Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual

Zwitter, Andrej; Gstrein, Oskar Josef; Yap, Evan

Published in:
Frontiers in Blockchain

DOI:
10.3389/fbloc.2020.00026

Publication date:
2020

frontiers in Blockchain

HYPOTHESIS AND THEORY
published: 28 May 2020
doi: 10.3389/fbloc.2020.00026

Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual

Andrej J. Zwitter[1], *Oskar J. Gstrein*[2]* *and Evan Yap*[3]

[1] University of Groningen, Campus Fryslân Data Research Centre, Professor of Governance and Innovation, Leeuwarden, Netherlands, [2] University of Groningen, Campus Fryslân Data Research Centre, Assistant Professor, Leeuwarden, Netherlands, [3] Lead of Research & Development at Mark Labs, Washington, DC, United States

While "classical" human identity has kept philosophers busy since millennia, "Digital Identity" seems primarily machine related. Telephone numbers, E-Mail inboxes, or Internet Protocol (IP)-addresses are irrelevant to define us as human beings at first glance. However, with the omnipresence of digital space the digital aspects of identity gain importance. In this submission, we aim to put recent developments in context and provide a categorization to frame the landscape as developments proceed rapidly. First, we present selected philosophical perspectives on identity. Secondly, we explore how the legal landscape is approaching identity from a traditional dogmatic perspective both in national and international law. After blending the insights from those sections together in a third step, we will go on to describe and discuss current developments that are driven by the emergence of new tools such as "Distributed Ledger Technology" and "Zero Knowledge Proof." One of our main findings is that the management of digital identity is transforming from a purpose driven necessity toward a self-standing activity that becomes a resource for many digital applications. In other words, whereas traditionally identity is addressed in a predominantly sectoral fashion whenever necessary, new technologies transform digital identity management into a basic infrastructural service, sometimes even a commodity. This coincides with a trend to take the "control" over identity away from governmental institutions and corporate actors to "self-sovereign individuals," who have now the opportunity to manage their digital self autonomously. To make our conceptual statements more relevant, we present several already existing use cases in the public and private sector. Subsequently, we discuss potential risks that should be mitigated in order to create a desirable relationship between the individual, public institutions, and the private sector in a world where self-sovereign identity management has become the norm. We will illustrate these issues along the discussion around privacy, as well as the development of backup mechanisms for digital identities. Despite the undeniable potential for the management of identity, we suggest that particularly at this point in time there is a clear need to make detailed (non-technological) governance decisions impacting the general design and implementation of self-sovereign identity systems.

Keywords: blockchain, digital identity, self-Sovereign identity, governance, innovation, human dignity

OPEN ACCESS

Edited by:
Glenn Parry,
University of Surrey, United Kingdom

Reviewed by:
Kaliya Young,
Merritt College, United States
Richard Tighe,
Oxfam, United Kingdom

***Correspondence:**
Oskar J. Gstrein
o.j.gstrein@rug.nl

Specialty section:
This article was submitted to Blockchain for Good, a section of the journal Frontiers in Blockchain

Received: *13 September 2019*
Accepted: *29 April 2020*
Published: *28 May 2020*

Citation:
Zwitter AJ, Gstrein OJ and Yap E (2020) Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual. Front. Blockchain 3:26. doi: 10.3389/fbloc.2020.00026

INTRODUCTION

As mankind continues its journey through the Digital Age our lives are increasingly becoming compositions of our offline and online activities. While the dimensions of "classical" human identity have kept philosophers busy since millennia[1], traditional thinking about "Digital Identity" is primarily machine related. Telephone numbers, E-Mail inboxes, or Internet Protocol (IP)-addresses seem to be irrelevant to define us as human beings at first glance. However, the discussion about surveillance in the digital domain (Council of Europe, 2018), and jurisprudence of the European Court of Justice (ECJ) struggling to clarify under which conditions IP-addresses should be qualified as personal data (ECJ, 2018; Gstrein and Ritsema van Eck, 2018, p. 80–81), show in detail how these technical necessities make it increasingly difficult to distinguish between our offline and online selves. The omnipresence of digital technology and its use to not only control, but also shape society result in the need to reconsider our world and ourselves as beings (Galič et al., 2017). The technological component of the amalgamation that we call "me" has increased considerably in the last decades (Kucklick, 2014, p. 189–235). When looking at these changes from a holistic perspective, it is almost natural to deduct that this digital space as parallel space does not mirror existing governance structures, power relations, human rights, and legal obligations. "Code is Law"—or at least has sometimes normative authority—and as it spreads across our lives new governance decisions are made by those who shape it in an ex- or implicit manner (Lessig, 1996, p. 1–9). Furthermore, it is not only governmental surveillance and "nudging" that shapes our digital identities right from the start, there is also "surveillance capitalism" (Zuboff, 2019, p. 11–12).

In an attempt to create an explicit and universal process, the United Nations (UN) in late 2013 have made a cautious start to address these developments by "[r]ecognizing that the same rights that people have offline must also be protected online." (United Nations, 2014, p. 2). In 2018 they called upon states to "[…] consider developing or maintaining and implementing adequate legislation, in consultation with all relevant stakeholders, including civil society, with effective sanctions and appropriate remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary collection, processing, retention or use of personal data by individuals, governments, business enterprises and private organizations […]" (United Nations, 2018, p. 6). In this spirit and to ensure that specifically digital identities live up to these requirements, the UN have supported the creation of the ID2020 Alliance[2]. As noble as these intentions might be, large corporations such as those assembled under the GAFAM acronym (Google, Apple, Facebook, Amazon, Microsoft) continue their considerable efforts to create a general identity for logins of digital services they themselves or others provide. It is practically impossible to activate the holy grail of expression in the digital age—the modern smartphone—without one or more accounts that are associated with those big players. However, since these actions result in siloed identities tied to proprietary services and applications (Verborgh, 2019), the advent of digital identity systems based on Blockchain and similar Distributed Ledger Technologies (DLT) might offer the opportunity for change.

More than a decade ago, Cameron (2005) formulated seven laws of identity aiming to guide the way from a patchwork of identity one-offs to a universal identity. Cameron's visionary view on the subject of identity, claims and privacy led him to formulate the following principles: (1) user control and consent; (2) minimal disclosure for a constrained use; (3) justifiable parties; (4) directed identity; (5) pluralism of operators and technologies; (6) human integration; (7) consistent experience across contexts. While it would go too far to explain each of them in detail, one can summarize that Cameron laid the foundational principles that many actors in the field of digital identity are aiming for. Only today, first attempts to a universal identity are made, but the reality remains that the individual is composed of a patchwork of identities, logins, usernames, passwords, etc.

The obstacle to an overarching digital-identity is the enforcement of one standard in cyberspace, as the battle over single-log-on's between Google and Facebook illustrates. Interestingly enough, the solution might not be found in the private, but in the public sector. For example, the Netherlands are using a progressive digital identity management system called "DigiD" which allows residents access to public records and governmental services since several years[3]. Furthermore, Georgia and Sweden used blockchain technology to create an immutable record of land titles, identifying individuals as landowners (Nimfuehr, 2018). The World Food Programme pioneered a similar Blockchain guided approach to biometric ID and digital payments with which refugees in a camp in Jordan could reserve funds and buy goods, without needing physical documents or valets (Juskalian, 2018; Wang and De Filippi, 2020, p. 14–17). Furthermore, the European Union (EU) is contemplating digital identity with the ascend of Schengen II and works on the mobility of identity related credentials in its member states through the implementation of the eIDAS Directive (EU Regulation No 910/2014).

Additionally, the concept of "self-sovereign identity" is emerging. While there is currently no universally and legally binding definition of the concept, Allen (2016) has described it as "[…] the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity." He goes on to propose ten principles that aim at describing the main characteristics of self-sovereign identity. Wang and De Filippi (2020, p. 9–11) discuss his proposal in-depth, and together with the relationship to so-called decentralized identifiers (DIDs), which are a form of URLs (e.g., unique web addresses) that resolve to a DID

[1]For illustrative purposes a bridge can be built from Aristotle who framed the human as "political animal," to Rene Descartes "rational self" in the context of "cogito ergo sum," further to Martin Heidegger's existence or "Dasein": Dieses Seiende, das wir selbst je sind und das unter anderem die Seinsmöglichkeit des Fragens hat, fassen wir terminologisch als Dasein.

[2]Available online at: https://id2020.org (accessed March 4, 2020).

[3]Available online at: https://www.digid.nl/en/what-is-digid (accessed March 4, 2020).

document (Wang and De Filippi, 2020, p. 9)[4]. Wagner et al. (2018, p. 27) have proposed to define self-sovereign identity as "a model of digital identity where individuals and entities alike are in full control over central aspects of their digital identity, including their underlying encryption keys; creation, registration, and use of their decentralized identifiers [. . .] The architecture gives individuals and entities the power to directly control and manage their digital identity without the need to rely on external authorities." In other words, DLT becomes an infrastructure for the creation of verifiable credentials. It allows to verify claims with (increased) independence of governments or powerful intermediaries. Ultimately, this new approach could replace conventional "legal identities."

