Digital Identity and Distributed Ledger Technology

Gstrein, Oskar J.; Kochenov, Dimitry

Published in:
Frontiers in Blockchain

DOI:
10.3389/fbloc.2020.00010

frontiers in Blockchain

HYPOTHESIS AND THEORY
published: 12 March 2020
doi: 10.3389/fbloc.2020.00010

Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World?

Oskar J. Gstrein[1]* *and Dimitry Kochenov*[2]

[1] Campus Fryslân Data Research Centre, University of Groningen, Leeuwarden, Netherlands, [2] Faculty of Law, University of Groningen, Groningen, Netherlands

While the digital layer of social interaction continues to evolve, the recently proclaimed hopes in the development of digital identity could be both naïve and dangerous. Rather than just asking ourselves how we could digitize existing features of identity management, and corresponding financial transactions on a community or state level, we submit that truly useful and innovative digital identities need to be accompanied by some significant rethinking of the essential basics behind the organization of the world. Once digital technologies leave the realm of purely online or deeply local projects, the confrontation with the world of citizenship's biases and the random distribution of rights and duties precisely on the presumption of the lack of any choice and absolute pre-emption of any disagreement comes into a direct conflict with all the benefits Distributed Ledger Technology purports to enable. Some proponents of Distributed Ledger Technology-based identity systems envisage "cloud communities" with truly "self-sovereign" individuals picking and choosing which communities they belong to. We rather see a clear risk that when implemented at the global scale, such decentralized systems could be deeply harmful, reinforcing and amplifying the most repugnant aspects of contemporary citizenship. In this contribution, we present a categorization of existing digital identity systems from a governance perspective and discuss it on the basis of three corresponding case studies that allow us to infer opportunities and limitations of Distributed Ledger Technology-based identity. Subsequently, we put our findings in the context of existing preconditions of citizenship law and conclude with a suggestion of a combination of several tests that we propose to avoid the plunge into a neo-feudal "brave new world." We would like to draw attention to the perspective that applying digital identity without rethinking the totalitarian assumptions behind the citizenship status will result in perfecting the current inequitable system, which is a move away from striving toward justice and a more dignified future of humanity. We see the danger that those might be provided with plenty of opportunities who already do not lack such under current governance structures, while less privileged individuals will witness their already weak position becoming increasingly worse.

Keywords: digital identity, self-sovereign identity, citizenship, human dignity, discrimination

OPEN ACCESS

Edited by:
Jane Thomason,
University of Queensland, Australia

Reviewed by:
Michael Shea,
Independent Researcher, Litchfield, CT, United States
Jon Crowcroft,
University of Cambridge, United Kingdom
Anwaar Ali,
University of Cambridge, United Kingdom, in collaboration with reviewer JC

***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: *16 August 2019*
Accepted: *11 February 2020*
Published: *12 March 2020*

Citation:
Gstrein OJ and Kochenov D (2020) Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World? Front. Blockchain 3:10. doi: 10.3389/fbloc.2020.00010

INTRODUCTION

The World Bank set up an Identification for Development program (ID4D) in 2014 (World Bank, 2018, p. 1). In the 2018 report of this program, it is claimed "that an estimated 1 billion people globally face challenges in proving who they are because they lack official proof of their identity. As a result, those people struggle to access basic services—including healthcare, education, financial, and mobile services—and may miss out on important economic opportunities, such as participating in the digital economy or formal employment" (World Bank, 2018, p. 3). Accordingly, the World Economic Forum (WEF) established a "Platform for Good Digital Identity" at the beginning of 2018 (WEF, 2018a). While this initiative remarkably focuses on "good" identities with the objective to "ensuring that everyone can participate in the digital society through identity and access mechanisms" (WEF, 2018b, p. 8), the question of technological feasibility remains largely open. It seems promising to explore, however, the role Blockchain and other Distributed Ledger Technologies (DLT; including Ethereum, IOTA, Hyperledger and others) could play in underpinning such systems of fully or at least largely decentralized identification (Verhulst and Young, 2018, pp. 30–31; Wagner et al., 2018)[1]. In a report from December 2018, the WEF presented research estimating that, by 2022, 150 million people will have "blockchain-based" digital identities (WEF, 2018b, p. 17). Additionally, the market for identity verification is projected to be between 16 and 22 billion dollars (Pike and Dickson, 2018). Much of this discussion and the associated hopes focus on enhancing the capabilities of inefficient identification systems in the Global South, as well as aiding structurally suppressed groups within developing countries. As is typically the promise when it comes to digitization in public administration (Fleer, 2018, pp. 1350–1354), DLT-based systems should be able to make public services more efficient. For developed countries, this can mean that it is quicker, more convenient for the citizen, and more cost-effective to provide them. For developing countries, however, the promise is that it is possible to provide "proper" public administration in many areas for the first time. In the context of how the use of innovative technology can aid in bridging the gap between the global north and south, the term "leapfrogging" is used (Parry, 2011), and it is not difficult to imagine such disruptive strides could be made in the area of digital identity once DLT systems are applied in large scale.

