Policy Design and Practice

Routledge
Taylor & Francis Group

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rpdp20

A global digital identity for all: the next evolution

Clare Sullivan & Scott Tyson

To cite this article: Clare Sullivan & Scott Tyson (14 Oct 2023): A global digital identity for all: the next evolution, Policy Design and Practice, DOI: 10.1080/25741292.2023.2267867

To link to this article: https://doi.org/10.1080/25741292.2023.2267867

Published online: 14 Oct 2023.

POLICY DESIGN AND PRACTICE
https://doi.org/10.1080/25741292.2023.2267867

Routledge
Taylor & Francis Group

RESEARCH ARTICLE

OPEN ACCESS Check for updates

A global digital identity for all: the next evolution

Clare Sullivan[a,b] and Scott Tyson[a]

[a]Cyber SMART Research Center, Georgetown University, Owings, Australia; [b]School of Continuing Studies, Georgetown University, Washington, USA

ABSTRACT

This paper chronicals the emergence of digital identity as a legal concept, how digital identity has grown in importance at the national level over the past decades and is now poised to become even more important internationally. This work builds on existing scholarship, to consider the next evolution of digital identity from what is now essentially a national concept into a global, legal concept. The examination looks to the likely emergence of a global digital identity for individuals in the near future and asks how that could be achieved. The authors examine the use of blockchain technology as a possible foundation of a global digital identity, along with the necessary development of existing international law on individual rights to support a global digital identity for all. Blockchain is viewed as relatively more secure and it enables individuals to have more control over how their identity information is managed and used. Blockchain's traceability provides advantages for government and the private sector in managing and verifying identity. It aids the integrity of identity information and related transactions. However, it is important to note that, while blockchain has advantages, its relative immutability can lead to the creation and use of false digital identities that cannot be easily detected or corrected. As this paper discusses, this aspect can undermine the integrity and reliability of digital identity nationally and internationally. Given that blockchain technology is fallible, the authors argue that international law has a vital role now and in the future in recognizing the right to digital identity and establishing norms of conduct.

ARTICLE HISTORY
Received 11 October 2022
Accepted 25 September 2023

KEYWORDS
Digital identity; evolution; blockchain; global digital identity; right to identity

1. Introduction

In 2006, digital identity was first examined as an emergent legal concept that was fundamentally changing the commercial and legal landscape. Now, the term "digital identity" has moved from obscurity to common parlance and its significance has

CONTACT Clare Sullivan cls268@georgetown.edu School of Continuing Studies, Georgetown University, 37th and O Streets NW, Washington, D.C. 20057, USA

grown, although its full implications, especially for future development, are not completely realized.

In 2011, in "Digital Identity," it was predicted that digital identity would move from a national to an international concept: "Such a scheme may seem unlikely now but globalization is merely the next step. Nations are currently sharing digital passport, visa, work permit and other immigration information as part of border control, and digital information, including biometrics, is shared between international law enforcement and defense authorities. Under these broader schemes, an individual's registered identity becomes his or her officially recognized identity not just on a national basis but as a citizen of the region and eventually of the world" (Sullivan 2010).

This paper examines this next evolution of digital identity into an international concept and the role Distributed Ledger Technology (DLT) could play in that development. Blockchain is perhaps the best known DLT and, for ease of reference, this paper collectively refers to DLT as blockchain. The discussion begins by describing the typical features and functions of digital identity, particularly as used to access public sector services and benefits. Then, international recognition of an individual's digital identity supported by blockchain technology is considered as a foundation for a global digital identity. The paper then imagines the near future where a blockchain-supported global digital identity is commonplace and considers the potential impact on identity management from the perspectives of governments, businesses, and individuals.

2. Digital identity as an emergent legal concept

In this paper, digital identity describes the set of information required to establish an individual's identity for official purposes, specifically to access and use public sector services. It is the group of identity information that is used to conduct those transactions.