Furthermore, if such self-sovereign identity management includes verification of claims based on "zero-knowledge proof" (ZKP) technology, the need to exchange and register "raw" personal data on platforms could be limited significantly. Wagner et al. (2018, p. 48) describe ZKP by stating that its "[. . .] use allows two different actors, the "prover" and the "verifier" to exchange the ownership of a piece of data, without actually revealing the data. The math, probability and cryptography behind this technology makes their application useful in for example allowing the verifier to prove the ownership of a credential to the verifier, such as a driving license [sic!] without revealing the identifier it has been initially issued to."

However, all of these attempts do not consider how identity is constructed from a philosophical perspective, what the legal consequences attached to identity look like, and what a universal digital identity should mean. This general lack of understanding of philosophical and legal underpinnings of identity remains prevalent. Nevertheless, upon closer scrutiny this is not surprising. As illustrated below, the concept of identity is ill-defined in the legal domain, and an attempt to define it spans many different fields with relevant norms in national and international legislation, as well as consideration of corresponding jurisprudence. In order to shed light onto what identity is composed of in practice, this paper presents:

1. An overview of selected philosophical perspectives on identity;
2. An overview of legal aspects of identity;
3. Expressions of identity and ways of identification;
4. A categorization of digital identity;
5. A discussion of opportunities and risks around digital identity.

With this primer on digital identity that includes perspectives on self-sovereign identity, we respectfully submit that before we are even able to seek a sustainable technological solution, identity as a concept should be carefully considered, taking into account the development of cyberspace from a philosophical, legal, and ethical perspective. We acknowledge that major strides toward digital identity are currently being undertaken by the DLT community. Furthermore, it is not our aim to replicate and review the significant number of purely technology-related blogs and white papers written on the subject. Rather, we aim to contribute to the concept of digital identity from a philosophical and legal perspective. Thereby, this paper aims to counteract the current trend to immediately jump on technology on the peak of the "hype-cycle" and present it as panacea for all problems.

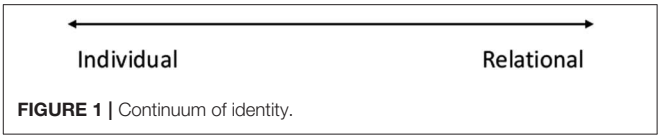

FIGURE 1 | Continuum of identity.

Another important disclaimer is that this paper does not treat digital identity as belonging to DLT exclusively. DLT is just one of many tools that are currently being deployed. Hence other, more centralized systems will also be discussed in their own right. Once these elements are profoundly understood in a larger context and from a legal and philosophical perspective, they can function as determinants of what we need technology to do for digital identities to truly enrich society and make human existence more dignified.

PHILOSOPHICAL PERSPECTIVES ON IDENTITY

The concept of identity in philosophy has many different aspects. Identity plays a central role in logics and metaphysics, in existentialism and other areas. To frame this discussion, we deem it useful to distinguish between two extreme positions at either side of an identity continuum: The naturalist world view ("identity is whole and distinguishable") and the constructivist world view ("identity is compartmentalized and shared"; see **Figure 1**). Roughly, the naturalist argues that identity is tied to the properties of an object or a person. In contrast, the constructivist sees identity as a whole constructed out of the relationship between objects and subjects. As we will show, both result in different degrees to which a universal digital identity can be realized and to what extent such a universal identity is limited by the identity and rights of others.

Naturalist World View

In a simplified manner, the naturalist worldview assumes that everything that resides inside the physical body or is more permanently connected with it forms its identity. It is thus the nature of the physical body and its delineation from other physical bodies that make it unique and distinguishable. From a metaphysical perspective, every physical object has unique properties, be it the position in space, its texture etc. Two objects are non-identical if they differ in at least one of their conditions (e.g., texture, color, composition etc.). Prominent proponents of this world view in recent times include John Dewey, Ernest Nagel, Sidney Hook and Roy Wood Sellars (Papineau, 2016). A common problem around identity is whether an object can be distinguished from another, if it does not differ in any of the conditions that define it as an object. This has already quite profound consequences for digital identity and corresponding problems in data protection, particularly when considering the

[4]Available online at: https://w3c.github.io/did-core/#introduction (accessed March 4, 2020).

use of biometric data for identification purposes (Jasserand, 2018, p. 155). Since digital identity by necessity is a digitalized and reduced reflection of what one voluntarily and involuntarily (e.g., think "data exhaust" or "data trail") projects into the digital sphere, any identity must be sufficiently distinguishable from other identities. **Uniqueness** is thus one criterion that derives from this naturalist world view.

Further assuming that both mind and soul reside in the physical body, this allows us to draw further relevant conclusions on identity. For example, Pythagorean and Platonic transmigration theories ("the wandering soul") raise a rather problematic aspect about whether the physical delineations are correct (Luchte, 2012, p. 174–177). It seems that the naturalist world view becomes already somewhat inconsistent. Does identity actually reside within the boundaries of the body, the soul, or a combination of it? If the answer is Yes, then the physical body is mostly a vessel with sufficient distinctive features for identification. The problem becomes even more pressing as researchers try to use personal profiles on social media and other "data exhaust" of persons to make them digitally "immortal" through the use of artificial intelligence, which also raises the interesting aspect of post-death autonomy or "post mortem privacy" (Harbinja, 2017). If the body has to be considered merely as vehicle for the mind, this means for digital identity and identification that we need to postulate a **Priority Thesis** of mind over matter. This is certainly the case when it comes to questions of uniqueness and of authentication. If the material body is subject to drastic change that can make it a sufficient representation for identification (biometrics), then priority has to be given to the mind for identification (knowledge, passwords, relationships). This leaves us with the following elements for identification:

- Physical body (nature): color of eyes, height, hair color, facial structure, iris, finger, and palm print etc. Essentially, everything that can be used to create biometrical data. Any of these features are subject to change and ultimately serve only as a proxy.
- Non-physical body (nurture): everything that was trained, what one has absorbed into character, education, training, behavior to the extent specific to my identity and sufficiently distinguishable from others. Expressions of the mind in this category are passwords and phrases (security) questions, and answers that only a particular user can know, as well as certain knowledge or abilities.

As argued, two principles of identity and authentication can be derived from the naturalist worldview: Uniqueness ("being sufficiently distinguishable from any other entity") and the Priority Thesis ("expressions of the mind have priority over the physical body"). They, however, raise questions themselves. For example, how distinct from others is an individual if crucial parts of its identity have been formed by nurture such as education, culture etc. which are ultimately derived from other people, and which can also be accessed by other people. This leads us to the other extreme on the identity continuum, constructivist identity.

Constructivist Identity

The extreme position of this view proclaims that identity is wholly shaped by social structure, the relationship with others, the norms and rules that shape the environment, institutions that testify to the existence of an identity (e.g., the government issuing an identity card), and other external factors with which a person interacts ("look at the person with the funny hat" -> becomes "person known for wearing a funny hat"). Social networks, such as LinkedIn and Facebook, very much take this stance: you are who you are connected with. Your social network and the nature of the individual relations to others define your uniqueness. This immediately raises a less discussed subject in the literature around constructivism, namely its relation to network theory. A detailed discussion would go beyond the scope of this primer, but it suffices to say that one important aspect of identity, namely power or the ability to influence others in network theory is a function of centrality within the network. This is helpful when trying to understand how Instagram and Youtube "stars" are able to leverage their identity for fame and financial gains (Rueb, 2019).

Constructivism in a less extreme form would at least argue that identity is relational (**Relationality**). In other words, who you are is a matter of who you relate to and the nature of this relationship. It is therefore not only the relation of identity X to Y (as existent or not existent), but also the relation of X to Y as a father to a son, as brothers, as spouses etc. This view also ties in with the philosophy of Jean-Paul Sartre as he emphasizes that individual identity is shaped by the interaction with "the other person" who is difficult to define in detail. While the environment seems entirely open and explorable to us, the other person is difficult to grasp, yet exists as an undeniable fact (Sartre, 2007, p. 412–413). One more philosophical reference that comes to mind is Georg Wilhelm Friedrich Hegel's dialectic of master and slave (or Lord and Bondsman more precisely). Here, identity is also defined through the role of individuals in society and the relationship they have with each other (Lichtenthähler, 2019, p. 104–123).