However, "digital identity" and "self-sovereign identity" are also "buzz" terms. The hopes vested in them could be both naïve and dangerous, unless accompanied by some significant rethinking of the crucial basics behind the organization of the world. In this submission, we will particularly focus on this tension in connection to the allocation of citizenship and "innate" individual rights. We argue that when implemented at the global scale, DLT-based digital identity systems could be deeply harmful, reinforcing and amplifying some of the most repugnant aspects of contemporary citizenship. While particularly people from developed countries take their privileged status for granted, citizenship remains one of the most crucial global instruments for upholding and reinforcing inequalities through installing (often impenetrable) barriers in a world where inequalities are rooted more in space than in class (Milanovic, 2012). Arguably, manifested in traditional identity management systems such as passports, glass ceilings are distributed among the human population, in many ways emerging as the core element of the contemporary world order. Therefore, one might propose that such behavior is opposed to the enlightenment ideal of equal human worth, the idea of deserving and rationality (Carens, 2015; Kochenov, 2019), as well as the concept of human dignity, which is at the core of modern human rights law (Petersen, 2012). In other words, the current citizenship system can be considered as a rigid cast system. This claim is supported by empirical evidence collected and analyzed by Kochenov and Lindeboom (2019) and Harpaz (2019). If technology is uncritically taking the side of the current status quo, instead of offering new rationales to question it, it will most probably emerge as yet another, immensely effective tool of oppression and injustice. Given the current trends and ongoing discussions, we perceive the likelihood of realization of such a grim perspective as high. Since we are currently living in a world where the majority of features associated with citizenship amount to liabilities—rather than bundles of rights as Kochenov (2019) outlines in detail throughout his monograph—it can be assumed that more and better identification is not necessarily a desirable way forward. The improved policing of the random distribution of privilege with the help of new technologies could result in less justice in the world.

Some proponents of DLT-based identity systems envisage "cloud communities" with truly "self-sovereign" individuals picking and choosing which communities they belong to (Orgad, 2018, pp. 251–260). While there is no universally acknowledged definition of self-sovereign identity, 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." Allen goes on to propose 10 principles that should be associated with self-sovereign identities. Wagner et al. (2018, p. 27) have proposed to define it 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 that sense, it is even imaginable that DLT-based systems would allow individuals to freely choose the communities they associate themselves with for different purposes and for a limited time (e.g., You prefer the education system of country A, but health care in country B suits your needs better? Why not have both if you meet the basic requirements?).

In this contribution, we propose a governance-focused categorization of existing approaches to digital identity systems, use three case studies of existing digital identity systems to infer opportunities and limitations of DLT-based identity

[1]For a detailed technical definition of standards for a decentralized identifier that is not necessarily based on DLT, see https://www.w3.org/TR/did-core/ (accessed November 23, 2019).

specifically, put these in the context of the existing preconditions of citizenship law, share our broader concerns on recent developments, and conclude with a suggestion of relevant tests for DLT-based identity systems that we put forward to avoid the plunge into a neo-feudal "brave new world"[2]. While only one of our digital identity case studies uses DLT, we describe the other already implemented large-scale digital identity systems to highlight salient aspects that are also relevant to the development and use of DLT-based systems. We see tensions embedding DLT in existing and undeniable power structures, using digital identities cross-border in a societally meaningful way, and backing digital identities up using biometrical data as anchor.

DIGITAL IDENTITY AND DISTRIBUTED LEDGER TECHNOLOGY AS APPLIED AT THE STATE OR LOCAL LEVEL

As we investigate innovative digital identity programs from a governance perspective and with a focus on assigning rights and duties in the public sphere, we can distinguish three categories:

1. Centralized Top-Down; e.g., Aadhaar, India[3]
2. Individual Incentive Based; e.g., E-Residency, Estonia[4]
3. Community Based Bottom-Up; e.g., Forus.io/"*Kindpakket*", Netherlands[5]

Not all of the examples mentioned use DLT or Blockchain as underpinning technologies. However, since they were built with digital technologies at the core, even those not using a Blockchain-like system share common characteristics, opportunities, and risks relevant for DLT-based and decentralized identity management systems. It is therefore useful to consider them in this submission, especially since some of them have already been implemented in very large scale. In this section, we will describe the context and main features of these three categories before outlining the main opportunities and risks we see.

Example No. 1: Aadhaar

The "Aadhaar" program in India is arguably one of the most prominent examples of a "Centralized Top-Down" approach to digital identity management. Since India, while not so highly developed, is a country with one of the largest populations worldwide, it understandably presents a considerable challenge to implement a smoothly working identification mechanism. It was estimated that, by 2008, the four most frequently used traditional identity programs in India were passports that were used by 40 million, Permanent Account Numbers (PAN) for use by the Indian Income Tax Department with 70 million registrations, the "Ration Card" (issued by states governments to allow for the purchase of essential commodities such as wheat) with 220 million registrations, and finally 500 million voter IDs issued by the Electoral Commission (Zelazny, 2012, p. 6). Given these digits and the knowledge of the current population of India, it is clear that identification management in India in 2008 was not working comprehensively covering the entire population. It was and continues to be difficult for the country to register citizens at birth (Masiero, 2018, p. 7). In such a situation, digitization is attractive to build a safer, quicker, more efficient, and transparent system.

