9

Blockchain, Digital Identity, E-government

Clare Sullivan and Eric Burger

Introduction

This chapter examines the legal and technical implications of the application of blockchain technology to authenticate and verify identity for e-Government services and transactions.

On 25 September 2015, the United Nations (UN) General Assembly formally adopted the 2030 Agenda for Sustainable Development which consists of 17 Sustainable Development Goals (SDGs) and 169 specified targets to be achieved by member nations within the next 15 years. A major objective is set by SDG 16.9 is for nations to "[b]y 2030 provide legal identity for all, including birth registration." This is a goal in its own right and it underpins seven other SDGs to be achieved by the UN

C. Sullivan (✉)
Center for National Security and the Law, Georgetown University,
Washington, DC, USA
e-mail: cls268@georgetown.edu

E. Burger
Computer Science, Georgetown University, Washington, DC, USA
e-mail: ewb25@georgetown.edu

H. Treiblmaier, R. Beck (eds.), *Business Transformation through Blockchain*,
https://doi.org/10.1007/978-3-319-99058-3_9

member nations. This is the first time that a legal identity for all persons has been officially stated as a global objective. It is a development that has significant implications for governments and individuals.

In a digital world where nations are moving to e-government systems that require a digital identity to transact, the goal of a legal identity for all is, for all practical purposes, a digital identity for all. "Legal identity" is not defined in SDG16.9 and unlike the terms "legal person" and "legal entity," legal identity is not a term which has legal meaning. Identity is not a concept traditionally recognized by the law in many countries, particularly those with a common law legal heritage. Even in civil law countries, where there is a legal concept of identity, it was developed for another era and does not address the nature and implications of a digital identity. This chapter outlines the typical composition and functions of digital identity and discusses its commercial and legal importance, and its emergent legal nature in light of SDG 16.9. This discussion highlights the importance of the accuracy and integrity of digital identity to both individuals and governments.

The application of blockchain technology to identity authentication and verification has the potential to fundamentally transform the way identity information is controlled, authenticated, and verified. This development has been presented controversially, as the means of creating an entirely new and separate virtual legal regime outside existing frameworks and norms. However, blockchain technology can be used within existing national and international legal frameworks to address security vulnerabilities inherent in existing procedures for identity authentication, verification, and storage. This chapter examines the legal, policy, and technical implications of this application of blockchain technology to digital identity, in the context of SDG 16.9, with a focus on the privacy and security implications.

The Evolution of Digital Identity as a Legal Concept

Digital identity is the unique identity assigned to an individual under a particular digital identity scheme, typically a government-backed scheme. Digital identity is composed of information that is derived primarily from a person's birth certificate which is the primary and seminal identity document. While the birth certificate and other identity documents are usually still in paper form, digital identity is stored and transmitted in digital form.

Historically, identity has been a nebulous notion under the law, particularly in common law countries. In contract law, for example, identity has largely been in the background as the law focused on whether there is an agreement and particularly whether there is a meeting of the minds necessary for a contract, informed consent, and arms-length dealing. This focus, which mainly developed in response to commercial practice in the nineteenth and twentieth centuries, led to identity being largely pushed to the sidelines in commercial dealings. Twenty-first century technological advances have created a whole new environment for interaction, including for commercial dealings, that does not involve personal acquaintance or even any personal dealings. As transactions previously conducted in person are replaced by those without any personal interaction, the requirement to have and to present a digital identity for transactions has increased to the point that it is now a primary way an individual transacts.

Digital identity is the means by which a person is recognized and is able to transact in the digital age. As a consequence, digital identity has moved from a notion of uncertain nature, especially in the law, to an unprecedented level of personal, commercial, and legal significance. Now digital identity is poised to assume even greater importance in view the UN SGD 16.9 for a legal identity for all by 2030. This recognition of the significance of legal identity which is in effect digital identity, is a turning point. It makes clear the importance of digital identity to governments and the private sector, and especially to individual. It also strengthens the call for greater protection of digital identity and for recognition of individual rights in identity under international law.

Significance of Digital Identity

Note: in order to fit the confines of a book chapter, this section is necessarily a summary of the major points raised by Sullivan (2007, 2010).

Digital identity has revolutionized service delivery for commerce and the way in which government transacts and interacts with its citizens. It has brought many benefits by increasing the efficiency and cost effectiveness of service delivery, but there are significant ramifications, especially for individuals. This is because of the architecture of digital identity schemes and the functions of digital identity.

Government-authenticated digital identity is necessarily based on the premise of one person: one identity. An individual can legitimately have only one, official digital identity under the scheme. This is a major development because traditionally under the law an individual could usually legitimately use an assumed name. Likewise, one could create a pseudonymous, on-line identity, for example. The move to digitalize government services and transactions is driven not only by the need to reduce costs and to increase efficiency in service delivery but most importantly, to reduce fraud. Uniqueness and exclusivity are therefore essential features of digital identity and these features underpin schemes that use digital identity, especially for transactions. This is so regardless of whether a nation has formally established a national identity scheme and has designated it such; or whether a de-facto approach has been adopted whereby a digital identity is used by individuals to transact. In either case, although it may not be an objective, the reality is that a digital identity used for government services will be used for transactions with the private sector. That has been the experience to date and it is an outcome that is clearly inevitable. What this means is that the digital identity required for government transactions effectively becomes the individual's digital identity for transactions generally, and that identity becomes the primary means by which an individual is recognized and can enter into transactions in the digital age.