Quite commonly, such relationships and family relationships, are registered by governments and expressed through documentation of relational identity such as birth certificates and the entry of someone's marital status into public record. These relational identity features are affecting the legal status of a person. They also define contractual rights and obligations, and other societal obligations such as tax payment. Hence, a public record of these identity features is crucial for society to work. Furthermore, the change in someone's identity can also result in changes for the identity of another person (e.g., with the death of a spouse the other becomes a widower). If identity is relational, information about this identity (often referred to as Personally Identifiable Information or "PII") can also be information about another identity. This aspect connects to the discussion on "data ownership" which is another topic of utmost importance for the future of cyberspace and its governance as it takes more and more control of physical infrastructure. It seems much more complicated than the common discourse suggests, because data about one person can also be data about another person. The information that X is friends with Y is a ready

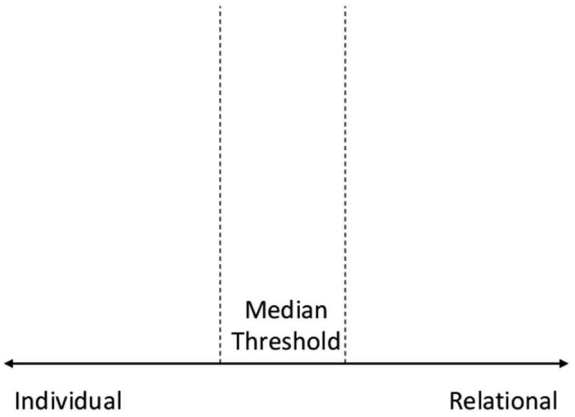

FIGURE 2 | Median threshold between individual and relational identity.

example of this conundrum as to who owns that information. Other relational criteria could be education (e.g., relationship with an educational institution—educational certificate), work (e.g., employer/employee—contract), culture and religion (e.g., membership with a religious community), hobbies and memberships in clubs, as well as membership in political parties. The crucial question is to what extent an extreme position of constructivist identity is feasible. After all, such a stance would be in an uneasy relationship with the principle of uniqueness.

As a result of the discussion on philosophical aspects of identity, we can postulate the existence of a **Median Threshold** that acts as a balance between the naturalist and the constructivist perspective (see **Figure 2**). The Median Threshold at the very least proposes the assumption that either extremes are untenable positions whether in the theory around identity or in the practice of digital identity. The truth and technologically most feasible solutions are probably found somewhere in the middle. For identity in general and digital identity specifically, one aspect can however be deduced. Whether identity is derived from either of these perspectives, they are always expressed in every individual in the whole of their combinations. In other words, every individual will contain and express all of the determinant factors of identity as a whole in itself. "I am a son, a father etc." remains also valid in absence of the other person"s presence to confirm such statements. In summary, this last aspect highlights a principle of identity without which the idea of universal identity is not workable: **Wholeness**.

LEGAL ASPECTS OF IDENTITY

In law, the concept of identity is rather badly developed and dispersed amongst several categories. It can be linked to the concept of personhood which is difficult to define in detail as well (Foster and Herring, 2017). We have already mentioned identity features to which legal consequences are attached, such as life and death. However, "legal identity" (or personhood) is also a relevant precondition to be able to sign a contract, being recognized as child or parent, as well as being entitled to vote or applying for a public post. However, identity as such is not at the center of those legal transactions and legal personhood could be described as a "technical device" (Brozek, 2017, p.12). On an international and national level, our first association might be identity cards and passports, which are attached to citizenship. While many will perceive "their citizenship" as natural and not further noteworthy, this seemingly evident concept turns out to be much vaguer and more complex upon closer inspection (Kochenov, 2009, p. 175–181).

International Law

International law, national law and individual identity are closely connected in the field of human rights (Mutua, 2016, p. 172–174). The state decides over the citizenship of a person and has the right to issue passports and identity cards as an intrinsic property of statehood and sovereignty. Associated with citizenship is the international legal prohibition of statelessness. No person should be without citizenship, because without it one has no legal recourse (Kochenov, 2009, p. 175–181). Legal personhood as a universal human right is enshrined in Article 16 of the 1966 International Covenant on Civil and Political Rights of the UN (ICCPR) and entails the right to be recognized as a person before the law (Blitz and Sawyer, 2011, p. 3–4). In short, recognition as a person with rights and duties is a fundamental aspect of identity, because it enables a person to enjoy associated elements that determine daily life and individuality such as:

- The right to life and to personal integrity as enshrined in Article 6 paragraph 1 ICCPR, as well as prevention from arbitrary arrest as enshrined in Article 9 paragraph 1 ICCPR: the naturalist world view is clearly expressed in this right, as the physical person is protected from any arbitrary interference into its biological workings and into its liberty of movement[5].
- The right to privacy and family life that includes the protection of honor and confidential correspondence as enshrined in Article 17 ICCPR (Cannataci, 2017, p. 36–41).
- The freedom of thought, conscience and religion as enshrined in Article 18 paragraph 1 of the ICCPR: this fundamental right attaches to the non-physical identity. We already discussed that the Priority Thesis postulates that the individual predominantly is an individual because of its mind rather than its body. In this composite human right, different aspects of non-physical identity come to the fore: the right to think what one wants, the right to build ones world view and the right to adopt any religion one wants (with the caveat that it is usually up to the state which religions are officially recognized).
- The freedom of expression as enshrined in Article 19 paragraph 1 and 2 ICCPR: as an extension of someone's non-physical identity, freedom of expression allows the external projection of identity, and can be seen as closely connected to identity.
- Furthermore, minority rights as individual rights to practice culture and religion are granted to persons who belong to a certain group identity as enshrined in Article 27 ICCPR.

[5]As for most human rights there are limitations and derogations possible, as for protection of the public order and for state of emergencies.

- Finally, in democratic countries legal identity also extends to political identity and includes the right to vote and to be elected. For example, this right is enshrined in Article 3 of the protocol of the European Convention on Human Rights of the Council of Europe from 1952.

All of the above shows that specifically within the field of human rights law, that has its heritage in humanism and individualism developed particularly during the period of enlightenment (Morsink, 2012, p. 1–13), individual identity finds several important elements and protection mechanisms. In addition, human rights law already determines which aspects of individual and shared identity are to be recorded to ensure their protection. We can summarize this as **Legal Determinacy** of identity. Some identity aspects are simply a legal necessity, specifically legal personhood, as they associate with the expression of individual identity in so many other areas.

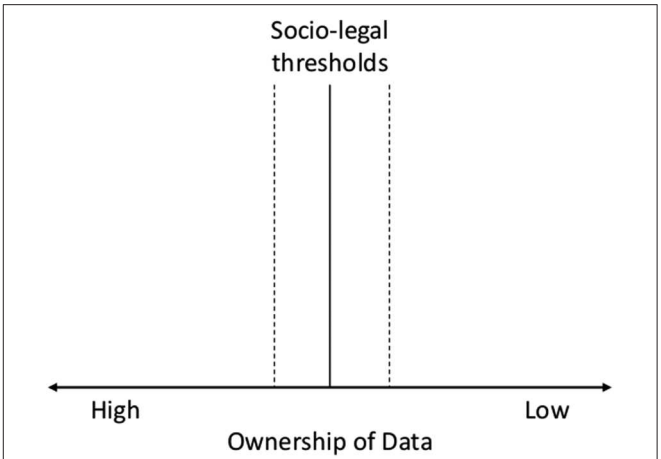

FIGURE 3 | Socio-legal thresholds regarding the individual ownership of data.

National Law

As already stated above many identity aspects that pertain to human rights are simultaneously relevant internationally and nationally. This is particularly visible in the case of European Union citizenship which has a hybrid status between international and national identity. It adds additional features for member state citizens while also producing effects for those who are not citizens of one of the member states of the union (Kochenov, 2009, p. 234–237). Nevertheless, in addition to the aforementioned rights states have developed a host of other identity related norms. As they are being dealt with quite differently across different legal traditions, this section will treat only a select few that one quite commonly encounters:

- Property rights and associated duties: ownership is an important identity characteristic particularly in market economies. Landownership is a specific subset of property rights as it is not only governed by contract law, but also by public law through land registries. This peculiarity stems from two considerations: First, with land being a high-stake property landownership deserves an increased protection by the law. Secondly, since land is placed on the territory of a state, the state reserves itself the right to govern this property title and in some states in cases of necessity, e.g., for the creation of public services, even to disown landowners (mostly under very strict conditions). Property is associated with the duty to pay taxes, which is why financial records and individual taxation form part of individual identity as a citizen or resident.
- Intellectual property rights: as expression of ownership of the products of one's individual mind, these include the rights to exclusively profit from artistic, technical, and scientific output. This element is very interesting in today's data economy as discourse on data ownership is emerging (Tjong Tijn Tai, 2018). Intellectual property rights pertain to a specific kind of data one is producing and that protects property of data of a certain quality with regards to artistic and intellectual qualities. As the value of personal data shifts, and as personal data has become a commodity much value, the threshold of artistic and intellectual quality of data needs to shift in favor of the person producing the data.