As explained in earlier scholarship (Sullivan 2010), historically, identity has been a nebulous legal concept and had a relatively unimportant role in transactions. An individual did not need a thing called an identity to transact; and in the absence of fraud, there was no requirement that a person use only one name, for example. This was largely because of the way transactions were conducted in earlier times. In the digital age, this has changed. Dealings conducted in-person, often with a history of personal acquaintance, have been replaced by remote transactions facilitated by technology. This fundamental change in the way we transact in the twenty-first century has made identity, and particularly digital identity, important. In most developed nations, a digital identity is now required for an individual to conveniently access government services and is necessary for most private-sector transactions. This is the case in the developing world too, with digital identity being used for at least some services for almost a decade (The World Bank 2016). A single, unique identity is now required by most governments and, hence, is needed by an individual (Sullivan 2018).

While the emergence of digital identity as a legal concept has been documented in legal scholarship from 2006 (Sullivan 2018), the term "digital identity" has since

become more widely used and understood, with a seismic shift occurring in 2017. In that year, digital identity and its new importance was formally recognized by the United Nations (U.N.). In its sustainable development goal (SDG) 16.9, the U.N. required that all member nations "[b]y 2030, provide legal identity for all, including birth registration" (United Nations 2023a). "Legal identity" is not defined in SDG 16.9, but, for all practical purposes, it includes digital identity. This assertion is well supported by the U.N. operational definition which defines legal identity with the same basic characteristics that comprise an individual's digital identity (i.e. name, sex, place and date of birth, as conferred through birth registration); with the specification that legal identity is retired by the issuance of a death certificate (United Nations 2023b). SGD 16.9 was a milestone in recognizing identity as important for individuals in all nations and in cementing digital identity's international significance.

2.1. Digital identity defined

Digital identity consists of information that has both meaning and function. This concept of words having function is familiar in computer science but it is a new concept in law. The function of the information that comprises digital identity is to single out one identity from all the others. When the required group or set of information is entered, it is used by the system to first recognize the particular identity from the many registered digital identities on record, and then to enable the requested transaction. Digital identity may be used in this way in the context of a formal national identity scheme, such as exists in Australia, or under more informal arrangements that are not necessarily designated as a digital identity scheme but which use a digital identity for transactions, as is the case in the United Kingdom, for example (Sullivan 2006; Australian Government 2023) The term "digital identity scheme" is used in this paper to encompass both formal and de facto digital identity schemes. Furthermore, while the same digital identity is often required for both public and private sector transactions, for ease of understanding, this paper focuses on the digital identity used by individuals for public sector dealings such as accessing and using government services.

The information that constitutes a person's digital identity for transaction purposes is a small, defined set of identity information. This information is largely derived from a person's birth record, which in most cases is the birth certificate. The birth certificate is the seminal identity document in most jurisdictions and this is recognized by SGD 16.9 when it refers to "birth registration." This document is usually in paper form although increasingly birth certificate information is also stored digitally.

The set of information that comprises transaction identity is typically the individual's full name, date of birth, and gender, and includes at least one piece of identifying information. Identifying information is considered unique to the individual, such as a PIN, a signature, an identifying number, or sometimes a biometric. The scheme requirements and the value and type of transaction dictate the identifying information required, including whether more than one piece of identifying information is necessary. Identifiers like biometrics are generally required for higher value and more sensitive transactions.

Other information that is more detailed sits behind transaction identity. This other information is usually a profile of the individual and their transactional history with associated administrative information that is upated on a regular basis, often in real time. This more detailed and dynamic information is linked to an individual by the much smaller set of more stable information that comprises transaction identity. (Sullivan 2010; Sullivan 2018).

2.2. Digital identity schemes and identity authentication and verification

All digital identity schemes used for transactions depend on two basic processes—identity authentication and identity verification. Although these terms are often used interchangeably, authentication occurs at the time a person first registers under the particular identity scheme and it may or may not be renewed periodically. Verification of identity occurs at the time of a transaction and is done by the system, usually automatically, when the required transaction identity information presented exactly matches the transaction identity on the record as established at the time of authentication (i.e. registration).