The Indian government started to draw up a plan for a new digital identity in 2006 and founded the Unique Identification Authority (UIDAI) in 2008 (Zelazny, 2012)[6]. Subsequently a Unique Identity (UID) was developed, which consists of 12 numbers. In order to link this identifier to a person, large amounts of personal data about it and its family are being collected (e.g., date of birth, parents' names, etc.). In particular, the number of biometric measurements is extensive and includes fingerprints as well as iris scans (Masiero, 2018, p. 4). This is also relevant for DLT-based digital identity systems, since the use of biometrics is considered as one possible solution to link "anonymous" digital wallets containing digital identities to their rightful owners (De Filippi and Wright, 2018, pp. 14–16). Although heavily disputed by some developers (Burt, 2019), biometrics continue to be an option for backup mechanisms in cases where users lose access to their digital identities, or if devices storing them have been destroyed or lost. This fits into a larger trend of increasingly using biometrical information to identify users on smartphones and mobile devices (Rattani et al., 2019, pp. 12–18).

At the end of 2018, it was estimated that 90.1% of the Indian population or more than 1.2 billion individuals were registered with the system[7]. Their UIDs are stored and managed in a centralized database system managed by the UIDAI. Although the Aadhaar system was lacking a specified list of purposes at the time of its inception, it was primarily intended to facilitate the delivery of social welfare (particularly nutrition) and to address concerns about ineffective distribution of the subsidies or fraudulent behavior (Masiero, 2018, pp. 6–7). Before turning to opportunities and risks of Aadhaar and similar Top-Down digital identity systems, we will continue to introduce case studies for the second and third category as indicated above.

Example No. 2: Estonian E-Residence

When it comes to digital identity based on individual incentives, the Estonian E-Residency program has gained a lot of attention[8]. Estonia has become one of the most innovative countries in the area of digital governance over the last decades. To promote the country as an economic hub within the European Union being open to business from everywhere, the government launched an E-Residency program on December 1, 2014[9]. This "new digital nation" supposedly consists of individuals from across the world

[2]With reference to Aldous Huxley's dystopian novel from 1932, where the allocation of roles in society was strictly predefined and controlled through advanced technological systems.

[3]https://uidai.gov.in (accessed August 8, 2019).

[4]https://e-resident.gov.ee (accessed August 8, 2019).

[5]https://forus.io (accessed August 8, 2019).

[6]The UIDAI has a website at: https://uidai.gov.in (accessed August 7, 2019).

[7]https://uidai.gov.in/images/state-wise-aadhaar-saturation.pdf (accessed August 8, 2019).

[8]https://e-resident.gov.ee/ (accessed August 8, 2019).

[9]Identity Documents Act and State Fee Act Amendment Act (Isikut tõendavate dokumentide seaduse ja riigilõivuseaduse muutmise seadus), RT I, 29 October 2014, 1.

who decide to establish their business in Estonia (Poleshchuk, 2016). Individuals interested in registering for E-Residence in Estonia can administrate their business remotely and use Estonia with its state-of-the-art digital technologies as their hub. They might consume Estonian services and products along the way, do business via the Estonian companies they found, and might eventually wish to move to Estonia, raising the country's profile. The program was launched with the target to have 10 million E-residents by the year 2025. At a later stage, the goal was added to attract 20,000 companies by the year 2021. On December 1, 2018, Estonia's population of E-residents is composed of a∼50,000 people from 157 countries, while a large portion of this growth reportedly occurred in 2018. Additionally, around 6,000 new companies have established themselves through the program (Korjus, 2018a). E-Residence essentially first intended to attempt to offset the deficiency of the original jurisdictions the E-Residence reside in and of which they hold the citizenship. It would be premature to report any real success, however: banking due diligence rules and frequent actual residence requirement meant that—for example—an Iraqi with an E-Residence is still first and foremost tied to her country and the possibility of doing business in or via Estonia is *de facto* very limited. To potentially mitigate some of these issues, the Estonian administration is looking into developing version 2.0 of this program (Korjus, 2018b).

Example No. 3: Kindpakket

The third category of digital identity programs we propose to consider consists of "Community Based Bottom-Up" approaches. Such programs might first seem limited in scope and impact. Indeed, they focus on significantly smaller populations. Communities such as the city of Zug in Switzerland (Kohlhaas, 2017) or the community of Zuidhorn/Westerkwartier in the province of Groningen in the Netherlands have successfully experimented with digital identity based on DLT in community settings (Velthuijs, 2018). In the case of the latter, a community child welfare program was realized (*Kindpakket*). The identity of a potential applicant gets stored in a digital wallet that is controlled through a smartphone application (called "Me"). Once the identity and the essential credentials are confirmed by the community/state or a trusted third party (e.g., certifying notary), the individual can "shop" for benefits that are tendered in different funds administered by the community or offered by other benevolent actors (e.g., humanitarian organizations). If the individual is interested in a specific program or fund (e.g., childcare benefits) that can be found on a platform, it is possible to apply directly. One of the additional benefits of the design of the system is that no raw personal data are being exchanged in the application process. The technology is able to assess the application just based on whether the criteria of the fund meet the credentials of the person. This is made possible by implementing a method called "Zero Knowledge Proof" (ZKP). According to Kulkarni (2018, p. 60), "ZKP allows a user to construct a mathematical proof so that, when a program is executed on some hidden input known only to that user, it has a particularly publicly known output, but without revealing any other information beyond this." Kulkarni goes on to explain that ZKP has been further developed with the emergence of "Zero-knowledge Succinct Non-Interactive Argument of Knowledge" (Zk-SNARKS), which allows one to prove something is true without revealing the reason for why it is true. With the implementation of such technologies in digital identity systems, the individual gains more control over the management of her own digital identity: she chooses under which circumstances she shares personal data, and the system is designed in a way that limits the exchange of raw personal data considerably. Therefore, it is often being claimed that such systems operationalize the concept of self-sovereign identity, solving the data protection-related "identity crisis" of the digital age (Toth and Anderson-Priddy, 2019, pp. 17–18). The individual and citizens become less dependent on intermediaries such as governments or other institutions. Once the individual meets the requirements, it receives either currency, or purpose-bound vouchers ("tokens") that can be used at merchants or for specific services (e.g., entrance to public swimming pool, sport lessons, etc.) that the backer of the fund wants to promote[10]. Since pilots in this area seem promising, it is not unlikely that such programs will become more common in many communities across the world in the years to come.