In summary, both international and national law impose a minimum set of data that by law is associated with the individual in most countries. In answer to the question of whether the individual would own a lot of data or very little, the legal requirements already indicated that no ownership of data around the identity as a citizen is not plausible. At the same time, as already indicated in the section on constructivist identity, much of what concerns identity data is relational data (e.g., being a mother relates to one's children, being a teacher to one's school and pupil etc.). This relational data is per definition data that concerns more than one entity. This means, the rights of one person to such relational identity data end where another person's rights start. This naturally leads to a socio-legal threshold of a minimum and a maximum ownership of data (see **Figure 3**).

PHILOSOPHICAL AND LEGAL THRESHOLDS OF DIGITAL IDENTITY

Summarizing what has been stated above in the sections on philosophical and legal aspects of identity, we observed that identity is generally regarded as a mixture of individual determination and relational aspects. While the **naturalist world view** establishes identity as a concept that hinges on the concept of **uniqueness** of any identity, it also evokes questions on the **priority thesis** or the dependence and interaction of an individual with its environment and society. Proponents of a constructivist identity emphasize **relationality** while questions of identity as a complete individual entity (**wholeness**) remain. As we went further to consider the legal domain, we observed that particularly in the human rights space identity is determined by several individual rights that states are obliged to grant to individuals (**legal determinacy**). Furthermore, aspects around the ownership of material and immaterial goods ultimately

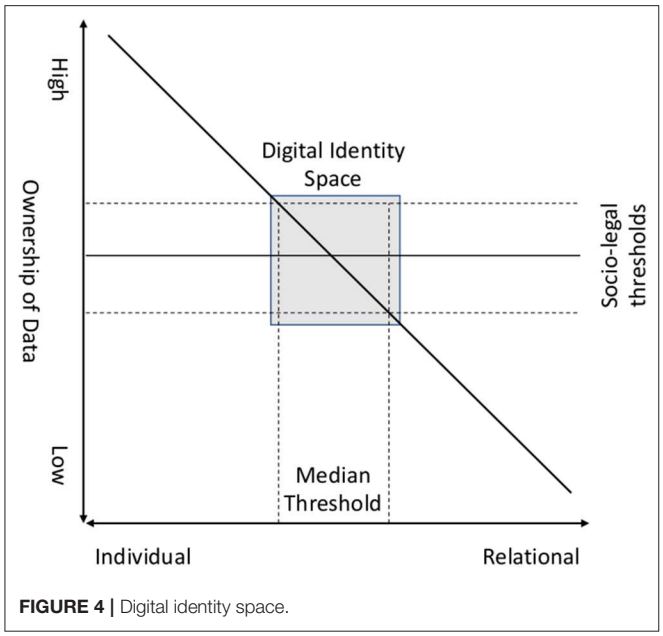

FIGURE 4 | Digital identity space.

highlight the issue of **data ownership** which could be essential to manifest fundamental and simple rights in the digital domain.

Bringing all the above together, allows us to hypothesis a space of digital identity that is both a compromise between the socio-legal threshold, as well as the median threshold between individual and relational identity conceptions. **Figure 4** visualizes this complex triangulation of philosophical and socio-legal conceptions about identity and highlights requirements which the digitization of identity—including DLT—might have to live up to:

DIGITAL IDENTITY CASES

While Blockchain and other DLTs (e.g., Ethereum, Hyperledger Indy, Veres One, IOTA) enable new paradigms of identity management (Blockchain Bundesverband, 2018), we strive to develop an initial categorization of digital identity schemes. As we continue to explore digital identity by portraying case studies of pilots in the public and private sector, including such implementing DLT, "self-sovereign identity," and ZKP, we will first briefly consider the drivers and trends that create the demand and opportunity for the digitization of identity management.

Digitization of Identity Management

Our digital and physical lives are becoming increasingly interlinked through apps and services. Our digital representation is embodied in the many versions and usages of digital identity through which we interact. While there are many reasons for these developments, we wish to highlight three trends that create demand for enhanced digital identities:

1. Necessity to improve process management and information security to protect against cybercrime and identity theft.
2. The feature of decentralization as an enabling factor for the individual.
3. The desire for increased participation in, as well as increased access and efficiency of social service provision and access to the economy.

To discuss the first trend, we should start with establishing that traditionally identity management encompasses a broad spectrum of instrumental identities, which serve the purpose of identification within a specific system or network. In a 2018 report on identity in a digital world of the World Economic Forum three archetypes are described:

- **Centralized** identity systems, where a single organization establishes and manages identity. This is typical for the direct relationship between a state and the individual. Examples include a government electoral roll, or a land registry system, but also the relationship with private actors such as a bank.
- **Federated** identity systems, where different public and private institutions establish stand-alone systems. These systems are subsequently linked through agreements or regulation and each of the managing institutions of the systems becomes a trust-anchor. This allows for some re-purposing of identity credentials, yet the activity remains driven by the initial purpose. For example, a driving license has the primary purpose to show the ability of someone to drive a vehicle, while it might also be used occasionally to prove age in other societal contexts.
- **Decentralized** identity systems, where the individual is at the center and institutions or private corporations just add (verified) credentials to a central "identity hub", "application", or "vault" that is controlled by the individual. In such a system, digital identity is initially purpose-free and becomes a resource or an asset as credentials are acquired (World Economic Forum, 2018b, p. 13–16).

As we will show below when discussing case studies, this last approach of decentralized identity management is becoming more and more popular. As the digital sphere emerges, one of the biggest challenges of siloed approaches of central and federated systems is that they overburden users with identity management. Many different accounts to access their digital identities for each use case are necessary. Already in 2015, it was estimated that in the United States an average e-mail address is associated with 130 digital accounts (Le Bras, 2015). Unsurprisingly, "identity theft" has become one of the major cyberthreats and most common cybercrimes that enables numerous fraudulent activities (Wall, 2013, p. 438–440). Furthermore, the weakness of such systems lies not only on the side of the individual. Data leaks have become a massive problem, as two data protection related fines of the United Kingdom's Information Commissioner's Office (ICO) of 2019 illustrate. As a result of an investigation, the international hotel group Marriott was fined almost £100 m after hackers stole the records of 339 million guests (Sweney, 2019b). In another case that led the ICO to levy the largest fine to date in applying the European Union General Data Protection Regulation (GDPR), the airline British Airways was required to pay £183 m in compensation after it was found that an extensive

amount of data (including login, payment card, name, address, and travel booking) of 500.000 users was stolen (Sweney, 2019a). Hence, there is a clear necessity to improve process management and information security in order to be able to use the digital sphere for meaningful exchanges of information and services.

However, this is not the only way to describe the ongoing transformation. Another important factor in this development is the question who or which entity is controlling/"owning" identity related information. Traditionally, the ownership of such identities lies with the issuer of the credentials, since this is also the institution that is guaranteeing for validity and thereby establishing trust. Hence, artifacts that prove identity such as passports need to be paid for, or the information associated with identity is monetized by private corporations in one of the manifold schemes of "surveillance capitalism" (Zuboff, 2019, p. 10–29). With decentralization however, this pattern might be changing. When focusing on this governance layer of digital identities, three types can be distinguished (Gstrein and Kochenov, 2020):

- **Centralized Top-Down-Approach**, such as for example applied in the world's largest digital identity program "Aadhaar" that is administered by the Unique Identification Authority of India since 2009[6]. This is a centralized system with more than 1.2 billion enrolled users that is not DLT based, but hinges heavily on biometrics to identify users (Rao, 2019), which is also discussed in the context of digital identity systems supported by DLT. The main purpose of Aadhaar is to improve social service provision, while critics fear that it is applied in inappropriate contexts as well. Such "mission creep" might affect the potential for development of groups negatively, and disproportionately limit individual privacy (Privacy International, 2018).
- **Individual Incentive Programs**, such as for example the E-residence scheme of Estonia. Essentially, individuals become virtual residents of Estonia which gives them a platform to operate from regardless of where they originate from. With this, a country tries to get more attractive for investment, or individuals who would like to setup a business. It can also be tied to other policy objectives such as emphasizing certain characteristics of a government, as well as creating a national brand (Poleshchuk, 2016).
- **Community-Based Bottom-Up Approach**, such as the decentralized identity platform Forus in the Netherlands[7]. We discuss it in more detail in the case studies below. Such systems are decentralized by design and entirely user focused. Platforms like Forus develop features incrementally as they grow from concrete use scenarios within communities to regional and potentially global relevance.

Another promise of putting the individual "in charge" of its own identity management has to do with aspects of social participation and the third trend creating demand for enhanced digital identities. Although it is often a non-issue for individuals living in developed countries, many people across the world are excluded from the social ecosystem as they cannot prove their identity. The World Bank Group estimated in 2018 that globally ∼1 billion people face challenges when proving their identity (World Bank Group, 2018, p. 3). The UN acknowledged this pressing need in Sustainable Development Goal (SDG) 16.9, which enshrines a right to legal identity for all, including birth certificates. However, this requires a complete overhaul of the way identities are managed on a national and global scale and will take years if not decades to change. Here, DLT based digital identities may become a catalyst for change, but it remains to be seen how countries which are at times struggling with basic infrastructural needs will be able to leapfrog toward fully decentralized digital identity. Nevertheless, according to an estimation by the World Economic Forum published in late 2018, there will be 150 million people with blockchain based identities by 2022 (World Economic Forum, 2018a, p. 19).