Digital identity, in this context, consists of two sets of information: transaction identity and a larger more extensive collection of information which records transactions and other information about the individual, depending on the mandate and particular purposes of the transacting organization/s. Each set of information has different purposes and functions and is of a different nature. The most main functions of transaction identity, that is the part of digital identity used for transactions, are first to recognize a person and then enable transactions, whereas the other information which makes up digital identity is more extensive and dynamic because it is updated to reflect transactions, and administrative information. It tells a story about a person and his/her transactions and usually other associated information; and that is its sole purpose. This information is personal information which is linked to an individual by, and through, transaction identity. It is generally protected under data protection law in most nations. This is because most nations have adopted the EU data protection model for domestic legislation, the notable exception being the United States.

Transaction identity is the most important part of digital identity, primarily because of its transactional functions. Transaction identity, that is, the part of digital identity required for transactions, is a small, defined, relatively static set of identity information, Typically, it is the individual's full name, date of birth, often place of birth, and identifying information such as a signature and/or a unique number such as a PIN but not all this information is necessarily needed for every transaction. The information needed varies depending on the requirements of the transacting entity and the nature and value of the transaction. Often all that is required for routine transactions is full name, date of birth, gender and a hand-written signature or PIN. This information is largely static and is derived from the seminal identity document, the birth certificate.

Digital identity schemes depend on two processes which are authentication of identity at the time of initial registration under the scheme; and verification of identity at the time of a transaction. On registration, an individual is required to establish his/her identity by providing identity documents which usually include birth certificate, passport, driver's and other licenses, marriage certificate if there has been a name change as a result of marriage, and other official documents such as those issued by government authorities, stating name and address. As mentioned, the birth certificate is the primary identity document from which most of the required documents, including other documents such as a passport, which are also considered primary, are derived. Identifying information such as signature, photograph, and biometrics such as a face scan, iris scans and fingerprints, are also usually recorded at the time of registration, or sometimes at the time an identity card is collected. The primary function of this information is to the link to the individual who presented the information and to link that person to the recorded digital identity.

The document checking required for identity authentication follows the Know Your Customer (KYC) requirements required under Anti-Money Laundering/Counter Terrorism Financing (AML/CTF) legislation that was widely adopted around the world following the September 11 attacks in the United States; and since that has been updated and expanded to regulate new money laundering targets and address new forms including use of trade in goods and services. The KYC protocols, also commonly referred to as the 100-point identity check, include an in-person interview at which time the applicant provides a range of specified identity documents that are ranked in terms of their standing to establish his/her identity. Originals of the identity documents are presented in person by the applicant and copies of those documents are made at that time by the authenticating agency for the record as required by the AML/CTF legislation. Much depends on the accuracy and integrity of this process including whether there is robust and independent checking of the presented documents because the information recorded from these documents establishes an individual's digital identity, particularly the set of information required to transact.

After registration, transaction identity is by the individual to transact. Identity is verified when all the required transaction identity information as presented matches the information on record. Transaction identity operates much like a key to allow access to the system to enable transactions. First, one digital identity is located from all the identities registered under the scheme; and then that identity is verified to enable it to transact under the scheme. Irrespective of whether the transaction identity is presented in person or remotely, if all the information as presented matches the information on record, then the system automatically authorizes dealings with that identity. Of course, the assumption is that dealings are with the person who presents the transaction identity but the system in fact deals with the digital identity (Sullivan 2016).

To understand transaction identity, we need to understand who, or what, is a person in law. However, this is the subject of much debate. Central to this debate is whether the legal person must "approximate a metaphysical person" (Naffine 2003). The orthodox positive view is that legal personality arises from rights and duties rather than from intrinsic humanity. The most well-known example is a corporation which the law has endowed with legal personality. For more in-depth discussion of the point, see Sullivan (2012, 234).

Transaction identity consists of information which has both meaning and function and arguably of a distinct legal character. The transacting entity deals with transaction identity, not with the individual. Invitations to treat and contracts are made with that identity—an identity that is composed of digitally stored information, which is accorded authenticity by the system and which arguably has legal personality, Transaction identity is a construct. It is a collection of designated information that is given legal status and effect by the scheme. It is information which, as a collective, has meaning and function. As such, it challenges the traditional legal approach on many levels and while it may seem bold to assert that it is endowed with legal personality, when viewed from the perspective of other disciplines such as computer science, the notion that information has function, as well as meaning, is well established (Sullivan 2016).

To illustrate these points, note that when considered separately and independently, the information that comprises traction identity is of limited use even in definitively identifying an individual. For example, unless it is especially unique, name alone will not single out an individual from a population. As a set, however, the information that constitutes transaction identity is more likely to identify a person; but transaction identity does more. It enables the automated system to transact. It is these operational functions that make transaction identity important, especially to an individual. This identity is generally the primary means by which a person is recognized and is able to transact in the digital era. Although a general assumption is that there is a reaching behind transaction identity to deal with a person, the system does not operate in that way. There is automated machine to machine matching of data. If for example, the transaction identity information as presented at the time of a transaction does not exactly match that on record, the system will not recognize the identity even if it is otherwise authentic and the system will not enable transactions. This can have serious implications, especially for an innocent individual. It underscores the point that the integrity of these systems depends on the accuracy of the information recorded at the time identity is authenticated, and on system integrity, particularly susceptibility to fraud and error (Sullivan 2016).