Opportunities and Limitations

It has been claimed that Blockchain is a solution searching for a problem (Frederik, 2018), and in the years 2018 and 2019, the "disruptive" potential of Blockchain and other DLT is questioned considerably. In particular, the financial sector seems to be disappointed after having made significant investments in the development of "proof of concepts." In that light, analysts claim that DLT solutions either work mainly as niche applications (e.g., supply chain sector), have modernization value replacing long-outdated systems, or have reputational value guaranteeing prestige (Higginson et al., 2019). To investigate the usefulness of DLT-based applications, Zwitter and Boisse-Despiaux (2018, p. 6) have proposed four guiding questions to find out whether DLT solutions are appropriate for the envisaged use case. Paraphrased, these are as follows:

1. Do the benefits of a DLT solution justify the costs of development and the scaling process?
2. Is the application demanding decentralization through distribution and built-in trust through transparency?
3. Does a ledger created by the application need to be immutable?
4. Does the final application comply with legal norms, relevant codes of conducts, ethical principles, and human rights?

If these questions cannot be answered affirmatively, the use of DLT might be unnecessary and other technologies might be better to achieve sustainable progress. However, despite these critical aspects, it is certainly too early to state that DLT as such have failed. There are still plenty of promising pilot projects[11],

[10]The project has been discussed with the developers in September and October 2018.

[11]https://blockchan.ge/curatedexamples.html (accessed August 8, 2019).

and the technology keeps developing beyond the "original" Blockchain system underpinning the cryptocurrency Bitcoin, which, at the time of writing, was already more than 10 years old (Nakamoto, 2008). In other words, DLT are "not monolithic concepts," with changing attributes that offer great potential in the area of "disintermediation, transparency, and accessibility." Therefore, it is still being widely believed that DLT can have a significant impact in the area of identity management, even if this might take longer than many have proposed in the past years (Verhulst and Young, 2018, p. 16).

If we consider the presented case studies and aim at identifying opportunities, we see the following: First, digitization of identity clearly offers a venue to be more precise, effective, and comprehensive in identity management. The sheer number of issued UIDs under the Aadhaar regime is impressive, and India might actually have found a tool to comprehensively issue identities for its entire population for the first time in its history. Secondly, it seems likely that the cost of administration of identities can be reduced due to the advantages of automatization. Thirdly, particularly the use of DLT and the implementation of the self-sovereign identity concept have the potential to put the individual in control of its own credentials. This could result in a profound culture change in an area in which individuals typically depend on the state, public institutions, or corporations to administer their identity. This can be enabling for individuals, offering them more choice and possibilities as the Estonian model and the study in Zuidhorn show. Additionally, many have associated hopes that this will increase the level of data protection and privacy, reducing the likelihood of large data breaches containing millions of personal credentials (Toth and Anderson-Priddy, 2019, pp. 17–18). Fourthly, DLT seems to facilitate cross-border cooperation. It is imaginable that not only communities or the state provide funds in the case of Community Based Bottom-Up approaches, but also humanitarian organizations or private parties do so to provide aid in areas that were struck by natural or man-made disaster. All of these opportunities are significant and explain the interest in the subject.

Nevertheless, for these opportunities to be realized, the following limitations need to be overcome: First, the development of DLT needs to be based on fundamental values and human rights. This can be tied to "human centered design" approaches (Giacomin, 2014). Concretely, DLT-based digital identities need to support governance structures respecting, protecting, and promoting privacy and more generally the autonomy of the individual. Poorly designed digital identity systems can seriously threaten the enjoyment of privacy, as the Aadhaar example demonstrates. In particular, biometrical data are very sensitive and difficult to protect with legal frameworks (Jasserand, 2018, p. 155), and the identifiers used relate to integral parts of the body of each individual. While it is possible to start or stop using a key, password, or any other credential used to create trust, the management of data relating to the physical shape of a human being requires much more refined frameworks. In this respect, it is also necessary to consider how attractive a centralized database containing credentials of more than 1 billion people is for private parties, as well as all types of cybercrime, cyberattacks, cyberespionage, or cyberwarfare. Not only from this perspective, the underlying regulatory and governance framework of Aadhaar seemed inappropriate since specified purposes, as well as safeguards and individual remedies for the use of the system, were not identified in a specific law at the inception of the system. In a judgment from 26 September 2018, the Indian Supreme Court tried to respond to these challenges by limiting the purposes the UID has to be used for (Indian Supreme Court, 2018). Following this judgment, it is no longer mandatory to use a UID when opening a bank account, buy mobile phone cards, in an admission process to a school, or for appearance in boards or common entrance examinations (Mahapatra, 2018; Privacy International, 2019).