At the time of registration, information is checked to determine its authenticity. A familiar example is the identity verification process that is usually required to obtain a driver's license, open a bank account, or apply for a passport. The process involves the provision of original documentation, typically beginning with the birth certificate and including driver's and other licenses, a marriage certificate, if there has been a name change as a result of marriage, passport and other official documents issued by government. Other required information can include memberships and employment records, for example. The birth certificate is the most important identity document from which most of the key information for other identity documents, such as licenses and passports, are obtained. The checking process generally follows the Know Your Customer (KYC) requirements for identity authentication contained in Anti-Money Laundering/Counter Terrorism Financing (AML/CTF) legislation that has been widely adopted by most nations to address money laundering and terrorism financing. The KYC protocols, formerly known as the 100-point identity check, usually include an in-person or virtual interview, at which time the applicant provides specified identity documents that are ranked in terms of their standing to establish identity and are used to cross-check the information provided against official records. Copies of the presented documents are usually made by the authenticating organizaton, whether it be a government entity or a third party authentication agency, and the copies are kept for their records to show compliance with the AML/CTF legislation (Sullivan 2010; Sullivan 2018; Sullivan 2006; Australian Government 2023; Gov.UK 2023).

The information registered at the time of authentication establishes the digital identity for the purposes of the scheme. Most importantly, it establishes transactional identity. In addition to full name, gender, and date of birth, identifying information, such as signature, photograph, and biometrics (e.g. face scan, iris scans, fingerprints) and assigned identifiers, such as a PIN, are recorded at this time. The primary role of this identifying information is to link an individual with the digital identity registered

for the scheme. At the time of registration, the digital identity is formed and comes into effect. The recorded identifying information is then associated with a particular person, even if there is error or fraud in the authentication process. That transaction identity then becomes the primary means by which that individual transacts under the scheme. Most schemes currently also permit in-person dealings but there is clearly a move to have most dealings online as computer ownership and computer literacy become ubiquitous.

The nature and functions of transaction identity, and its significance in the digital era, mean that the consequences of system error or fraud in the identity authentication and verification processes are serious. There are two main scenarios and both are concerning. The first is where a legitimate digital identity is used by another person for a bogus transaction. The transaction appears legitimate because it is verified under the scheme, so the transaction is difficult to successfully contest, often requiring proof of impossibility such as complete incapacity at the time of the transaction. The second scenario is where a new false digital identity is created from fabricated information. The identity may be completely fabricated or it may contain some legitimate information of a person or persons. The latter situation can be especially difficult to detect, investigate, and unravel. In either case, however, the identity is inauthentic but appears to be authentic because it is linked to a specific person at the time of authentication. The identity is apparently legitimate and indeed is given legitimacy by the scheme until proven otherwise. This means that, in the interim, that transaction identity can be used for a range of apparently legitimate transactions. This has implications for government, business, and individuals. The consequences for innocent individuals can be especially onerous because the transactions for which they are assumed responsible can be difficult to disprove due to the nature and functions of transaction identity (Sullivan 2010; Sullivan 2018).

Transaction identity operates much like a key to allow access to the system to enable transactions. When the transaction identity information on record aligns with the information presented for the transaction it effectively "opens the door" to allow the transaction. Transaction identity is designed to locate a single digital identity from all those registered under the scheme, then to verify that identity for the requested transaction. If all that identity information as presented matches the information on record, then the system automatically authorizes the transaction. In actual operation, the transaction is entirely machine-driven. This is how identity theft and fraud and error can occur and how illegal transactions can be legitimized by the scheme. There is an underlying assumption that all the registered identity information is correct and authentic to the person presenting it at the time of identity authentication and, subsequently, to verify identity for a transaction. That presumption, however, depends on the scheme being infallible, which of course cannot be so (Sullivan 2010). Even a robust system can fail as a result of deliberate deception, unauthorized access, human error, or spontaneous system error. The significance of digital identity means that the consequences are serious for all involved, whether they be organizations or individuals.