Case Studies in the Public Sector

Public-based digital identity solutions revolve around citizenship and the usage in the interaction with public and private institutions. Governments provide individuals with a variety of different services which are becoming increasingly available online (Schou and Hjelholt, 2018, p. 112–115). The digitization of governmental service includes the need for a safe, portable and easily accessible digital identity. Currently, the only "top-down" implemented use case of a (partly) blockchain-based national identity is Estonia which has established one of the most technologically advanced national ID-card systems. The mandatory card allows access to all secure e-services (Sullivan and Burger, 2017), including travel within the EU, national health insurance, access to bank accounts, e-voting, the administration of medical records, and even tax claims [8].

The physical card is protected with 384-bit ECC public key encryption and can also be used within a digital environment for verification. It utilizes blockchain technology to ensure the validity of the personal information, whilst allowing full control and portability. During a brief period in November 2017 the system could not be used due to a security problem resulting from a design vulnerability of the chip on the card. Estonia's administration reacted quickly, but the incident raised the question how countries with more than ∼1.5 million residents could address such a crisis that entails going back to traditional administrative methods, as well as addressing the security issue by potentially having to replace all cards in use (Asmae, 2017). Nevertheless, the implementation of the system is generally regarded as a success. Although the identity is sometimes deemed "self-sovereign", since the flow of information is fully controlled by the identity owner, there are restrictions in terms of usage. Hence, it could be argued that this system does not represent a pure embodiment of the self-sovereign identity concept and should not be considered as such. Furthermore, it has to be mentioned that this system focusing on Estonian citizens is different from the E-residence scheme of Estonia that

[6]Available online at: https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/about.html (accessed September 13, 2019).
[7]Available online at: https://forus.io (accessed March 4, 2020).
[8]Available online at: https://e-estonia.com/solutions/e-identity/id-card *(accessed March 4, 2020).*

has been described in the governance-focused categorization as an example for individual incentive programs. E-residence is oriented toward foreigners which wish to use Estonia as a business hub. Besides Estonia, such programs seem particularly interesting for countries with a track record in investment migration (Surak, 2016, p. 8–13).

However, the most successful solutions in the public sector aiming at the implementation of decentralization and DLT enabled self-sovereign identity management are based on the Community-based bottom-up model. One example for such a platform is being built in the north of the Netherlands by the foundation Forus[9]. Together with the community of Zuidhorn/Westerkwartier in the province of Groningen a solution to digitize social service provision was developed and implemented from 2017 to March 2018 (Velthuijs, 2018). The main aim of the system is to support children from non-privileged families ("Kindpakket"). During a process of intensive collaboration with the municipality and other partners from the private sector, Forus built an easy to use system for administrative purposes. It allows parents to efficiently and quickly receive funding for children who require financial aid (Van der Beek, 2018). The platform uses DLT and particularly self-sovereign identity as core design elements, as well as ZKP mechanisms to limit the exchange of raw personal data. It is designed to use cryptocurrency (typically Ethereum) as much as possible. However, it can also be used with traditional currency (Euro) when linked to a Dutch bank account. The basic design of interaction entails four roles: the applicant who uses a digital identity application ("Me"), merchants and service providers that register for the platform and also have digital identities, sponsors like public or private institutions that provide funds for which the users can apply, as well as validating parties that confirm credentials if needed. The open-source platform has in the meanwhile also been used for other projects in communities in the Netherlands[10], and continues to be developed adding new features and use cases.[11]

Similar to Forus, Kiva[12] is a decentralized digital identity platform that is being developed and implemented since 2018 in Sierra Leone (Wang and De Filippi, 2020, p. 11-14). Although the system has the support of the central government, it is currently rather limited in reach and is iteratively developed with a small community of users (Wang and De Filippi, 2020, p. 11). Hence, this development can also be considered as a community-based approach that evolves step-by-step. Kiva has the main objective of facilitating the creation of credit history. The system tries to make credit markets accessible for "unbanked people" via the creation of a secure digital identity and stimulates economic development through microloans. It is based on Hyperledger Indy as underlying blockchain layer. While the first implementation steps of Kiva seem promising, current practice is still reliant on guardian- and custodianship. While technically designed to enable identity management along the paradigms of self-sovereign identity with the use of ZKP, lacking technological infrastructure and limited technical knowledge among users highlight that it still will take some time until such solutions can be implemented without friction. At least during this transition period there is a need for concrete governance frameworks that limit and mitigate risks, particularly relating to privacy and individual autonomy (Wang and De Filippi, 2020, p. 13–14).

While these two projects are very promising, it should not be overlooked that many more projects using the Community-based bottom-up approach exist in other parts of the world. Without trying to provide a enumerative list of pilots at the time of writing, initiatives in Austria (Danube Tech), Canada (British Columbia; TheOrgBook), Spain (Alastria), Switzerland (City of Zug; UPort and ti&m), and the United States of America (Illinois Blockchain initiative; Blockchain Bundesverband, 2018, p. 54–56) can be mentioned. Potentially, the relative success of the Community-based bottom-up approach can be explained when considering the aspect that a lot of the difficult questions relating to philosophical and legal aspects of identity are not as pressing on a community level, or are relatively easy to remedy with pragmatic workarounds facilitated by smaller institutional settings.

The digital identity systems described in this section usually use a publicly verifiable digital signature showing governmental approval and are therefore recognized. Hence, these identities could also be used to communicate with other (semi-)public institutions (e.g., hospitals), as well as civil society organizations (CSOs). In this area DLT-based electronic patient records are among the most prominent use cases for pilots. Many organizations such as Medicalchain, MedRec, and MediBloc are focusing on building decentralized record management systems for electronic health records which comply with the regulatory framework (Ekblaw et al., 2016). Nevertheless, medical records are highly sensitive and require utmost care when sharing with other institutions. Still, interoperability and more patient control would be highly desirable as most hospitals work with siloed databases, which can lead to fragmented information regarding the patient and its medical needs. Additionally, inappropriate regulations such as those in the United States have halted the implementation of such solutions (Salzman, 2018).

The digitization of identity management is certainly also appealing in a cross-border context. For example, Dubai partnered with a startup from the United Kingdom named ObjectTech to ensure blockchain-based security measures for the airport. ObjectTech has been working alongside the Dubai Immigration and Visas department to develop digital passports which allow for the elimination of manual checks. At the time of writing it is being stated that Dubai will also introduce a fully developed self-sovereign identity system. However, use cases outside traveling scenarios are not available. The proposed solution is a marriage between a blockchain-based authentication system and biometric verification of an individual (Zhao, 2017). The role of DLT remains limited to the management and validation of the data once it has been registered. Hence, DLT does not aid in ensuring the validity of the submitted data.

[9]https://forus.io (accessed March 1, 2020).

[10]The webshop of the community of Nijmegen with an explanation of the scheme is available via. Available online at: https://nijmegen.forus.io (accessed March 4, 2020).

[11]Available online at: https://github.com/teamforus (accessed March 4, 2020).

[12]Available online at: https://www.kiva.org/protocol (accessed March 1, 2020).

Currently, emerging technologies capable of addressing this issue hinge on the use of biometric identification, which in turn has its own legal and ethical constraints as we know from other fields of application such as surveillance (Jasserand, 2018, p. 154–165). We will further elaborate on this aspect in the discussion.

To conclude this section, there are also cases where governments are unable to provide citizens with humanitarian aid they require due to natural or man-made disasters. As we have already briefly mentioned in the introduction of this article, decentralization, DLT, and self-sovereign identity could potentially remedy the failure of public institutions. Several use cases have already been recorded in the humanitarian domain, where the Word Food Programme and other agencies have successfully implemented digital identity solutions (Zwitter and Boisse-Despiaux, 2018; Wang and De Filippi, 2020, p. 14–16).

In the process of humanitarian intervention and aid, beneficiaries are registered to ensure an organized process of aid delivery. This enables aid organizations to track the amount of people they helped and in what manner, e.g., number of vouchers for providing food or shelter. Corporations such as Tykn and Aid:Tech are prominent examples in this field, as they both have developed and implemented solutions in such environments. Aid:Tech has collaborated with the UN World Food Programme in 2018 and built a wallet with biometric verification for refugees (Juskalian, 2018). With this, highly vulnerable individuals are able to buy items at stores in the camp without requiring a physical wallet (Zambrano et al., 2018). Tykn built a solution in collaboration with the 510-data team of the Dutch Red Cross that has the aim to provide humanitarian aid through data and digital products[13]. Following the destruction by Hurricane Irma in 2017, a pilot was tested on the island of St. Martin to use DLT for to manage disaster relief funds. After setting up a "digital wallet", users would be able to receive digital vouchers, which they could use purchase food, water and other relief goods (Erjula, 2018). Both systems hinge on the self-sovereign identity concept where beneficiaries can manage their own information and have full agency.

