tobin, A. (2022) 'eIDAS 2.0: how Europe can define the digital identity blueprint for the world', *Evernym*, 24 February. Available at: https://www.evernym.com/blog/eidas/ (Accessed 6 February 2024).

Tobin, A. (2023) 'The Identerati are dead: long live the Credentialites', 11 July. Available at: https://www.linkedin.com/pulse/identirati-dead-long-live-credentialites-andrew-tobin/ (Accessed: 11 July 2024).

Tobin, A. and Reed, D. (2016) *The inevitable rise of self-sovereign identity*. Available at: https://sovrin.org/library/inevitable-rise-of-self-sovereign-identity/ (Accessed: 30 July 2023).

Tomlinson, M. (2008) '"The degree is not enough": students' perceptions of the role of higher education credentials for graduate work and employability', *British Journal of Sociology of Education*, 29(1), pp. 49–61. doi: https://doi.org/10.1080/01425690701737457

Torpey, J. (2000) *The Invention of the Passport*. Cambridge: Cambridge University Press.

Trottier, D. (2013) *Identity problems in the Facebook era.* London: Routledge.

Trust over IP Foundation (2021) *Introduction to Trust over IP*. Available at: https://trustoverip.org/wp-content/uploads/Introduction-to-ToIP-V2.0-2021-11-17.pdf (Accessed 25 July 2023).

Turkle, S. (1995) *Life on the Screen: Identity in the Age of the Internet*. Simon & Schuster, New York.

Van Den Meerssche, D. (2022) 'Virtual borders: international law and the elusive inequalities of algorithmic association', *European Journal of International Law*, pp. 171-204. doi: https://doi.org/10.1093/ejil/chac007

Van der Ploeg, I. (1999) 'Written on the body: biometrics and identity', *Computers and Society*, 29(1), pp. 37-44. doi: https://doi.org/10.1145/382042.382051

Van der Vlist, F.N. *et al.* (2024) 'Super-appification: conglomeration in the global digital economy', *New Media & Society* 00(0), p.p. 1-24. Available at: https://doi.org/10.1177/14614448231223419.

Van Bokkem, D. *et al.* (2019) 'Self-sovereign identity solutions: the necessity of blockchain technology'. Available at: http://arxiv.org/abs/1904.12816 (Accessed: 2 February 2022).

Van Deursen, A.J. and Van Dijk, J.A. (2019) 'The first-level digital divide shifts from inequalities in physical access to inequalities in material access', *New Media & Society*, 21(2), pp. 354–375. doi: https://doi.org/10.1177/1461444818797082

Van Dijck, J. (2013) '"You have one identity": performing the self on Facebook and LinkedIn', *Media, Culture & Society*, 35(2), pp. 199–215. doi: https://doi.org/10.1177/0163443712468605

Van Dijck, J. (2014) 'Datafication, dataism and dataveillance: big data between scientific paradigm and ideology', *Surveillance & Society*, 12(2), pp. 197–208. doi: https://doi.org/10.24908/ss.v12i2.4776

Van Dijck, J. and Jacobs, B. (2020) 'Electronic identity services as sociotechnical and political-economic constructs', *New Media & Society*, 22(5), pp. 896–914. doi: https://doi.org/10.1177/1461444819872537

Van Dijck, J., Nieborg, D. and Poell, T. (2019) 'Reframing platform power', *Internet Policy Review* 8(2), pp. 1-18. doi: https://doi.org/10.14763/2019.2.1414

Van Dijk, J. (2020) *The Digital Divide*. Cambridge: Polity Press.

Van Zoonen, L. (2013) 'From identity to identification: fixating the fragmented self', *Media, Culture & Society*, 35(1), pp. 44–51. doi: https://doi.org/10.1177/0163443712464557

Vidan, G. and Lehdonvirta, V. (2019) 'Mine the gap: Bitcoin and the maintenance of trustlessness', *New Media & Society*, 21(1), pp. 42–59. doi: https://doi.org/10.1177/1461444818786220

Viljoen, S. (2021) 'A relational theory of data governance', *The Yale Law Journal* 131(2), pp. 1-76. doi: http://dx.doi.org/10.2139/ssrn.3727562

Viljoen, S. (2021b) 'The promise and limits of lawfulness: inequality, law, and the techlash', in *Journal of Social Computing*, 2(3), pp. 284-296. doi: 10.23919/JSC.2021.0025

Vrabec, H. U. (2021), *Data Subject Rights under the GDPR.* Oxford: Oxford University Press.

Wacjman, J. (2004) *TechnoFeminism*. Cambridge: Polity Press.

Wahl-Jorgensen, K., Bennett, L. and Taylor, G. (2017) 'The normalization of surveillance and the invisibility of digital citizenship: media debates after the Snowden Revelations', *International Journal of Communication* 11, pp. 740-762.

Wall Street Journal (2023) 'Why banks are waging a digital-wallet war with Apple', 29 March. Available at: https://www.wsj.com/video/series/news-explainers/why-banks-are-waging-a-digital-wallet-war-with-apple/AB361EA0-7C80-4ED1-B3DD-723408EAC5F9 (Accessed: 3 October 2023).

Wang, F. and De Filippi, P. (2020) 'Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion', *Frontiers in Blockchain*, 2(28), pp. 1-28. doi: https://doi.org/10.3389/fbloc.2019.00028

Watts, L. (2019). *Energy at the End of the World: An Orkney Islands Saga*. Cambridge: MIT Press.