2.3. Blockchain technology and digital identity authentication and verification

Blockchain and other DLT technology, collectively referred to as blockchain technology in this paper, can improve the transparency and security of existing identity authentication and verification processes. An individual's identity information is distributed across the blockchain, enabling the individual and others authorized by the individual, to see select information. The individual can determine the information to be shared as well as to whom and when. This added control and visability enables an individual and others, like investigators and law enforcement, to spot anomolies, errors, and fraudulent activity.

While blockchain is not the only available approach, and has critics as well as supporters, it can improve security and give individuals more control over when and how their identity information is disclosed. It has been shown to do so in early adopters, like Estonia. Consider the registration process where originals of the required identity documents are provided to authenticate identity. Copies of these documents are taken at that time and are scanned into the records that an authenticating entity keeps as part of the registration process and for KYC compliance. This process is carried out when opening an account, applying for a benefit or service, and applying for a driver license, to mention just some of the many occasions when identity must be authenticated. The result is that there are multiple records of these documents held by a wide range of public and private-sector bodies that only increases over time. While some of the required documents change over the years, such as when a person obtains a new passport, the seminal identity document, the birth certificate, remains the same. Over the course of a person's lifetime, that document will be copied on multiple occasions and the copies stored in hundreds of databases. The security of those copies and the information they contain is largely dependent on the protocols used and enforced by each entity. Even if protocols are strong, they are never infallible. The more copies are held in multiple databases, the greater the likelihood of an important identity document, like a birth certificate, being compromised, whether by hacking, fraud, system error, or system failure.

A blockchain is a public ledger distributed across many computers, using cryptography to provide confidentiality and security. It is touted as being essentially trust-based, the trust being in the network of servers and the software system rather than a particular organization, like a government department. While blockchain technology is fallible, its security risks are comparatively fewer, making it a strong alternative for storing and accessing important identity documents. There are many approaches that have been suggested for the broader use of blockchain, including for identity, but public blockchain is the most promising in terms of improved security for identity documents because it enables an individual to control and monitor access. In this respect, blockchain shifts the current paradigm by giving an individual, not a government or private-sector organization, control over the individual's identity information and who can view it.

3. Public blockchain and identity authentication

This section examines the nature of public blockchain and outlines in simple terms how it can apply to digital identity, especially for identity authentication. The

advantages of public blockchain are compared to the paper-based identity authentication used in most jurisdictions. This discussion provides the basis for the following section which examines the possibility of a blockchain-based global identity.

3.1. Public blockchain for identity authentication and verification

Public blockchain is the technology that underpins Bitcoin, which enables users to transact without using a traditional intermediary such as a bank or government body. A public blockchain, like that used for Bitcoin, does not have access restrictions whereas a private blockchain controls access. A private blockchain may be presumed to be more secure because of controlled access but the opposite is often true due to the nature of blockchain technology.

A public blockchain is more secure because it is decentralized, with information encrypted and stored on multiple devices. There is a chain of linked records called blocks. As data is added, new blocks are added to the chain. Each block has a hashed key that links it to the preceding block, a time stamp when it was added or altered, and transaction data. This distribution means that the network exists and can still function even if a node is unavailable.

With a blockchain-based system, the source documentation, such as identity documents, can be stored off of the blockchain, the document hash can be compared to the hash on the blockchain, and the comparison can then be stored on the blockchain. The benefits of this approach are that the authenticating organization can, for example, prove by a ledger entry on the blockchain that the KYC checking has been done without the need to handle paper documents or the scanning and storing of copies. This is a much more secure approach that also gives the individual more control over crucial identity documents and the information they contain.