This highlights a second limitation that needs to be addressed. As powerful as digital identities might be, it is important to make sure existing governance structures are precise, adequate, and have the capability to link them to "the real world." The ambitious Estonian E-Residence program ran into this limitation at the point at which individuals started to apply for bank accounts in the country. Tax authorities and other actors along the value creation chain find it currently difficult to work with digital identity, which in turn makes these identities practically useless. Estonia aims at addressing this issue in version 2.0 of the E-Residence program (Korjus, 2018b), but the underlying issue here might be the different requirements in different areas of the regulatory space (e.g., Anti-money-laundering frameworks), which all have to be proportionate and aligned in order for digital identity to work (Kaiser, 2018, pp. 578–587). Community-Based Bottom-Up approaches seem to be less sensitive to this problem since the scope of their operations is smaller and the technology is applied "closer" to the individual, which allows one to tailor it more carefully, taking the concrete problems into account.

A third limitation we see is the impact on the development of groups and social equality in general. While the Indian government has claimed that Aadhaar particularly helps the poor, careful observers such as Usha Ramanathan claim that inaccurate use of biometric data, the spreading mandatory nature of the UID, and other shortfalls create challenges for weak and sick people living in rural areas and can result in life-threatening situations for members of the transgender community or others whose identity may now be clear, but still not accepted widely in society (Bhardwaj, 2018). The datafication of social interaction reshapes the relationship not only between the individual and the government but also between groups and the rest of society (Taylor et al., 2017, pp. 226–235). Possibly, this aspect raises one of the most important aspects when discussing digital identities and the use of DLT in this area. If digital identities will fully replace existing concepts such as citizenship, they will not be able to do so in an environment that is free of customs, traditions, and power structures. This has also significant implications for deciding how centralized or decentralized the architecture of a DLT-based digital identity system can be. A fully decentralized system might be potentially empowering for the individual on the one hand, but the necessity to keep the link to society (and the resources it controls) remains on the other.

DIGITAL IDENTITY AT THE GLOBAL LEVEL: TOTALITARIAN NEO-FEUDALISM

What would happen if DLT-based digital identity was applied globally and became the standard tool of choice, eventually digitizing citizenship? To develop an answer to this question, it is useful to clarify that citizenship does not depend on the need of documenting identity, which many of the predominantly technology-focused proponents arguably aspire to solve. Virtual nations or "cloud communities," as long as they aim at replicating existing national structures, will probably make the world worse off, particularly those individuals who are less privileged already. The framing of this complex topic that academics such as Orgad (2018, pp. 251–260) propose seems unhelpful, especially in the context of his aspirational concept of a "global" citizenship, and leaving beside what such a global citizenship would ultimately mean in detail. If digital identity management driven predominantly by concerns relating to technological feasibility was to replace traditional identity management and citizenship, this arguably random segregation of the global population into relatively closed groups of varying value will continue (Kochenov, 2019). Some of these DLT-based digital identities—just as currently citizenship—will come with far-reaching rights, whereas others will predominantly represent liabilities. Hence, digitized identity management will first and foremost make this segregation process more granular, and effective.

To illustrate this with a concrete example, if someone is assigned a humiliating set of liabilities in real life—e.g., a Central African Republic citizenship—instead of a noble and democratic status—e.g., citizenship of France—virtual nations will not change anything from the perspective of individual rights and human dignity. The lack of any rights worldwide coming with some citizenships as opposed to a bundle of rights coming with others can be measured. By comparing the gross domestic product (GDP), Human Development Index (HDI), travel freedom, settlement, and work rights abroad, it is easy to see why being French—a status welcoming you to the job market of 41 countries—is infinitely better than being a citizen of the Central African Republic (Kochenov and Lindeboom, 2017, 2019). Hence, the actual problem derives from already existing real-world inequalities between identities and citizenships. It is not only that citizenships by definition exclude, the difference between citizenships matters (Kochenov, 2018, pp. 321–324). The question is how the digitization of identity management will implicitly or explicitly affect and interact with this reality.