A key feature of all modern identity schemes is that the information needed to establish identity at the time of a transaction varies depending on the requirements of the transacting entity. Typically, all that is required for routine transactions is full name, date of birth, gender, and a signature or PIN. In some schemes biometrics are used though not typically for all transactions. Most routine transactions only involve matching a photo, hand-written signature, or a PIN. In many cases, only signature and photo will be checked. The primary purpose of this "identifying" information is to link the digital identity with a person but that link is relatively tenuous. All the identifying information currently used have error rates which can result in false positives and false negatives. Photo and signature checks have the highest incidence of error but biometrics also have error rates. For example, in a study in which supermarket cashiers compared real people not known to them to photographs on the credit cards they presented, only 50 percent accurately accepted or rejected the cards. When the card contained a photograph resembling the person presenting it, only 36 percent of the cashiers correctly rejected the card (Kemp et al. 1997). Also see (Hancock et al. 2000; Walker and Hewstone 2006; Hancock and Rhodes 2008; Kerstholt et al. 1992; Stevenage and Spreadbury 2006) for more on biometric identification errors.

A number of features and factors make digital identity susceptible to fraud, misuse and mistake in the initial authentication process, and subsequently when digital identity is used for verified transactions. The nature and functions of digital identity, and particularly of transaction identity, and its significance in the digital era means that the consequences of system error, or fraud are serious especially for the affected individual. Difficulty can arise in the individual establishing in both that "I am who I say I am" and in establishing "I am not who the record says I am."

Conventional Digital Identity

A conventional digital identity system is a centralized system that stores potentially encrypted or hashed values of identifiers and associates them with the digital identity. After establishing a digital identity, the individual can access that identity using an authentication system. Most authentication systems use one or more factors, usually derived from something you are (e.g., biometrics), something you have (e.g., a security token), or something you know (e.g., a password or PIN (Personal Identification Number).

There are two principal interoperable ways that digital identity systems extend identity beyond one system or network. For example, proprietary identity management systems, such as those offered by Facebook, Google, Microsoft, Yahoo, and others, provide digital identity within their proprietary platforms, but also will extend that identity to anyone who the user gives permission to the identity provider. You may have experienced this when logging into one system that asks you to use your Google or enterprise credentials to access a third-party service. The specific technology for this is known as OAuth (Hardt 2012).

This method has the benefit of reusing existing relationships the individual might have. However, there are very few instances of such identity providers using strong enrollment procedures. For the most part, what the identity provider is attesting to is the validity of an email address. However, some identity providers, such as universities and the Federal government, will be attesting to the actual identity of the individual.

Besides the (usually) weak identity verification on enrollment, the first method suffers from a number of security issues. First, if the underlying information is stored in a retrievable format, for example, actual passwords, social security numbers, addresses, etc., then there is the possibility of that information leaking due to a breach. Second, the availability of the identity service is at the pleasure of the identity provider. They may choose to withhold information to an entity the subject wishes to transact with. Finally, they may use or sell the subject's personal information without the subject's knowledge or consent.

The second convention method of identity is to use public key cryptography. In public key cryptography, we use mathematical functions that are easy to compute in one direction, but the inverse function is incredibly hard to compute. The conventional function we use is to take the modulus of the multiplication of two coprime numbers. While relatively easy to do the multiplication and remainder calculation, it is extremely hard to factor a large number. The mathematics of the most common public key cryptosystem, RSA, is such that we can publish one of the factors as a public key and one of the factors as a private key. People can use the public key either to encrypt a message for the key owner that only the key owner, with the private key can decrypt or to decrypt a message from the key owner that only the key owner could have encrypted using their private key (Rivest et al. 1978).

One issue with public key cryptography is knowing the public key is really the public key of the subject. In digital commerce we do not generally assume the subject can physically meet the transacting party in order to exchange keys. The conventional approach is to use a Public Key Infrastructure (PKI). In a PKI, there will be a set of trusted Certificate Authorities (CAs). The public keys of this trusted set of CAs are distributed with operating systems, browsers, etc. With that bootstrap of public keys in devices, we then have the CAs sign the public key of the subject. When an entity is presented with the subject's public key, the entity verifies that a trusted CA has signed the subject's public key.

In this manner, the CA acts as the identity provider. The transacting entity trusts the CA to do the appropriate level of identity validation for the use of the public key. For example, in order to issue a domain validated certificate, for using TLS (Transport Layer Security protocol), for example, for HTTPS (secure Web browsing), a CA validates the requestor in fact has control over the domain in question. For an enterprise validated certificate (where the green lock icon with the corporate name highlighted), the CA validates the existence of the company and that a registered agent is requesting the public key signing. The US Federal government, when it issues a PIV card (Personal Identity Verification card) or CAC (Common Access Card), or the Estonian government, which it issues an e-ID card, requires a face-to-face interview, often including biometric collection and verification.

What distinguishes the first from second model of conventional digital identity is in the former model, the identity provider holds all of the information on the subject and access to verification data is under the control of the identity provider. In the latter model, the CA only vouches for the veracity of the identity by the kind of signature they calculate over the subject's public key. From that moment on, the subject is in control of whom they give their public key to or uses of their private key.

Blockchain and Digital Identity

Public blockchain is best known as the technology that underpins Bitcoin, a virtual peer-to-peer currency and payment system that enables users to transact without using a traditional intermediary such as a bank or government department or agency. Simply explained, a blockchain is a chain of linked records called blocks. As data is added, new blocks ae added to the chain. Each block has a hashed key that links it to the preceding block, a timestamp for when it was added or altered, and transaction data. A feature of blockchain is its immutability, meaning that once a transaction is recorded on the chain, data cannot be retroactively altered. With public blockchain, at least a majority of nodes computing the blockchain would have to collude to undo a transaction. This is highly unlikely to occur in practice. We call the distributed nature of this verification of blockchain "consensus based." Unlike the conventional digital identity systems, where one either trusts in the organization running the identity provider or the organization running the CA, public blockchain is said to create a new trust-based system, where the trust is in the network of servers and the software system, not on any one particular company.