Case Studies in the Private Sector

In many ways, digital identity systems using DLT, self-sovereign identity and ZKP can be understood as a response to the commodification of digital identity by powerful private Internet corporations such as Facebook, or Google. After all, the original intention of Blockchain was to get independent of centralized institutions and trust anchors (Nakamoto, 2008, p. 1). DLT-based identity solutions for the private sector are very similar to those described in the previous section, with the focus on leveraging blockchain for (cross-border, cross-system) interoperability, data agency, and potentially also compliance with new regulations such as the EU General Data Protection Regulation (GDPR) (Finck, 2018b). The possibilities for DLT-based identity solutions in the private sector are frequently intertwined with those in the public sector as some require verified credentials by governmental institutions.

When considering concrete applications in the private sector, know-your-customer (KYC) related solutions are a prominent example. Due to insufficient human resources and volume of regulatory change many companies struggle with the escalating costs and complexity in their KYC process. For the year 2016 it was estimated that financial institutions and their corporate customers spent ∼$500 million annually for KYC processes worldwide (Harrop and Mairs, 2016). A partnership between PwC, Onfido and uPort has tried to address this issue with a more efficient solution, potentially used for consumer identities in UK financial services. The ConsenSys-backed uPort showcases the self-sovereign aspect as users can manage the transfer of their own identifiable information, keys and data through their personal device (Wood, 2019).

Another application lies in the area of verification of governmental identity to drive innovations such as e-mobility. In a partnership between Deutsche Telekom, Riddle&Code, Bundesdruckerei and Jolocom a digital identity solution was developed. First, users are verified in person by Bundesdruckerei. Once their identity is confirmed, they can upload their traditional German identity cards into a smart wallet to get access to e-scooters (Habel, 2019). This pilot seems particularly interesting, since such systems could remove the requirement to create a new account when signing up to a new mobility service. However, from the description of the pilot it is not clear whether and how payment could be handled.

A closely related example is age limit control. For example, when age verification is needed (e.g., buying alcoholic beverages, entrance permission to a venue), the age of the client needs to be verified. In many cases this is done by the provider checking the customers identity card. However, this typically means the customer has to share more personal data than required, as identity documents such as driving licenses, identity cards, or passports include much more information than needed for this purpose. Hence, it seems useful to look into the feasibility of ZKP. In a collaboration between Budweiser and Civic at the 2018 Consensus conference they aimed to showcase the value of ZKP for age verification to buy a Budweiser (Capilnean, 2018). For the pilot, Civic provided a digital wallet where the governmental identity document was stored and digitally signed for verification purposes. The wallet is run in a digital device such as a smartphone, which is also used to scan a QR code on a vending machine that provides beer. The vending machine is instructed to only dispense beer to those over the age of 21. While the trial worked as such, some participants had to wait for more than 20 min to be served by the machine. Maybe this might not be untypical in current real-life circumstances when waiting for a beer in a busy bar, but it highlights that ZKPs might be working slower than expected, and are potentially limited in terms of scalability. Nevertheless, it seems not unlikely that the technology will continue to improve and increase efficiency over time.

DISCUSSION

Throughout this piece we are aspiring at describing and framing the changing landscape in the management of digital identity.

[13] Available online at: https://www.510.global (accessed February 22, 2020).

As we have illustrated several of the most promising use cases in the public and private sector, we are now turning to discuss the potential implications of these innovations on the power balance between the individual, government, and corporations. Since this is a subject of immense breadth and where many societal disciplines and fields play a role (Finck, 2018a, p. 182–209), we choose to do so through the application of the lenses of individual and group privacy, as well as considerations on suitable backup-mechanisms for DLT based digital identity systems.

The discussion of privacy is useful, since the topic is a proxy for the division between the sphere of the individual and the sphere of the public (Cannataci, 2017, p. 36–41). We also highlighted this aspect in the section focusing on philosophical perspectives about identity, particularly when considering the constructivist perspective. It must be emphasized however, that privacy should not only be interpreted as a defensive right. As the UN has acknowledged throughout its work on privacy in the digital age, privacy also has an enabling character allowing the individual to develop its views on the world and itself (United Nations, 2016, p. 2). While the concept of self-sovereign identity has many elements that strengthen the individual in its position against governments and corporations, only final products and concrete applications will show whether this promise materializes. For example, when analyzing how responsibilities of controllers could be applied for operating Bitcoin in the regulatory framework of the EU GDPR, there remain uncertainties whether the collective—as partnership—is responsible within the meaning of Article 4 paragraph 7 GDPR, or its individual members are joint controllers under Article 26 GDPR (Buocz et al., 2019, p. 196). In other words, it is impossible to claim individual rights, if it is unclear who precisely has a responsibility of respecting, protecting and promoting them.

Furthermore, potential tensions should be considered on questions such as the private and public nature of data, enforcement of concrete individual rights (e.g., amendment, access, erasure/"right to be forgotten", etc.), data protection by design and default, and other requirements of state of the art data protection law (Finck, 2018b, p. 26–32). While proponents of DLT might question the relevance of high data protection standards for the operation of innovative digital identity systems, since the underlying assumptions of data protection might seem outdated as such to them, it is also fair to remain a believer in the core principles enshrined in regulations such as GDPR. Currently, GDPR and international agreements such as Convention 108+ of the Council of Europe represent two of the few effective safeguards preventing the Facebook, or "Googlization" of Everything (Vaidhyanathan, 2012). This is even more relevant in a time in which whole groups are unaware of the fact that the deployment and use of omnipresent digital technology is significantly affecting—if not eradicating—their opportunity for informational self-determination (Taylor et al., 2017, p. 226–234). As digitization is on the verge of defining what human identity is, and should be worth, these aspects become even more important to address. Hence, if DLT is about to take over identity management in the digital age, for which there are many good practical reasons, and if such identities should be "good identities" enabling a dignified co-existence (World Economic Forum, 2018a, p. 17), the technology also needs to be designed in a way in which classical privacy and data protection safeguards, as well as individual remedies are embedded by default.

However, regardless of how much identity will be digitized, one aspect that probably will have to remain tied to the physical domain is the backup-mechanism for DLT based digital identities. If a device containing a self-sovereign identity gets lost, stolen, or broken, or if the user forgets its access key, there must be a way to restore agency over such elemental information. Many options currently discussed circle around the use of biometrics to generate and potentially restore access to digital wallets, or identity hubs. While biometrics have the advantage that they are relatively persistent and cannot get lost, these characteristics are also the basis for why their omnipresent use can be dangerous.

Once biometrical characteristics of a person are registered, it is possible to paint incredibly detailed pictures of someone's life and interactions. This is often attached to completely unintended consequences, as an example from humanitarian aid shows. In 2019 the UN World Food Programme demanded from Houthi officials in Yemen to allow for the deployment of biometric technologies like iris scans and digital fingerprints to monitor suspected fraud during food distribution (Lontero, 2019). The refusal by the Houthi officials to deploy biometrical recognition over surveillance concerns lead to the cancellation of the aid efforts. This development was met with criticism on the initial demand, claiming that the UN's action was disproportionate and resulting in harm for the weakest (Martin and Taylor, 2019). However, this incident is not the only indication that the widespread, pervasive, and under-considered use of biometrics for identification purposes results in negative outcomes.

The Indian Aadhaar system hinges heavily on the use of biometrics. While the use of Aadhaar by private corporations has been limited by the Indian Supreme Court in a high-profile judgment from 26 September 2018 (Indian Supreme Court, 2018), the appropriateness of the dependency on biometrics was acknowledged as such. The judges came to the conclusion that the information security regarding the management of the biometric data of more than 1.2 billion people stored in a centralized system can be guaranteed by the government. Without speculating about the threat of the government itself abusing this power, only time will tell if the finding is true and whether the data can be kept safe from attackers. As stated in the dissenting judgment from Justice Chandrachud: "The invisible threads of a society networked on biometric data have grave portents for the future. Unless the law mandates an effective data protection framework, the quest for liberty and dignity would be as ephemeral as the wind." (Indian Supreme Court, 2018, p. 337) Therefore, the use of biometrics as backup mechanism for digital identities requires at least well thought through and detailed oversight and review procedures, coupled with the possibility to demand review of decisions and management practice on the basis of individual

request. Ultimately however, it might be desirable to consider other backup-mechanisms which are safer and have less potential for undesirable and dangerous side-effects. The use of biometric data might be part of the solution to this problem, but not the solution as such (Wang and De Filippi, 2020, p. 8–9).