To elaborate on this point, citizenship's core function throughout history has been to establish and police global race- and wealth-based hierarchies. This unfolds in many different perspectives, such as gender: it took US women almost a 100 years to get the right to vote, and women in the Swiss canton of Appenzell-Innerrhoden had to wait until 1991 and a decision of the Federal Supreme Court was necessary (Swiss Federal Supreme Court, 1990). Compared with women in "developed countries," individuals living in colonial territories fared even worse. While African Americans have not been enjoying the same rights as "Caucasian" US citizens historically, the same is true for those with different ethnic backgrounds living in European and Asian empires. Emmanuelle Saada has researched how arbitrary—based entirely on skin color—the ascription of French citizenship in the colonies of the Republic was (Saada, 2012). After decolonization was finished following the Second World War, the former colonial subjects are now confined to places around the world reserved uniquely for the losers of Ayelet Shachar's infamous "birthright lottery" (Shachar, 2009). Hence, the world has both changed and remained the same. It changed, because in the second half of the 20th century, the Western world has started to accept women's rights. Furthermore, racial and indigenous minorities within "first world" states are also respected in many cases. Nevertheless, in other aspects, the world has remained the same. Milanovic (2012) has outlined that inequalities can now been found between states, rather than within national borders. Hannah Arendt's concept of a "right to have rights" citizenship for individuals who would otherwise be stateless is a status associated with rights in a handful of countries only (Oman, 2010, pp. 280–289). In many others, it is a severe and undeserved liability with sometimes fatal consequences. Those locked into the poorest former colonies do not inhabit the same narrative as privileged individuals of the global north. Citizenships are thus about preserving inequality worldwide. If cloud communities, digital identity projects, and virtual nations do not address this issue in their design, these fundamental realities will remain the same.

In other words, before considering potential benefits of a set of quasi-citizenships and the deployment of digital identity to create virtual nations, it is crucial to be fully aware of the drastic differences between citizenships in "real life." This has to be considered in the light that many see digital identities as an opportunity to fully "identify" populations in countries that fail to register individuals at birth, or comprehensively throughout their lives. To be identifiable is not necessarily "a good thing." If the development and deployment of DLT-based digital identities do not recognize and take into account the circumstances, the promised benefits will remain a dream, and digitized identity management might ultimately see a considerable societal push-back.

CONCLUSION: A HOLISTIC ASSESSMENT OF DIGITAL IDENTITY

Coming back to the start of this submission, and the question how a "good" digital identity can be achieved, we hope to have convincingly made the point that such an achievement can only be realized if the current culture and understanding of identity and citizenship can be significantly improved. In other words, what is needed for true and meaningful progress is technology-enabled change of the status quo (Grinbaum and Groves, 2013, pp. 139–140), rather than the mere and value-neutral digitization of existing paradigms and power structures. Potentially, such an attempt to provide an ethically sound version of digital identity can also be inspired by the discussion around the ethical valuable use of artificial intelligence (Gath, 2018). Unless this cannot be guaranteed by the proponents and implementing actors of DLT-based identities, it might be overall better for society to stick with the current systems despite their "gray" areas and incomplete features. In the end, this might result in

more freedom and opportunities for the individuals concerned and enable more societal development than artificially restricting frameworks based on immature technological systems.

Nevertheless, we believe that digital identities based on DLT have potential if designed in the right way. For example, the GENESIS Design principles for Blockchange seem capable as guidelines (Verhulst and Young, 2018, pp. 74–77). The acronym is composed of (G)overnance legitimacy based on (E)thically sound intentions. The aim should be to produce solutions for real problems, (N)ot to promote technology as such. In this submission, we have shown that the Community-Based Bottom-Up approach seems particularly promising in this respect. This may also be one of the main reasons why the studies in this area deliver immediately tangible and solid results. Still, the (E)cological footprint of DLT-based systems remains an open question (De Vries, 2018, p. 804). However, as mentioned earlier in this submission, we think that it is important to keep in mind that DLT are still developing and, as other technologies in the past, might also get more energy effective over time. In particular, as we follow the discussion about the transition of "Proof of Work" to "Proof of Stake" consensus mechanisms, this seems not unlikely (Xu, 2018). The next principle is aimed at making sure that DLT use is (S)ynchronized with existing initiatives. We have alluded to this aspect in this submission at various stages, but believe that particularly the four-step test proposed by Zwitter and Boisse-Despiaux (2018) adds a useful perspective to this consideration. Additionally, when designing identity systems, (I)nteroperability and open standards are crucial to avoid vendor lock-in or dependence on large players. It is hard to imagine a truly self-sovereign identity based on proprietary technological standards. Finally, the last principle is to (S)ecure first block accuracy, which can also be interpreted as making sure that once personal data (especially biometrical data) are put on an immutable ledger, these data are accurate and do not cause unnecessary harm for the respective individual or citizen.

To conclude, we suggest that implementing DLT-based systems for identity management needs a holistic approach taking all of the aforementioned aspects into account and putting them at the center of the design process of applications. As we aimed at demonstrating throughout, it seems particularly useful to take into account existing knowledge, inequalities, and the limitations of citizenship law. Since the Centralized Top-Down approach and Individual Incentive programs particularly tend to make overgeneralized assumptions on individual (and collective) identity, we see less space for their success in the short- to mid-term. Still, we believe that it is useful to consider the development of such systems since they provide the background for a discussion on what identity should and could mean in the Digital Age. Nevertheless, the immediate future seems to belong to Bottom-Up digital identity approaches with their ability to improve gradually and incrementally, taking the complex social environment into account on a much more granular and practical level.

DATA AVAILABILITY STATEMENT

All datasets for this study are included in the article. For further information and data please contact the corresponding author.

AUTHOR CONTRIBUTIONS

Initially, OG took the lead on section Digital Identity and Distributed Ledger Technology as Applied at the State or Local Level, while DK took the lead on section Digital Identity at the Global Level: Totalitarian Neo-Feudalism. At a later stage, the authors worked on all of the sections of this piece together, reviewing and reformulating each other's arguments throughout.