Public blockchain technology provides non-repudiation of events by a group of distributed servers, usually controlled by different people in different locations. A block chain is a public ledger distributed across many computers, using cryptography to ensure the security and accuracy of the information stored in the ledger. Most public blockchain systems use keys and signatures to control who can do what within the shared ledger. Blockchain nodes within the network have their own copy of the ledger, and transactions added to the ledger are public and broadcast to all the participating nodes so in effect, that transaction appears in all copies of the blockchain. According to rules agreed to by the network, one, any, or all of the participants can add transactions to the blockchain. Blockchain algorithms aggregate transactions in "blocks," and blocks are added to the chain of existing blocks, using a cryptographic signature. For public blockchains, that signature includes a proof of work. This proof of work makes it cryptographically unlikely that anyone, including a fraudster of hacker, can alter prior blocks. The public and distributed nature of the blockchain makes it hard to get a false block accepted by the network.

Trust Enabled by Blockchain

From a computer science perspective, there is no difference between a sovereign state issuing a proprietary digital identity stored on a computer under the state's control and a digital identity stored on a blockchain. However, there are practical differences that result in s models that are easier to embody on a blockchain. The issue for the conventional digital identity is the subject has to trust the state or agent (such as a company) to protect the subject's identifying information; to only release that information to parties with a need to access the information; to ensure the information is not incorrectly altered or lost; and that the information is available when needed. Moreover, the subject is trusting the state or agent to not lie about the identifier. Finally, the digital identity is "owned" by the state or agent: they have total control over the identity.

A public blockchain provides secure, public storage with integrity guarantees. Information on the blockchain cannot be maliciously altered or withheld (although one could argue that since the information is open for all to see, this is a bug, not a feature). The information is highly available, given there are hundreds of copies of the blockchain in the network. Most importantly, except for the organization promoting and managing the policy for the blockchain, the blockchain itself and the data on it is not owned by anyone.

Note that many blockchains being established today have concepts of built-in access rights. The idea is to give the subject access control to the data via encryption, instead of identity provider-enforced policy. For example, the subject can encrypt select data on the blockchain belonging to the subject and the subject can select who gets the appropriate key(s) to decrypt the data.

Example of Blockchain for Identity Use

An example of the use of blockchain is to provide a digital identity for a refugee who is unable to produce documentation such as a birth certificate, which is the seminal identity document, to establish his/her identity. The refugee may have no identity documents, but the refugee may have nearby family relations. Identity is important as an individuals' inability to produce any identity documents can hamper the provision of humanitarian aid and the person's ability to obtain employment, education, health care, and generally build a new life. One idea is to create a web of trust, similar to the web of trust established by the PGP (Pretty Good Privacy) public key web of trust. Extending the web of trust to digital identity, a person who is undocumented may say his name is Jamal al-Assad, that he was born in a particular village, on a particular date. That assertion may be substantiated by other members of his family such as his parents and siblings and member of his village who may say for instance that they were neighbors at the time of his birth and know he was borne into the family at the asserted time. One could setup a blockchain-based digital identity system such that individuals can "vouch" for the identity of others on the blockchain. With a web of people vouching for each other, the consensus is that this refugee is who they say they are, and that "fact" is substantiated by the blockchain community.

This is the basic approach used by Bitnation, one of several blockchain-based initiatives. Bitnation describes itself as "a decentralized, open-source movement, powered by the Bitcoin blockchain 2.0 technology, in an attempt to foster a peer-to-peer voluntary governance system, rather than the current "top-down," "one-size-fits-all" model, restrained by the current nation-state-engineered geographical apartheid, where your quality of life is defined by where you were arbitrarily born." Bitnation further states that it "provides the same services traditional governments provides, from dispute resolution and insurance to security and much more—but in a geographically unbound, decentralized, and voluntary way. Bitnation is powered by Bitcoin 2.0 blockchain technology—a cryptographically secured public ledger distributed among all of its users. As we like to say—"Bitnation: Blockchains, Not Borders." (Tempelhof et al. 2017) Key to this view and these services is the use of blockchain to vouch for claimed identity outside existing legal frameworks. As noted above, rather than using strict, mostly deterministic KYC procedures as required by AML/CTF legislation, identity is authenticated and verified by the community, using a distributed ledger on a global, open platform, essentially establishing a system of self-sovereign identity.

Bitnation gained international prominence by providing an emergency block-chain-based digital identity to enable access to aid for Syrian refugees who cannot establish their identities to open a bank account to receive funds. A digital identity is established on the blockchain and financial aid is delivered to the refugee through a Bitcoin Visa card. Susanne Templehof, founder of Bitnation explains that "the Blockchain Emergency ID is a rudimentary emergency ID, based on the blockchain technology, for individuals who cannot obtain other documents of identification." "[W]e are providing emergency ID and then this visa card because most refugees will be unemployed. They won't be legally able to get a job for several years and they can't open a bank account." The blockchain is used to cryptographically establish an individual's existence and family relations to generate a digital identity. That identity then generates a Quick Response Code, an optical label that contains information in machine-readable form that can be read by a mobile phone, to apply for a Bitcoin Visa card which can then be used throughout Europe without the need for a bank account (Allison 2016).