While there are still points of attack, blockchain is consensus-based and a majority of nodes comprising the blockchain would have to collude to remove or change data; so, in theory, fraud is more difficult to perpetrate and relatively easier to detect. Moreover, access rights enable the individual to control access to the data via encryption, instead of control being through an identity provider—enforced policy. Most public blockchain systems use keys and signatures to control the shared ledger. Each blockchain node within the network has its own copy of the ledger and data added to the ledger is sent to all participating nodes so the data appears in all copies of the blockchain. Any of the participants can add data to the blockchain and algorithms aggregate data in "blocks." These blocks are added to the chain of existing blocks using a cryptographic signature. For public blockchains, that signature includes a proof of work that makes it cryptographically unlikely that anyone will alter the prior blocks. The proof of work is a consensus algorithm that is used to verify transactions and to add new blocks to the chain. Solving the proof of work algorithm is difficult, though not impossible, in the sense that any alteration also requires alteration of a prior block, which means redoing the work for all subsequent blocks. This makes it cryptographically more secure and unlikely that anyone will alter the prior blocks. Overall, the public and distributed nature of the blockchain makes it difficult to have

a falsified block accepted by the network. This is the immutability feature of blockchain.

An individual can encrypt select data on the blockchain and can select who gets the key/s to decrypt the data. The way this works for identity authentication is that, instead of a person taking their identity documents to the authenticating organization and having that organization take copies for its records, the individual can allow the organization to view specific information through the public blockchain. The source document such as a birth certificate is stored off of the blockchain, but the document hash can be compared to the hash on the blockchain, and the comparison stored on the blockchain to show that the document has been checked and validated as part of the identity authentication procedures. Blockchain technology can also be used for identity verification for transactions, though the main advantage of the public blockchain is its use for identity authentication.

While there is no doubt that blockchain provides more security than paper-based authentication procedures, it has weaknesses. The immutability of blockchain can have a significant downside in that it makes errors and inaccuracies recorded on the blockchain difficult, though not necessarily impossible, to remove or correct. A digital identity that is inaccurate may be enshrined on the blockchain. This can be done through mistakes in data entry that are either inadvertent or deliberate, such as creating a false identity through the use of fabricated identity documents and information. Once that information is put on the blockchain, it is accorded a level of permanency and assumed authenticity that is difficult to dispute and change. In effect, a false identity is created. However, as discussed, this presumed authenticity and accuracy also exists in paper-based systems and correction is similarly burdensome.

In most developed nations and in many developing nations, digital identity is the primary means by which an individual is acknowledged to exist and to have standing to transact with a range of public and private-sector organizations; so an inaccurate digital identity has serious consequences, especially for the individual concerned. The consequences are more concerning if the error results in a person being able to use a digital identity other than their own, as can happen if there has been identity theft, or if there has been system error where records have been incorrectly assigned. This situation is often difficult to fix in any scheme, but when the information is on the blockchain it can be more difficult to correct, though it may be easier to detect. These strengths and weaknesss of blockchain can have widespread effects. While there is clear impact on individuals, there are also the broader consequences of bogus transactions for businesses and the public sector.

3.2. Public sector use of blockchain for identity authentication

The emergence of digital identity and realization of its increasing significance has led to use of blockchain in relation to identity authentication. Many jurisdictions are exploring, or have recently implemented, blockchain initiatives for public sector functions at the national or state level. Estonia, however, is a more mature example of the use of blockchain to underpin digital identity for government services.

Estonia is a leader in its use of blockchain and a pioneer in its early use of digital identity in its national identity scheme for its citizens and permanent residents, and for the Estonian e-Residency program. The latter is for persons who are located outside the country and who do not have Estonian citizenship or phyical residency, to enable them to do business in Estonia. Estonia was the first nation to use blockchain technology, specifically KSI Blockchain, which is also used by NATO and the U.S. Department of Defense. Data is not stored on the KSI Blockchain. Instead, a one-way hash of the data to be protected is generated. A one-way hash is a mathematical function that converts a variable-length input string into a fixed-length binary sequence. It is one-way because it is practically impossible to derive the original text from the outputted string and is therefore more data-protective and secure. The one-way hash is combined with prior hashes, and then published on a blockchain-like chain of hashes (E-Estonia 2019). The system can provide immutability for petabytes of data every second (PricewaterhouseCoopers 2019).