ACKNOWLEDGMENTS

The authors are grateful to Prof. Liav Orgad and Prof. Rainer Bauböck for their critical engagement with some of the ideas, which DK contributed to the EUI online debate on Cloud Communities: The Dawn of Global Citizenship, which are developed further in this paper. Additionally, we would like to thank Maarten Velthuijs and Jamal Velij for taking the time to discuss and explain the underpinning technological paradigms and features. Finally, Carolin Kaiser deserves a special mention for the numerous inspiring exchanges on the subject.

REFERENCES

Allen, C. (2016, April 26). The Path to Self-Sovereign Identity. *Life With Alacrity*. Available online at: http://www.lifewithalacrity.com/previous/ (accessed November 22, 2019).

Bhardwaj, A. (2018, September 26). Here's what Prashant Bhushan and Usha Ramanathan have to say on #AadhaarVerdict. *Newslaundry*. Available online at: https://www.newslaundry.com/2018/09/26/heres-what-prashant-bhushan-and-usha-ramanathan-have-to-say-on-aadhaarverdict (accessed August 8, 2019).

Burt, C. (2019, October 4). Self-sovereign identity community discusses the future of digital ID at IIW XXIX. *Biometricupdate*. Available online at: https://www.biometricupdate.com/201910/self-sovereign-identity-community-discusses-the-future-of-digital-id-at-iiw-xxix (accessed November 22, 2019).

Carens, J. (2015). *The Ethics of Immigration*. New York, NY: Oxford University Press.

De Filippi, P., and Wright, A. (2018). *Blockchain and the Law*. Cambridge, MA: Harvard University Press.

De Vries, A. (2018). Bitcoin's growing energy problem. *Joule* 2, 801–809. doi: 10.1016/j.joule.2018.04.016

Fleer, P. (2018). Digitization and the continuities of change in administrative information processing. *Adm. Soc.* 50, 1335–1359. doi: 10.1177/0095399718791540

Frederik, J. (2018, August 25). De blockchain: een oplossing voor bijna niets. *de Correspondent*. Available online at: https://decorrespondent.nl/8628/de-blockchain-een-oplossing-voor-bijna-niets/519071687772-2a5ee060 (accessed October 30, 2018).

Gath, C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Phil. Trans. R. Soc. A* 376:20180080. doi: 10.1098/rsta.2018.0080

Giacomin, J. (2014). What is human centred design? *Design J.* 17, 606–623. doi: 10.2752/175630614X14056185480186

Grinbaum, A., and Groves, C. (2013). "What is "responsible" about responsible innovation? Understanding the ethical issues," in *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society,* eds R. Owen, J. Bessant, and M. Heintz (New York, NY: Wiley & Sons), 119–142.

Harpaz, Y. (2019). *Global Citizenship 2.0*. Princeton NJ: Princeton University Press.

Higginson, M., Nadeau, M. C., and Rajgobal, K. (2019, January). Blockchain's Occam problem. *McKinsey & Company*. Available online at: https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem (accessed August 8, 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

Kaiser, C. (2018). *Privacy and Identity Issues in Financial Transactions* (dissertation Thesis). University of Groningen, Gronigen, Netherlands.

Kochenov, D. (2018). "Escapist technology in the service of neo-feudalism," in *Debating Transformations of National Citizenship. IMISCOE Research Series,* ed R. Bauböck (Cham: Springer), 321–326.

Kochenov, D. (2019). *Citizenship*. Cambridge, MA: MIT Press.

Kochenov, D., and Lindeboom, J. (2017). Empirical assessment of the quality of nationalities: The quality of nationality index (QNI). *Eur. J. Compar. Law Governance* 4, 314–336. doi: 10.1163/22134514-00404007

Kochenov, D., and Lindeboom, J. (2019). *Kälin and Kochenov's Quality of Nationality Index*. Oxford: Hart Publishing.

Kohlhaas, P. (2017, December 7). Zug ID: Exploring the First Publicly Verified Blockchain Identity. *Medium*. Available online at: https://medium.com/uport/zug-id-exploring-the-first-publicly-verified-blockchain-identity-38bd0ee3702 (accessed August 8, 2019).

Korjus, K. (2018a, November 30). E-Residency is 4 Years Old so Here's 4 Surprising Facts About the Programme. *Medium*. Available online at: https://medium.com/e-residency-blog/e-residency-is-4-years-old-so-heres-4-surprising-facts-about-the-programme-c3a9d64c988d (accessed August 8, 2019).

Korjus, K. (2018b, September 11). E-Residency 2.0: What do Estonians think of the programme? *Medium*. Available online at: https://medium.com/e-residency-blog/e-residency-2-0-what-do-estonians-think-of-the-programme-99853274a55b (accessed July 22, 2019).

Kulkarni, K. (2018). *Learn Bitcoin and Blockchain : Understanding Blockchain and Bitcoin Architecture to Build Decentralized Applications*. Birmingham, UK: Packt Publishing Ltd.

Mahapatra, D. (2018, September 27). *Times of India*. Available online at: https://timesofindia.indiatimes.com/india/aadhaar-stays-minus-fangs-and-pangs/articleshow/65972588.cms (accessed August 8, 2019).