Note that on the face of it, Bitnation could have setup a conventional data base and provided this service as a conventional identity provider. However, a question that would immediately raise is, "By what authority does Bitnation issue digital identity?" While blockchain does not directly answer that question, it does address the issue. Namely, if Bitnation used conventional means to be an identity provider, individuals, enterprises, and states would have to fundamentally trust Bitnation to properly account for the identities and links in its identity web of trust; one would have to trust the integrity of Bitnation's data base and operations; and one would have to trust the integrity of the links in Bitnation's web of trust. For conventional identity providers, we have this trust based on fiat and audit. We trust the digital identity provided by a government because the government asserts the identity is accurate (fiat). We (sometimes) trust a digital identity provided by an enterprise because beyond the enterprise asserting the identity is accurate, that enterprise may be subject to government-imposed laws (such as KYC-AML for banks) or the enterprise may, for example, voluntarily subject itself to audit to raise the public's trust expectations in the enterprise's assertions of its customers' digital identities.

As evidenced by the quote above by Bitnation's founder, Bitnation is somewhat antagonistic to traditional government sovereignty. It would be unlikely for any government to provide or accept Bitnation's claims of data integrity or conventional third-party audits of the Bitnation system. By definition, Bitnation is not following conventional KYC-AML identity verification norms, as refugees do not have the means to conventionally prove their identity.

Bitnation uses blockchain to overcome these issues of trust. All refugee's digital identities are published, for all to see, on the blockchain. As the blockchain is immutable, one cannot change the information on the blockchain, such as a person's name, place of birth, or family/trust relationships. Moreover, the web of trust assertions, such as "this is my son" or "I was the village elder and I vouch this individual was born and named as shown in the identity record" are all public. That means the individuals themselves can build up a picture of identity assertions, audit them, and third parties can also analyze the assertions to audit their validity. For example, a claimed village elder who vouches for one person in Aleppo cannot also vouch for another person in Homs on the same date.

The utility of the blockchain-based emergency digital identity in these circumstances are clear. However, the process of identity validation bypasses existing national and international governance and regulation which has been established for good reason and as a result there are broader consequences. The most serious possibility is the creation of a digital identity without lawful basis that can be used to conceal real identity and associated records. Although the digital identity created on the blockchain is justified as a short-term solution, for a person who is otherwise unable to establish identity, in effect this process creates a digital identity for the next stages of the person's life. Bitnation claims that it is unlikely that a false identity can be created because it requires collusion, it is certainly not impossible. The even more concerning aspect is that while a person's basic identity information, that is, full name, date of birth, place of birth, and gender as substantiated by consensus, may be accurate, past history including involvement in criminal and subversive activities are not known nor verifiable.

According to Templehof, the broad objective of Bitnation is "to gain recognition for Bitnation as a sovereign entity, thus creating a precedent for open-source protocol to be considered as sovereign jurisdictions." (Allison 2018) In effect this will "establish a new virtual jurisdiction with its own rules." In addition to the huge increase in stateless people in Europe from the refugee crisis, Bitnation is looking at developing markets, assisted economies and the gray economy. For example, the registry capabilities of blockchain are being considered as a means of recognizing land rights in the developing world in countries like Ghana, where 70 percent of land is reportedly untitled and land is traded peer to peer. In other words, blockchain technology is seen as the basis for a new system for a full range of commercial applications outside existing legal governance and regulation. Templehof cites the example of marriage between a same sex couple which is not recognized as legal in many countries but can be recognized on the blockchain. "[T]o get married on the blockchain would take you ten minutes between writing the contract and time-stamping it." She points out that "you could marry as many people as you want, any gender." Templehof warns, however, that "the intrinsic immutability of blockchain systems means it could be very hard to get a divorce, suggesting short term marriage contracts of four or five years at a time."

There are also broader implications. The use of blockchain in this type of situation to create an emergency, temporary digital identity to enable aid to be given to an individual who is unable to otherwise establish his/her identity may be admirable. However, it does raise security concerns particularly in the use of this means to create and new, false identity and to engage in nefarious and covert activity ranging from crimes like money laundering to activities endangering national and international security.

Although Bitnation may aspire to sovereignty, as an autonomous cyber jurisdiction, the transactions registered by Bitnation do not have legal standing. Nevertheless, the use of blockchain technology in this way can have potentially serious implications for legitimate identity and the activities it supports especially if information verified outside existing legal framework transitions into the real world. For example, depending on the rule and rigor of the checking required for registration under a particular national identity scheme, a name change as a consequence of a marriage recorded and recognized on the blockchain, may be used to register that name as part of a national digital identity scheme, thereby creating a new digital identity and in effect, a new legal identity, that is not in fact correct or legitimate. It is this potential for cross-over into the real world that is the most significant risk to the integrity of digital identity. An iteration that operates entirely outside existing law can lead to creation and use of new, false identities and illegal use of legitimate identities as ideal vehicles for fraud, tax avoidance and laundering of money that subsequently can be used to fund illicit activity ranging from organized crime to terrorist activity.

Bitnation's model of self-sovereign blockchain-based identity is problematical and is highly unlikely to gain mainstream acceptance or any kind of legal recognition. However, it is an example of using a public blockchain to record an "authoritative" digital identity for an individual outside the context of a sovereign state or proprietary platform. As such, blockchain technology has the potential to fundamentally change the way identity information is controlled and authenticated.

Blockchain and E-government

What if individuals and governments and private sector organizations could benefit from the advantages of the use of blockchain for identity within exiting legal frameworks? This is an approach which is of considerable interest to governments.

Estonia's use of blockchain concepts predates the Bitcoin blockchain. Estonia was an earlier adopter with blockchain hash publication underpinning its national identity scheme for citizens and permanent residents and for its newer international e-Residency program. Specifically, Estonia uses the concept of generating a one-way hash of the data it wants to protect, combined with prior hashes, and then publish that information publicly. In the early 2000s, that information was literally published in newspapers around the world. Today, that publication is on a blockchain-like chain of hashes.