WC3 (2022) *Decentralized identifiers (DIDs) v1.0 becomes a W3C recommendation*. Available at: https://www.w3.org/2022/07/pressrelease-did-rec.html.en (Accessed 6 February 2023).

Weatherbed, J. (2023) 'Google wallet is getting custom cards and state IDs this month', *The Verge*, 1 June. Accessible at: https://www.theverge.com/2023/6/1/23745168/google-wallet-state-id-drivers-license-custom-cards (Accessed: 26 September 2023).

Weigl, L. *et al.* (2022) 'The EU's digital identity policy: tracing policy punctuations', in *15th International Conference on Theory and Practice of Electronic Governance*. Guimarães, Portugal, 4-7 October, pp. 74–81. doi: https://doi.org/10.1145/3560107.3560121

Weigl, L., Barbereau, T. and Fridgen, G. (2023) 'The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions', *Government Information Quarterly*, 40(4), pp. 1-18. doi: https://doi.org/10.1016/j.giq.2023.101873

Weitzberg, K. (2020) 'Biometrics, race making, and white exceptionalism: the controversy over universal fingerprinting in Kenya', *The Journal of African History*, 61(1), 23–43. Doi: https://doi.org/10.1017/S002185372000002X

Weitzberg, K., *et al*. (2021) 'Between surveillance and recognition: rethinking digital identity in aid', *Big Data & Society* 8(1), pp. 1-7. doi: https://doi.org/10.1177/20539517211006744

Wheelahan, L. and Moodie, G. (2022) 'Gig qualifications for the gig economy: micro-credentials and the "hungry mile"', *Higher Education*, 83(6), pp. 1279–1295. doi: https://doi.org/10.1007/s10734-021-00742-3

Whitley, E.A., Gal, U. and Kjaergaard, A. (2014) 'Who do you think you are? A review of the complex interplay between information systems, identification and identity', *European Journal of Information Systems*, 23(1), pp. 17–35. doi: https://doi.org/10.1057/ejis.2013.34

Whitley, E.A. and Hosein, G. (2010) *Global challenges for identity policies*. Palgrave Macmillan UK.

Whitley, E.A. and Hosein, I.R. (2008) 'Doing the politics of technological decision making: due process and the debate about identity cards in the U.K.', *European Journal of Information Systems*, 17(6), pp. 668-677. doi: 10.1057/ejis.2008.53

Whitley, E.A. and Schoemaker, E. (2022) 'On the sociopolitical configurations of digital identity principles', *Data & Policy*, 4(38), pp. 1-14. doi: https://doi.org/10.1017/dap.2022.30

Williams, R. and Edge, D. (1996) 'The social shaping of technology', *Research Policy* 25, pp. 865-899. doi: https://doi.org/10.1016/0048-7333(96)00885-2

Windley, P.J. (2021) 'Sovrin: an identity metasystem for self-sovereign identity', *Frontiers in Blockchain* 4, pp. 1-14. doi: https://doi.org/10.3389/fbloc.2021.626726

Winner, L. (1980) 'Do artifacts have politics?', *Deadalus* 109(1), pp. 121-136.

Winner, L. (1986) *The Whale and the Reactor*. *A Search for the Limits in the Age of High Technology*. Chicago: Chicago University Press.

Wired (2022) 'Inside the digital wallet revolution', 26 October. Available at: https://www.wired.co.uk/bc/article/inside-the-digital-wallet-revolution-jp-morgan (Accessed: 13 March 2024).

Woodall, A. and Ringel, S. (2020) 'Blockchain archival discourse: trust and the imaginaries of digital preservation', *New Media & Society*, 22(12), pp. 2200–2217. doi: https://doi.org/10.1177/1461444819888756

Woolgar, S. (1990) 'Configuring the user: the case of usability trials', *The Sociological Review*, 38(1), pp. 58-99. doi: https://doi.org/10.1111/j.1467-954X.1990.tb03349.x

World Economic Forum (2018) *Identity in a digital World: a new chapter in the social contract*. Available at: https://www.weforum.org/reports/identity-in-a-digital-world-a-new-chapter-in-the-social-contract/ (Accessed 15 July 2023).

World Economic Forum (2023*) Reimagining Digital ID*. Available at: https://www.weforum.org/reports/reimagining-digital-id/ (Accessed: 10 July 2023).

Young, K. (2018) 'There's a Facebook alternative, it's called self-sovereign identity', *Coindesk,* 6 April. Available at: https://www.coindesk.com/markets/2018/04/06/theres-a-facebook-alternative-its-called-self-sovereign-identity/ (accessed: 6 December 2023).

Young, K. (2022) 'Seeing self-sovereign identity in historical context'. Available at: https://identitywoman.net/wp-content/uploads/Seeing-Self-Sovereign-Identity-in-Historical-Context.pdf (Accessed: 20 June 2024).

Zuboff, S. (2019) *The Age of Surveillance Capitalism*. London: Profile Books.

Zwitter, A.J., Gstrein, O.J. and Yap, E. (2020) 'Digital identity and the blockchain: universal identity management and the concept of the "self-sovereign" individual', *Frontiers in Blockchain*, 3, pp. 1-14. doi: https://doi.org/10.3389/fbloc.2020.00026