Every Estonian has a government-issued digital identity as part of this sophisiticated and long-established scheme that provides digital access to all of Estonia's e-services. In 2014, Estonia substantially expanded its digital identity program to include persons located outside Estonia who are neither Estonian citizens or permanent residents. This Estonian e-Residency program is essentially an economic development initiative. So called "e-Residents" cannot access all the services available to Estonian citizens and permanent residents but they can remotely access and use a range of Estonian e-government and private sector services for commerce. The identity issued to an e-Resident is a government-authenticated, transnational digital identity and, as such, it is a major step toward a global digital identity.

A further step toward the globalization of digital identity occurred in December 2015, when Estonia and Finland became the first countries in Europe to develop a joint data exchange platform based on X-Road that allows data to be automatically exchanged between countries. X-Road is used for the Estonian digital identity scheme for citizens, permanent residents, and e-Residents to enable Internet-based data exchange between national information systems and for automatic data exchange between countries. In addition to its implemention in Finland, X-Road has since been implemented in Azerbaijan, Namibia, Faroe Islands and, most recently, in Mexico (PricewaterhouseCoopers 2019).

These steps show the feasibility of a blockchain-based transational identity and its advantages in facilitating national and international interoperability, albeit on a relatively small scale. However, use of blockchain for identity, especially on a broader scale, is largely untested and it raises questions about the responsibility of those who vouch for the accuracy of the information and for the ensuing consequences of relying on that information.

While blockchain is touted as being more secure than existing systems, it is not foolproof. We know that blockchain can provide opportunity for fraud in relation to the authenticity of the documents and information placed on the chain and the creation and use of false identities from that information. Even in the absence of fraud or coercion, mistakes made in recording key information can be difficult to correct. More widespread use of blockchain for identity authentication and verification may reveal new security vulnerabilities in addition to those we now know.

To address this potential downside, a hybrid approach can be a way forward. For example, distributed ledgers for identity authentication can be used under existing KYC systems. Blockchain can use source data from various government offices, such as passport, motor vehicle and the post offices, and from utility companies, to prove a person's identity. The Illinois Blockchain Initiative is an example in the U.S. Illinois was the first U.S. state to create a consortium of state and county agencies to collaborate and explore innovations presented by distributed ledger technology (Thomas 2016). Similar blockchain-based approaches have been considered and implemented by other U.S. states (Desouza, Chen, and Somvanshi 2018). Distributed ledger technolgy can be developed within existing state and national frameworks for digital identity, but there is also scope for a regional, transnational identity, such as is underway within the European Union (E.U.) (European Commission 2023) and more broadly amongst other trusted nations. When used in this way, blockchain can provide greater protection for identity information and documents because documents do not have to be copied and stored in multiple databases. This approach can also empower individuals with greater control over when and by whom their information is accessed and provide more transparency on that access.

4. Global legal basis and standard

Blockchain was designed to remove the need for a traditional intermediary. This approach fits well with notions of sovereign identity and individual control that are grounded in autonomy. Control by the individual is important on many levels, including who accesses an individual's identity documents and identity information, and when and how that access is permitted. A right to identity that is based on individual autonomy exists under international law and this right to identity has grown in importance recently.

The right to identity is a fundamental human right that arises at birth under the Convention on the Rights of the Child (CRC), which has been ratified by almost all nations, the major exception being the U.S. A right to identity is expressly included in Article 8 and the CRC distinguishes this right from the right to privacy in Article 16. Article 8 was included in the CRC as the result of a campaign by the grandmothers of "The Disappeared" in Argentina for a right to identity (Hodgkin, Newell, and UNICEF 2007). They asserted that Argentina's adoption laws at the time facilitated illegal adoption and child placements by concealing children's real identities and by creating false identities. Under Article 8 (1) of the CRC, there is an express right to identity. Although the CRC is confined to rights of minors, considering the nature of the right to identity, there is a strong argument that the right continues to adulthood.

In the E.U., the European Court of Human Rights (European Court) recognizes the right of both minors and adults to identity under Article 8 of the European Convention Protection of Human Rights and Fundamental Freedoms (ECHR). Furthermore, the argument for recognition of a right to identity for all has also been considerably strengthened by the formal adoption of SDG 16.9, which requires that

all U.N. member states provide legal identity for all, including birth registration, by 2030.