Furthermore, a crucial question of power balance remains. Even if the individual might have full control over his/her credentials and the information contained in a decentralized identity management system, the control over the network and its design remain in the hands of those developing and maintaining the underpinning technological infrastructure. Furthermore, the choice of whether or not to have a digital identity in the future will equal the choice of whether or not to use applications like Facebook or WeChat, that have become omnipresent quasi-standards in many societies. The same network effect that makes it convenient to use these tools creates social pressure, particularly for those who refuse to use them. It should not be taken for granted that advanced digital identities fix these issues. They might as well enable an era of "neo-feudalism" and increased social division, especially if their implementation is done naïvely purely focusing on questions of technical feasibility (Gstrein and Kochenov, 2020).

Bringing the empirical cases together with the theoretical elaborations yields quite interesting results. On the meta-level, it becomes clear that the practice of digital identity management and the theoretical conceptions of uniqueness, relationality and legal determinacy remain relatively disconnected. The concept of legal determinacy is best represented as both private and public sector projects in general are aware and try to abide by legal frameworks such as the GDPR. Almost exclusively, however, most projects focus on the individual as a bearer of identity rights; relational aspects of identity and the problems that will emerge around data protection and data ownership in these cases seem to have no priority for stakeholders in both sectors.

CONCLUSION

The emergence of DLT and the abundance of private and public sector initiatives, as well as the emergent debate around digital identity, make it profusely clear how important it is to gain a profound understanding of the legal and philosophical conceptions and norms that govern identity in general. A sound framework of digital identity management needs to take into account questions of privacy, relationality of identity data, and data ownership. Ultimately, specifically the direct relation between the philosophical conception of identity and its socio-legal foundations, as elaborated in this article, can serve as a foundation toward defining the "self-sovereign" individual with its rights, obligations and limitations.

At the same time, a digital identity management framework is not pre-determined by certain ideas around DLT such as decentralization and immutability. If anything, DLT has enriched the governance toolkit. Public and private sector actors can select among a range of top-down to bottom-up management approaches. Even if decentralization is "en vogue" at the moment in both, the governance debate as well as amongst blockchain advocates, it is by no means a panacea for all old ailments. DLT can be a part of useful solutions, but only if it can incorporate socio-legal and philosophical necessities that digital identity brings with it. Once translated well into practice, DLT has the capacity to strengthen the rights of the individual by providing access to tools that enhance the individual's agency as self-sovereign actor.

AUTHOR CONTRIBUTIONS

AZ, OG, and EY contributed to the conception and design of the study and wrote sections of the manuscript. All authors contributed to manuscript revision, read, and approved the submitted version.

REFERENCES

Allen, C. (2016). *The Path to Self-Sovereign Identity. Life With Alacrity April 26, 2016.* Available online at: http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html (accessed February 5, 2020).

Asmae, K. (2017). *Estonia's ID Card Crisis: How E-State's Poster Child Got Into and Out of Trouble.* ZDNet November 13, 2017. Available online at: https://www.zdnet.com/article/estonias-id-card-scrisis-how-e-states-poster-child-got-into-and-out-of-trouble/ (accessed September 13, 2019).

Blitz, B. K., and Sawyer, C. (2011). *Stateless in the European Union*. Cambridge, UK: Cambridge University Press.

Blockchain Bundesverband (2018). *Self-Sovereign Identity: A Position Paper on Blockchain Enabled Identity and the Road Ahead.* Available online at: https://bundesblock.de/groups/digital-identity/blog/new-position-paper-self-sovereign-identity-defined (accessed September 13, 2019).

Brozek, B. (2017). "Legal personhood: animals, artificial intelligence and the unborn," in *The Troublesome 'Person'*, eds A. J. Visa, T. P. Kurki (London, UK: Springer), 2017. doi: 10.1007/978-3-319-53462-6_1

Buocz, T., Ehrke-Rabel, T., Hödl, E., Eisenberger, I. (2019). Bitcoin and the GDPR: allocating responsibility in distributed networks. *Comput. Law Secur. Rev.* 35, 182–198. doi: 10.1016/j.clsr.2018.12.003

Cameron, K. (2005). The laws of identity. *Kim Cameron's Identity Weblog (blog),* May 11, 2005. Available online at: https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf (accessed September 13, 2019).

Cannataci, A. (2017). "Data protection and privacy under pressure transatlantic tensions, EU surveillance, and big data," in *Games People Play: Unvarnished Insights About Privacy at the Global Level*, eds. G. Vermeulen, E. Lievens, (Antwerp: Maklu Uitgevers), 13–47.

Capilnean, T. (2018). First ever anonymous age verifying beer vending machine in partnership with anheuser-busch inbev. *Civic Blog May 12, 2018.* Available at: https://www.civic.com/blog/first-ever-anonymous-age-verifying-beer-vending-machine-in-partnership-with-anheuser-busch-inbev/ (accessed July 19, 2019).

Council of Europe (2018). *Cybercrime Convention Committee (T-CY), Preparation of a 2nd Additional Protocol to the Budapest Convention on Cybercrime, Conditions for Obtaining Subscriber Information.* Available at: https://rm.coe.int/t-cy-2018-26-ip-addresses-v6/16808ea472 (accessed September 13, 2019).

ECJ. (2018). *Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14.* EU:C:2016:779.

Ekblaw, A., Azaria, A., Halamka, J. D., Lippman, A. (2016). *A Case Study for Blockchain in Healthcare: "MedRec" Prototype for Electronic Health Records and Medical Research Data. Whitepaper.* Available online

at: https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf (accessed September 13, 2019).

Erjula, T. (2018). *510 is Exploring the Use of Blockchain In Humanitarian Aid With* Tykn. tech. 510 x Tykn Press. Available online at: https://tykn.tech/510-x-tykn-press-release/ (accessed September 13, 2019).

Finck, M. (2018a). *Blockchain Regulation and Governance in Europe*. Cambridge, UK: Cambridge University Press. doi: 10.1017/9781108609708

Finck, M. (2018b). Blockchains and data protection in the European union. *Eur. Data Protect. Law* 2018, 17–35. doi: 10.21552/edpl/2018/1/6

Foster, C., and Herring, J. (2017). "Summary and Conclusion," in *Identity, Personhood and the Law, SpringerBriefs in Law* (Champ: Springer), 57–70. doi: 10.1007/978-3-319-53459-6_5

Galič, M., Timan, T., and Koops, B. J. (2017). Bentham, deleuze and beyond: an overview of surveillance theories from the panopticon to participation, philos. *Technology* 30, 9–37. doi: 10.1007/s13347-016-0219-1

Gstrein, O. J., and Kochenov, D. (2020). Digital identity and distributed ledger technology: paving the way to a neo-feudal brave new world? *Front. Blockchain*. 3, 1–8. doi: 10.3389/fbloc.2020.00010

Gstrein, O. J., and Ritsema van Eck, G. (2018). Mobile devices as stigmatizing security sensors: the GDPR and a future of crowdsourced 'broken windows'. *Int. Data Privacy Law* 8, 69–85. doi: 10.1093/idpl/ipx024

Habel, P. (2019). *Xride: First-of-Its-Kind, Blockchain-Based E-Mobility Project*. Telekom Media. Available online at: https://www.telekom.com/en/media/media-information/archive/xride-first-of-its-kind-blockchain-based-e-mobility-project-580934 (accessed March 1, 2020).

Harbinja, E. (2017). Post-mortem privacy 2.0: theory, law, and technology. *Int. Rev. Law Comput. Technol*. 31, 26–42. doi: 10.1080/13600869.2017.1275116

Harrop, M. D., and Mairs, B. (2016). *Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity*. Press Release May 9, 2016. Available online at: https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html (accessed July 18, 2019).

Indian Supreme Court (2018). *Justice K.S. Puttaswamy (Retd) vs Union of India (2017)*. Writ Petition (Civil) W.P. (C) No.-000494-000494/2012.

Jasserand, C. (2018). Law enforcement access to personal data originally collected by private parties: missing data subjects' safeguards in directive 2016/680? *Comput. Secur. Rev.* 34, 154–165. doi: 10.1016/j.clsr.2017.08.002

Juskalian, R. (2018). Inside the Jordan refugee camp that runs on blockchain. *MIT Technology Review April 12, 2018*. Available online at: https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain/ (accessed September 13, 2019).

Kochenov, D. (2009). Ius tractum of many faces: European citizenship and the difficult relationship between status and rights. *Colum. J. Eur. Law* 15, 169–237.

Kucklick, C. (2014). *Die Granulare Gesellschaft, Der Granulare Mensch Oder Wie Wir Uns Neu Erfinden*. Berlin: Ullstein.

Le Bras, T. (2015). *Online Overload - It's Worse Than You Thought*. Dashlane Blog July 21, 2015. Available online at: https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/ (accessed September 13, 2019).

Lessig, L. (1996). *Code ver 2.0*. New York, NY: Basic Books.