Estonia's approach is to revolutionize traditional approaches rather than integrate blockchain into procedures such as KYC (Sullivan and Burger 2017). Other countries are seriously considering integrating blockchain technology into their identity checking protocols including the KYC requirements. The United Kingdom for example, is looking at the advantages of blockchain and in the United States, the state government of Illinois is undertaking six blockchain pilot programs including for a blockchain-based birth registry/ID system. The idea is to create "a secure 'self-sovereign'" identity for Illinois citizens during the birth registration process. The Illinois Blockchain Initiative commented, "To structurally address the many issues surrounding digital identity, we felt it was important to develop a framework that examines identity from its inception at child birth… Identity is not only foundational to nearly every government service, but is the basis for trust and legitimacy in the public sector." The site goes on to explain that in the proposed framework, "government agencies will verify birth registration information and then cryptographically sign identity attributes such as legal name, date of birth, sex or blood type, creating what are called 'verifiable claims' or attributes. Permission to view or share each of these government-verified claims is stored on the tamper-proof distributed ledger protocol in the form of a decentralized identifier… This minimizes the need for entities to establish, maintain and rely upon their own proprietary databases of identity information." This approach is notable because it applies from birth and in that regard accords with both SDG 16.9 and the fact that digital identity is based on information which is mostly established at birth. The idea is to "ta[ke] the source data from the passport office, from the DMV, from the post office, from the utility companies, and using that to prove granular things about a person's identity" (Illinois Department of Commerce and Economic Opportunity 2017).

Conventional KYC-AML laws require the enterprise validating the customer's identity to scan and store the customer's primary documentation, such as their passport or identity card. With a blockchain-based system, the source documentation can be stored off of the blockchain, the document hash can be compared to the hash on the blockchain, and the comparison can be stored on the blockchain. The benefits of this approach are that the enterprise need not store the source documents, yet the enterprise can also prove, via a ledger entry on the blockchain, they performed the KYC-AML validation. By not storing the source documents, the enterprise cannot lose them in a breach—it is impossible to lose data that one does not have.

By leveraging blockchain technology, identity providers can enable identity subjects to control the use of their information. It is true that an identity provider can promise subjects that they will contact the subject before divulging their information or verifying their identity. However, all the subject has is the provider's promise. With public blockchain technology, the subject can verify that only hashes of their personal data or encryption of their personal data with user-generated keys are stored. In that latter, more extreme version of data protection, the data user must contact the subject to obtain a decryption key to access the data. In other words, the user is directly in the loop for data retrieval, and the user can thus choose to not divulge their keys, and thus their data.

When used in this way, blockchain has clear benefits, especially in giving an individual control over his/her identity information and documentation and who has access to them. Distributed ledger technology like blockchain obviates the need for private sector organizations verifying the originals of identity documents such as birth certificate, passport, and utility bills, to copy, upload, and store a scan. Instead, a person can place his/her identity information and documents on the blockchain and use the PKI, directly authenticating the source data from the passport office or other government departments and utility companies. Security is improved because copies of identity documents are not stored on a number of databases, and are not as susceptible to erasure, loss, unauthorized access, alteration and misuse. This system also assists persons in the situation faced by Syrian refugees who unable to obtain or verify their identity information from official sources because they and the information held no longer exists. Blockchain is a comparatively more durable and enduring means of authenticating and verifying identity.

Security is improved because the identity documents are stored on, and authenticated by, the distributed ledger without the need for multiple copies to be retained on government and proprietary systems as part of the KYC process. Instead, a record of the authorization is stored in the chain. It improves security in that it eliminates multiple copies that increases the odds of them compromised and the blockchain provides a record of attribution and is generally a more accountable process. It is true that access could be tracked and proved without blockchain, but that requires much more work, trust, and integration with an infinite number of applications. Most importantly, blockchain could provide the individual with more control. The individual controls who accesses his/her identity documents and identity information and the timing of that access. The blockchain also provides the individual with timely information about who in fact accessed that information and when that occurred. Note that if implemented poorly, this model of total sunshine has a problematic feature: while it is true that anyone can validate that an individual's transactions occurred and it is impossible to erase or modify those transactions, everyone can see the individual's transactions. For example, while one could verify that an individual opened a bank account, got married, and purchased a house, one could also learn they paid a criminal debt and was admitted to a mental institution for a period of time.

Blockchain is touted as being more secure than existing systems and that appears to be borne out in its use for Bitcoin, but the security of its broader use, especially for identity documents and information is untested and is unknown. Moreover, blockchain is like any complex system in that implementation errors, as well as architectural errors, can result in undesired behavior (Price 2016). It is a new approach which may involve new security vulnerabilities. It may, for example, be found to have issues as to the authenticity of the documents and accuracy identity information placed on the blockchain and with the veracity of the identity authentication and verification process. The legal issues regarding responsibility and accountability of those who vouch for the accuracy of that information and the ensuing consequences, are also entirely undeveloped and as yet unknown. Blockchain changes the premise of established law. The applicable law depends on whether the blockchain is owned and operated by government, or whether there is an outsourcing arrangement with a private entity (the model being followed in many jurisdictions), and the location and control of the blockchain ledgers. However, for example, most data protection law is based around the data controller being a government or private organization that is processing an individual's personal information. Public blockchain challenges the balance of power so that in effect the individual becomes the data controller What is clear is that the legal implications are complex.