A right to identity can also be recognized under the International Covenant on Civil and Political Rights (ICCPR) which, unlike the CRC, has been ratified by the U.S. Article 1(1) of the ICCPR states, "All peoples have the right of self-determination. By virtue of that right they freely determine their political status and freely pursue their economic, social and cultural development." Artcle1 (1) of the ICCPR applies to all people; and it is worth noting that the International Covenant on Economic, Social and Cultural Rights (ICESCR) contains an identical provision. The CRC and the ICCPR can provide theoretical legal basis for recognizing the right to identity for all individuals and, hence, the right to digital identity.

Depending on jurisdiction and circumstances, these treaty provisions may be invoked to protect the integrity of identity information on the blockchain. The ICCPR potentially has greatest impact on state conduct through the monitoring of national implementation of the ICCPR by the U.N. Human Rights Committee (UNHRC). The UNHRC has not clearly defined self-determination in Article 1 of the ICCPR. However, while the exact meaning and application of Article 1 is open to interpretation, it is generally considered to be in-line with the international legal meaning of self-determination, and to cover both the internal and external aspects of the right identified by the United Nations. The internal aspect which is most relevant to digital identity is the right of all peoples to freely pursue their economic, social, and cultural development without outside interference. The external aspect of self-determination implies that all peoples have the right to determine freely their political status and their place in the international community based upon the principle of equal rights.

While the external aspect has not been the subject of judicial consideration in this context, it can arguably apply to digital identity in a global context. Digital identity is protected under Article 1(1) of the ICCPR which protects individual autonomy. Individual autonomy is directly relevant to the use of blockchain for identity authentication considering that blockchain purports to give the individual control over identity information and who can access it. Self-determination under Article 1 of the ICCPR invokes protection of the private sphere as advocated by Charles Reich (Reich 1991). According to Reich, the individual sector is the source of an individual power as necessary for the healthy development and functioning of the individual and is absolutely essential to the health and survival of democratic society. A right to identity is part of that personal sphere and can include the right to digital identity.

Treaty obligations can operate as international standards and may form the basis of legal action under national law to effectively regulate state conduct and uphold individual human rights. However, at present, the UNHRC considers that only individual rights recognized in Part III of the ICCPR (Articles 6 to 27 and not Article 1(1)) can be examined under the individual complaints procedure established by the Optional Protocol to the ICCPR. The first Optional Protocol to the ICCPR allows individuals to submit written communications to the UN Human Rights Committee. However, the country must be party to the ICCPR and the Protocol, and the individual who claims their rights under the ICCPR have been violated, must have exhausted

all avenues for domestic remedies. Although the UNHRC will not examine individual complaints based only on Article 1, ratifying nations must still report to the UNHRC regarding implementation of Article 1 of the ICCPR. All states must report on the measures they have adopted relating to the rights described in the ICCPR within one year of ratifying the ICCPR. After submitting their initial report, periodic reports are required every four years. The Committee examines each report and addresses its concerns and recommendations to the state as "concluding observations" (United Nations Human Rights Office 2022). This reporting is currently the most effective strategy in overseeing and encouraging compliance because the UNHCR findings are published. While there are nations that notoriously do not comply, for the most part, the observations by the UNHRC present significant moral and political impetus for nations that have committed to the treaty. This could be the basis for international recognition of the importance of digital identity, for the concomitant right to identity, and for establishment of an international protocol for protection.

5. Conclusion

Blockchain technology provides decentralized, cryptographically-signed proof of existence and the potential for individuals to control access to their identity information. In theory, an individual can provide access to select parts of their identity information and documentation on the blockchain. Blockchain technology provides greater security and significant benefits that herald the near future in identity, authentication, and verification. Transnational initiatives such as Estonian e-Residency, which is blockchain-based, are the beginning of expansion of digital identity beyond national boarders. Other countries and regions, most notably the E.U., are pursuing a similar expansion of digital identity. These developments are paving the way for similar progress in other regions and global expansion is next. While these developments can bring major benefits, there are accompanying risks that are largely dependent on the rigor of processes for authenticating identity and for dealing with unintended effects.