Lichtenthähler, S. (2019). Intersubjektive konstitution des selbstbewusstseins? *Arch. für Rechts- und Sozialphilosophie* 105, 104–123. doi: 10.25162/arsp-2019-0006

Lontero, M. (2019). *Stop Surveillance Humanitarianism*. New York Times July 11, 2019. Available online at: https://www.nytimes.com/2019/07/11/opinion/data-humanitarian-aid.html (accessed July 19, 2019).

Luchte, J. (2012). "Pythagoras and transmigration: wandering souls," in *Epilog: The Fate of the Doctrine of Transmigration,* ed. J. Luchte (New York, NY: Bloomsbury Publishing Plc), 169–173.

Martin, A., and Taylor, L. (2019). *Biometric Ultimata - What the Yemen Conflict Can Tell Us About the Politics of Digital ID Systems*. Global Data Justice June 21 2019. Available online at: https://globaldatajustice.org/2019-06-21-biometrics-WFP/ (accessed July 19, 2019).

Morsink, J. (2012). *Inherent Human Rights: Philosophical Roots of the Universal Declaration*, Philadelphia, PE: University of Pennsylvania Press.

Mutua, M. (2016). *Human Rights Standards: Hegemony, Law, and Politics*, Albany: SUNY Press.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Bitcoin.org. Available at: https://bitcoin.org/bitcoin.pdf (accessed September 13, 2019).

Nimfuehr, M. (2018). *Blockchain Application Land Register: Georgia and Sweden Leading*. Medium, August 18, 2018. Available online at: https://medium.com/bitcoinblase/blockchain-application-land-register-georgia-and-sweden-leading-e7fa9800170c (accessed September 13, 2019).

Papineau, D. (2016). *Naturalism. The Stanford Encyclopedia of Philosophy*. Winter 2016 Edition. Available online at: https://plato.stanford.edu/archives/win2016/entries/naturalism/ (accessed September 13, 2019).

Poleshchuk, V. (2016). *'Making Estonia Bigger': What E-Residency in E-Estonia Can Do for You, What It Can Do for Estonia*. IMC Policy Briefs 2016/1. Available at: https://investmentmigration.org/download/making-estonia-bigger-e-residency-e-estonia-can-can-estonia/ (accessed September 13, 2019).

Privacy International (2018). *Initial Analysis of Indian Supreme Court Decision on Aadhaar*. Privacy International September 26, 2018. Available online at: https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar (accessed September 13, 2019).

Rao, U. (2019). Population meets database: aligning personal, documentary and digital identity in aadhaar-enabled India. *South Asia J. South Asian Stud.* 42, 537–553. doi: 10.1080/00856401.2019.1594065

Rueb, E. S. (2019). *Your Instagram Feed Is About to Have More Ads From Influencers*. New York Times June 4, 2019. Available online at: https://www.nytimes.com/2019/06/04/technology/instagram-ads-influencers.html (accessed September 13, 2019).

Salzman, S. (2018). *Electronic Medical Records: Holy Grail for Blockchain*. MedPage Today August 22, 2018. Available online at: https://www.medpagetoday.com/practicemanagement/informationtechnology/74695 (accessed July 17, 2019).

Sartre, J. P. (2007). *Das Sein und das Nichts - Versuch einer phänomenologischen Ontologie, 13th Edn.* ed. T. König (Reinbek bei Hamburg: Rowohlt Taschenbuch Verlag), 412–413.

Schou, J., and Hjelholt, M. (2018). *Digitalization and Public Sector Transformations*. Cham: Palgrave Macmillan. doi: 10.1007/978-3-319-76291-3_6

Sullivan, C., and Burger, E. (2017). E-residency and blockchain. *Comput. Law Secur. Rev.* 33, 470–481. doi: 10.1016/j.clsr.2017.03.016

Surak, K. (2016). *Global Citizenship 2.0 - the Growth of Citizenship by Investment Programs*. IMC-RP 2016/3. Available online at: https://investmentmigration.org/download/global-citizenship-2-0-growth-citizenship-investment-programs/ (accessed September 13, 2019).

Sweney, M. (2019a). *BA Faces £183m Fine Over Passenger Data Breach.* The Guardian July 8, 2019. Available online at: https://www.theguardian.com/business/2019/jul/08/ba-fine-customer-data-breach-british-airways (accessed September 13, 2019).

Sweney, M. (2019b). *Marriott to be Fined Nearly £100m Over GDPR Breach*. The Guardian July 9, 2019. Available online at: https://www.theguardian.com/business/2019/jul/09/marriott-fined-over-gdpr-breach-ico (accessed September 13, 2019).

Taylor, L., van der Sloot, B., Floridi, L. (2017). Conclusion: what do we know about group privacy? *Group Privacy, Philosoph. Studies Series* 126, 225–237. doi: 10.1007/978-3-319-46608-8_12

Tjong Tijn Tai, E. (2018). Data ownership and consumer protection. *J. Eur. Consum. Market Law* 7, 136–140. doi: 10.2139/ssrn.3172725

United Nations (2014). *General Assembly, The Right to Privacy in the Digital Age.* Resolution 68/167, January 21, 2014.

United Nations (2016). *General Assembly, Resolution A/HRC/32/L.20*. June 27, 2016.

United Nations (2018). *General Assembly, The Right to Privacy in the Digital Age.* A/C.3/73/L.49/Rev.1, November 14, 2018.

Vaidhyanathan, S. (2012). *The Googlization of Everything*. Oakland, CA: University of California Press.

Van der Beek, P. (2018). *Blockchain Kindpakket Zuidhorn Wint Prijs.* Computable March 30 2018. Available online at: https://www.computable.nl/artikel/nieuws/digital-transformation/6329958/250449/blockchain-kindpakket-zuidhorn-wint-prijs.html (accessed September 30, 2019).

Velthuijs, M. (2018). *Platform Forus Richt Gemeentelijke Dienstverlening Echt Anders in*. SBIR Gegevenslandschap eindrapportage FASE I. Available online at: https://www.berenschot.nl/publish/pages/6150/sb1bg17020_openbare_samenvatting_2.pdf (accessed September 13, 2019).

Verborgh, R. (2019). *Re-Decentralizing the Web, for Good This Time*. Weblog January 11, 2019. Available at: https://ruben.verborgh.org/articles/redecentralizing-the-web/ (accessed September 13, 2019).

Wagner, K., Némethi, B., Renieris, E., Lang, P., Brunet, E., and Holst, E. (2018). *'Self-Sovereign Identity' Position Paper*. Blockchain Bundesverband. Available online at: https://www.bundesblock.de/wp-content/uploads/2018/10/ssi-paper.pdf (accessed August 7, 2019).

Wall, D. S. (2013). Policing identity crimes. *Polic. Soc.* 23, 437–460. doi: 10.1080/10439463.2013.780224

Wang, F., and De Filippi, P. (2020). Self-sovereign identity in a globablized world: credentials-based identity systems as a driver for economic inclusion. *Front. Blockchain* 28, 26–42. doi: 10.3389/fbloc.2019.00028

Wood, M. (2019). *PwC, Onfido Join Blockchain Identity Platform uPort September, 2019*. Available at: https://www.ledgerinsights.com/pwc-onfido-blockchain-identity-platform-uport/ (accessed February 22, 2020).

World Bank Group (2018). *ID4D Annual Report*. Available at: https://id4d.worldbank.org/sites/id4d.worldbank.org/files/2018_ID4D_Annual_Report.pdf (accessed September 13, 2019).

World Economic Forum (2018a). *Our Shared Digital Future - Building an Inclusive, Trustworthy and Sustainable Digital Society*. Available at: https://www.weforum.org/reports/our-shared-digital-future-building-an-inclusive-trustworthy-and-sustainable-digital-society (accessed September 13, 2019).

World Economic Forum (2018b). *Identity in a Digital World - A New Chapter in the Social Contract*. Accessible at: http://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf (accessed September 13, 2019).

Zambrano, R., Young, A., and Verhulst, S. (2018). *Connecting Refugees to Aid Through Blockchain Enabled Id Management: World Food Programme's Building Blocks*. GovLab October 2018. Available online at: https://blockchan.ge/blockchange-resource-provision.pdf (accessed September 13, 2019).

Zhao, W. (2017). *Dubai Plans Digital Passports Using Blockchain Tech*. Coindesk June 9, 2017. Available online at: https://www.coindesk.com/dubai-plans-gate-less-airport-security-using-blockchain-tech (accessed September 13, 2019).

Zuboff, S. (2019). Surveillance capitalism and the challenge of collective action. *New Labor Forum* 28, 10–29. doi: 10.1177/1095796018819461

Zwitter, A., and Boisse-Despiaux, M. (2018). Blockchain for humanitarian action and development aid. *J. Int. Humanit. Action* 3:16. doi: 10.1186/s41018-018-0044-5

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.