Blockchain, Digital Identity, E-government and a Right to Identity

The full legal implications of blockchain are not yet known but use of a distributed ledger clearly raises new legal issues regarding responsibility for the documents and information stored and accessed on the ledger and for the ensuing consequences if their accuracy, integrity, and security is compromised. While there is much uncertainty as to how current data protection and privacy law will and can apply, there is scope for development of a much more effective individual right—the right to identity.

An individual right to identity exists under international law and is poised for greater recognition in light of UN SDG 16.9 and the use of blockchain for identity. The right to identity is a fundamental human right that arises at birth under the Convention on the Rights of the Child (CRC), which was adopted and opened for signature, ratification, and accession by UN General Assembly Resolution 44/25 of 20 November 1989, entered into force 2 September 1990, in accordance with Article 49. A right to identity is expressly included in Article 8 and the CRC distinguishes the right to identity 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 the right to identity (Detrick et al. 1992). They argued that the country's adoption laws enabled concealment of children's true identities and the creation of false identities. Their campaign led to Argentina recognizing a constitutional right to identity (Avery 2004).

Under Article 8 (1) of the CRC there is an express right to identity and although the CRC is confined to rights of minors, considering the nature of the right to identity, arguably it continues when a child becomes an adult. The argument that a right to identity for all be recognized has now been considerably strengthened by the formal adoption by the UN General Assembly of Sustainable Development Goal 16.9 which provides that member states provided a "legal identity for all, including birth registration" by 2030 (United Nations 2015).

In the EU, an international leader in the development and recognition of human rights, the European Court of Human Rights (European

Court) under Article 8 of the European Convention Protection of Human Rights and Fundamental Freedoms (ECHR) has recognized the right of both minors and adults to identity.

The right to identity can also be recognized under the International Covenant on Civil and Political Rights (ICCPR), which was adopted by the UN General Assembly Resolution 2200A (XXI) of 16 December 1966, entered into force on 23 March 1976, in accordance with Article 49, for all provisions except those of Article 41; 28 March 1979 for the provisions of Article 41 (Human Rights Committee), in accordance with paragraph 2 of Article 41, particularly under Article 1(1):

> 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.

The CRC and the ECHR can provide the basis for legal action by an individual whose identity information is not accurately recorded or which has not been adequately protected on blockchain. The treaty obligations as standards may form the basis of legal action under national law or in the case of ECHR action may be taken under the treaty itself, though it should be noted that human rights claims have different objectives and standards of proof from typical damages claims. The former is designed to regulate state conduct and standards in upholding individual human rights, whereas the latter are primarily designed to compensate for damage caused, though usually the is a consequential impact on conduct and processes. As such, the ICCPR potentially has greatest impact on state conduct through the monitoring of national implementation of the ICCPR by the UN Human Rights Committee (UNHRC).

The right to self-determination under Article 1 of the ICCPR 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 (Sullivan 2016). Note that the HRC has not clearly defined "self-determination" in Article 1. Committee on the Elimination of Racial Discrimination (CERD) has identified an internal and an external aspect. The internal aspect as defined by CERD is "the rights of all peoples to pursue freely their economic, social and cultural development without outside interference. In that respect there exists a link with the right of every citizen to take part in the conduct of public affairs at any level." CERD states that "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 in areas other than colonization not been the subject of analysis, arguably it can ostensibly apply to digital identity.

Self-determination under Article 1 of the ICCPR invokes protection of the "private sphere" as advocated by Charles Reich (Reich 1991). "The individual sector" according to Reich is the " 'zone of individual power' necessary for the healthy development and functioning of the individual" and "absolutely essential to the health and survival of democratic society." A right to identity is part of that personal sphere, and arguably it now includes the right to digital identity (Sullivan 2016). Digital identity is protected under Article 1(1) of the ICCPR because the Article protects individual autonomy and that is directly relevant to the use of blockchain for identity authentication, especially considering that it purports to give the individual control over his/her identity information and who can access it.

The UNHRC refuses to examine individual complaints based only on Article 1. Although it has been criticized for this view, the HRC considers that that only individual rights recognized in Part III of the ICCPR (articles 6–27) can be examined under the individual complaints procedure established by the Optional Protocol to the ICCPR, adopted and opened for signature and accession by General Assembly resolution 2200 A (XXI) of 16 December 1966. However, nations including Estonia must report to the UNHRC regarding implementation of Article 1 of the ICCPR and this reporting is the most effective part of overseeing compliance. Because countries that have ratified the ICCPR must report every 4 years. The UNHCR publishes its findings, identifying any areas of concern. These "concluding observations," by the UNHRC are a significant moral and political obligation for a government like that of Estonia which has committed itself to complying with the treaty.

Conclusion

Digital identity, particularly digital identity established on blockchains, is revolutionizing the delivery of e-government. Classical identity is established through government-issued paper documents, such as birth certificates, passports, and identity cards. Modern identity is established through digital identifiers such as national identity numbers and digital identity certificates. While a national identity number can identify an individual, it does not authenticate that the 'person' asserting they have that number is, in fact, that person. This is why contemporary digital identity systems use public key cryptography, digital certificates, and secure access to the private keys through the use of passphrases, biometrics, and PINs.

The point of identity, especially digital identity, is to enable the individual to conduct transactions, whether they be transactions with the government, such as receiving benefits, paying taxes, voting, and so on; or transactions with other entities, such as banking, receiving a salary, buying goods, paying rent, and so on. These transactions, particularly the commercial transactions, happen because the parties involved trust the credentials. Specifically, they trust the credentials do in fact represent the authenticated identity the claim to represent.