The next evolution toward a global, digital identity will present challenges for nations that will require cooperation and trust that go well beyond the type of trust that underpins blockchain. Policy makers and legislators will have to ensure there are adequate security protocols in place and a supporting legal framework to protect an individual's right to an accurate and functional digital identity.

While there have been notable national and, more importantly, transnational successes, they have involved small nations with technical, cultural, and legal similarities and synergies. Large-scale, diverse applications are as yet untested and the ensuing consequences and implications are not yet known. Some of the current concerns about blockchain, such as scaling and its perceived environmental impact, are likely to be addressed by technological advancements in coming years.

However, the most significant issues impacting identity relate to its authenticity and integrity and individual rights. As discussed, there is the risk that identity information authenticated on the blockchain but which is otherwise invalid may find its way into traditional channels to enable creation of false identities. Apart from concerns about illicit activity that this may shield, if identity authentication is

compromised, it could undermine the integrity and reliability of the scheme, whether it be national, transnational, or global. These issues are unlikely to be solved by technology alone.

International law therefore has a crucial role. The foundation exists for formal recognition of the right to identity as a fundamental human right and for establishing norms of state conduct for giving effect to that right.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This material is based upon work supported by the National Science Foundation under Award No. [NSF AWD-7775009].

References

Australian Government. 2023. "Digital Identity System." Home | Digital Identity.

Desouza, K., Y. C. Chen, and K. K. Somvanshi. 2018. "Blockchain and U.S. State Governments: An Initial Assessment." https://www.brookings.edu/blog/techtank/2018/04/17/blockchain-and-u-s-state-governments-an-initial-assessment/.

E-Estonia. 2019. "Estonian Blockchain Technology." https://e-estonia.com/wp-content/uploads/2019sept-nochanges-faq-a4-v03-blockchain-1-1.pdf.

European Commission. 2023. "European Digital Identity." European Digital Identity (europa.eu).

Gov.UK. 2023. "Enabling the Use of Digital Identities in the U.K." Enabling the use of digital identities in the UK – GOV.UK (www.gov.uk).

Hodgkin, R., P. Newell, and UNICEF. 2007. "Implementation Handbook for the Convention on the Rights of the Child." 3rd ed., pp. 97–109. https://digitallibrary.un.org/record/620060?ln=en.

PricewaterhouseCoopers. 2019. "Estonia – the Digital Republic Secured by Blockchain" estonia-the-digital-republic-secured-by-blockchain.pdf (pwc.com).

Reich, C. 1991. "The Individual Sector." *The Yale Law Journal* 100 (5): 1409. https://doi.org/10.2307/796695

Sullivan, C. 2006. "The United Kingdom Identity Cards Act 2006 – Proving Identity?" *Macquarie Journal of Business Law* 3: 259.

Sullivan, C. 2018. "Digital Identity – from Emergent Legal Concept to New Reality." *Computer Law & Security Review* 34 (4): 723–731. https://doi.org/10.1016/j.clsr.2018.05.015

Sullivan, C. 2010. "*Digital Identity: An Emergent Legal Concept*. http://www.adelaide.edu.au/press/titles/digital-identity/

The World Bank. 2016. "Enabling Digital Development: Digital Identity." World Development Report 2016. https://documents1.worldbank.org/curated/en/

Thomas, S. 2016. "Illinois Blockchain Initaitive." Department of Innovation & Technology. Microsoft Word -NASCIO IL 2018-Emerging and Innovative Technologies-Blockchain.docx.

United Nations Human Rights Office. 2022. "Reporting Guidelines." OHCHR | Reporting guidelines.

United Nations. 2023a. "Department of Economic and Social Affairs, Sustainable Development." Goal 16 | Department of Economic and Social Affairs (un.org).

United Nations. 2023b. "United Nations Legal Identity Agenda at Home – UN Legal Identity Agenda." Home—UN Legal Identity Agenda.