Masiero, S. (2018). Explaining trust in large biometric infrastructures: a critical realist case study of India's Aadhaar project. *E J Info Sys Dev Countries* 84:e12053. doi: 10.1002/isd2.12053

Milanovic, B. (2012). *Global Income Inequality by the Numbers: In History and Now*. Policy Research Working Paper No. 6259 of The World Bank. Available online at: http://documents.worldbank.org/curated/en/959251468176687085/Global-income-inequality-by-the-numbers-in-history-and-now-an-overview (accessed July 26, 2019).

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org. Available online at: https://bitcoin.org/en/bitcoin-paper (accessed August 8, 2019).

Oman, N. (2010). Hannah Arendt's "Right to Have Rights": a philosophical context for human security. *J. Hum. Rights* 9, 279–302. doi: 10.1080/14754835.2010.501262

Orgad, L. (2018). "Cloud communities: the dawn of global citizenship?" In: *Debating Transformations of National Citizenship. IMISCOE Research Series*, ed R. Bauböck (Cham: Springer), 251–260.

Parry, J. (2011). Leapfrogging into the future. *BMJ* 342:d2990. doi: 10.1504/IJISD.2005.008087

Petersen, N. (2012). *Human Dignity, International Protection*. Max Planck Encyclopedia of Public International Law. Available online at: https://opil.ouplaw.com/abstract/10.1093/law:epil/9780199231690/law-9780199231690-e809?rskey=DtxXVW&result=1&prd=EPIL (accessed July 22, 2019).

Pike, S., and Dickson, F. (2018). *Identity on the Blockchain Special Report: Forecast and Analysis for Blockchain-Based Identity Solutions, Jul 2018 - Special Study - Doc # US44070617*. International Data Corporation.

Poleshchuk, V. (2016). *"Making Estonia Bigger": What E-Residency in E-Estonia Can Do for You, What It Can Do for Estonia*. Investment Migration Working Papers. Available online at: https://investmentmigration.org/download/making-estonia-bigger-e-residency-e-estonia-can-can-estonia/ (accessed August 8, 2019).

Privacy International (2019, September 26). Privacy International, Initial analysis of Indian Supreme Court decision on Aadhaar. *Privacy International Website*. Available online at: https://privacyinternational.org/long-read/2299/initial-analysis-indian-supreme-court-decision-aadhaar (accessed August 8, 2019).

Rattani, A., Derakhshani, R., and Ross, A. (eds.). (2019). "Introduction to selfie biometrics," in *Selfie Biometrics*, *Advances in Computer Vision and Pattern Recognition* (Cham: Springer), 1–18.

Saada, E. (2012). *Empire's Children – Race, Filiation, And Citizenship in the French Colonies*. Chicago, IL: University of Chicago Press.

Shachar, A. (2009). *The Birthright Lottery - Citizenship and Global Inequality*. Cambridge, MA: Harvard University Press.

Swiss Federal Supreme Court (1990). *116 Ia 359*.

Taylor, L., van der Sloot, B., and Floridi, L. (eds.). (2017). "Conclusion: what do we know about group privacy?" in *Group Privacy, Philosophical Studies Series* (New York, NY: Springer), 225–237. Available online at: https://www.springer.com/gp/book/9783319466064

Toth, K. C., and Anderson-Priddy, A. (2019). Self-Sovereign digital identity – a paradigm shift for identity. *IEEE Secur. Priv.* 17, 17–27. doi: 10.1109/MSEC.2018.2888782

Velthuijs, M. (2018, March 30). *Forus, Gemeente Zuidhorn, Berenschot, Platform Forus garandeert de betrouwbaarheid, SB1GL17005*. Veiligheid en toegankelijkheid.

Verhulst, S. G., and Young, A. (2018). Field Report - On the Emergent Use of Distributed Ledger Technologies for Identity Management. *GovTech report*. Available online at: https://blockchan.ge/blockchange-fieldreport.pdf (accessed August 7, 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).

WEF (2018a). *Platform for Good Digital Identity*. World Economic Forum Web Portal. Available online at: https://www.weforum.org/projects/digital-identity (accessed August 7, 2019).

WEF (2018b). *Our Digital Future – Building an Inclusive, Trustworthy and Sustainable Digital Society*. World Economic Forum Web Portal. Available online at: https://www.weforum.org/reports/our-shared-digital-future-building-an-inclusive-trustworthy-and-sustainable-digital-society (accessed August 7, 2019).

World Bank (2018). *Identification for Development 2018 Annual Report*. World Bank ID4D program webpage. Available online at: https://id4d.worldbank.org/sites/id4d.worldbank.org/files/2018_ID4D_Annual_Report.pdf (accessed November 23, 2019).

Xu, B. (2018, April 5). Blockchain vs. Distributed Ledger Technologies. *Medium*. Available online at: https://media.consensys.net/blockchain-vs-distributed-ledger-technologies-1e0289a87b16 (accessed August 8, 2019).

Zelazny, F. (2012). *The Evolution of India's UID Program: Lessons Learned and Implications for Other Developing Countries, Policy Paper 008*. Washington, DC: Center for Global Development.

Zwitter, A. J., and Boisse-Despiaux, M. (2018). Blockchain for humanitarian action and development aid. *J. Int. Humanit. Action* 3, 1–16. 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.