We have raised issues with non-governmental entities that issue digital identities, more especially those whom do not follow enrollment validation that are on a par with the various KYC regulations. One would expect that over time, such digital identities would have less and less value. However, we have outlined the mechanisms used by Bitnation in their efforts to issue digital identities for individuals for whom it would be impossible to do a full KYC validation, as their paper documents have been lost or destroyed.

For a company like Bitnation, establishing trust using conventional means, especially given their apparent antagonistic relationship with established governments, would be virtually impossible. However, by using public blockchain technology, they are able to establish trust in their crowd-sourced identity verification system. Moreover, they are able to establish trust in the veracity and integrity of their identity assertions by leveraging the immutability of the blockchain and opportunity to have the data on the blockchain publicly available.

For a country like Estonia, which has a real threat of invasion from large, hostile nation states, using the chained hash technology of blockchain enables them to build an electronic government infrastructure that can withstand electronic or kinetic attacks, as well as the seizure of computer, data, and network assets.

Acknowledgments The Army Research Office provided funding for this paper through the Minerva Initiative agreement # W911NF-15-1-0595.

References

Allison, I. (2016, September 29). *Decentralised Government Project Bitnation Offers Refugees Blockchain IDs and Bitcoin Debit Cards.* Retrieved April 8, 2018, from International Business Times. https://www.ibtimes.co.uk/decentralised-government-project-bitnation-offers-refugees-blockchain-ids-bitcoin-debit-cards-1526547

Allison, I. (2018, February 8). *Bitnation and Estonian Government Start Spreading Sovereign Jurisdiction on the Blockchain.* Retrieved April 8, 2018, from International Business Times. https://www.ibtimes.co.uk/bitnation-estonian-government-start-spreading-sovereign-jurisdiction-blockchain-1530923

Avery, L. (2004). Return to Life: The Right to Identity and the Right to Identify Argentina's "Living Disappeared". *Harvard Wonem's Law Journal, 27*, 235.

Detrick, S., Doek, J. E., & Cantwell, N. (1992). *The United Nations Convention on the Rights of the Child. A Guide to the "Travaux Préparatoires"*. Dordrecht: Martinus Nijhoff Publishers.

Hancock, K., & Rhodes, G. (2008). Contact, Configural Coding and the Other–Race Effect in Face Recognition. *British Journal of Psychology, 99*(1), 45–56.

Hancock, P., Bruce, V., & Burton, A. M. (2000). Recognition of Unfamiliar Faces. *Trends in Cognitive Science, 4*(9), 330–337.

Hardt, D. (2012). *The OAuth 2.0 Authorization Framework.* Internet Engineering Task Force, RFC 6749.

Illinois Department of Commerce and Economic Opportunity. (2017, August 31). *State of Illinois Partners with Evernym to Launch Birth Registration Pilot.* Retrieved April 8, 2018, from https://www2.illinois.gov/IISNews/14759-DCEO_Birth_Registration_Pilot_Release.pdf

Kemp, R., Towell, N., & Pike, G. (1997). When Seeing Should Not Be Believing: Photographs, Credit Cards and Fraud. *Applied Cognitive Psychology, 11*, 211–222.

Kerstholt, J., Raaijmakers, J., & Valeton, J. M. (1992). The Effect of Expectation on the Identification of Known and Unknown Persons. *Applied Cognitive Psychology, 6*(2), 173–180.

Naffine, N. (2003). Who Are Law's Persons? From Cheshire Cats to Responsible Subjects. *Modern Law Review, 66*, 346–367.

Price, R. (2016, June 17). *Digital Currency Ethereum Is Cratering Because of a $50 Million Hack*. Retrieved 8 2018, April, from Business Insider. http://www.businessinsider.com/dao-hacked-ethereum-crashing-in-value-tens-of-millions-allegedly-stolen-2016-6

Reich, C. (1991). The Individual Sector. *The Yale Law Journal, 100*(5), 1409–1448.

Rivest, R., Shamir, A., & Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM, 21*(2), 120–126.

Stevenage, S., & Spreadbury, J. (2006). Haven't We Met Before? The Effect of Facial Familiarity on Repetition Priming. *British Journal of Psychology, 97*(1), 79–94.

Sullivan, C. (2007). Who's Who—Conceptualising Identity. *International Review of Law, Computers and Technology, 21*(3), 237–261.

Sullivan, C. (2010). *Digital Identity: An Emergent Legal Concept*. Adelaide: University of Adelaide Press.

Sullivan, C. (2012). Digital Identity and Mistake. *International Journal of Law and Information Technology, 20*(3), 223–241.

Sullivan, C. (2016). Digital Citizenship and the Right to Digital Identity Under International Law. *Computer Law and Security Review, 32*, 474–481.

Sullivan, C., & Burger, E. (2017). E-residency and Blockchain. *Computer Law & Security Review, 33*(4), 470–481.

Tempelhof, S., Teissonniere, E., Tempelhof, J., & Edwards, D. (2017, April). Retrieved April 8, 2018, from Bitnation Pangea | Your Blockchain Jourisdiction. https://github.com/Bit-Nation/Pangea-Docs/raw/master/BITNATION%20Pangea%20Whitepaper%202018.pdf

United Nations. (2015). *Transforming Our World: The 2030 Agenda for Sustainable Development*. Retrieved April 8, 2018, from https://sustainabledevelopment.un.org/post2015/transformingourworld

Walker, P., & Hewstone, M. (2006). A Perceptual Discrimination Investigation of the Own-Race Effect and Intergroup Experience. *Applied Cognitive Psychology, 20*(4), 461–475.