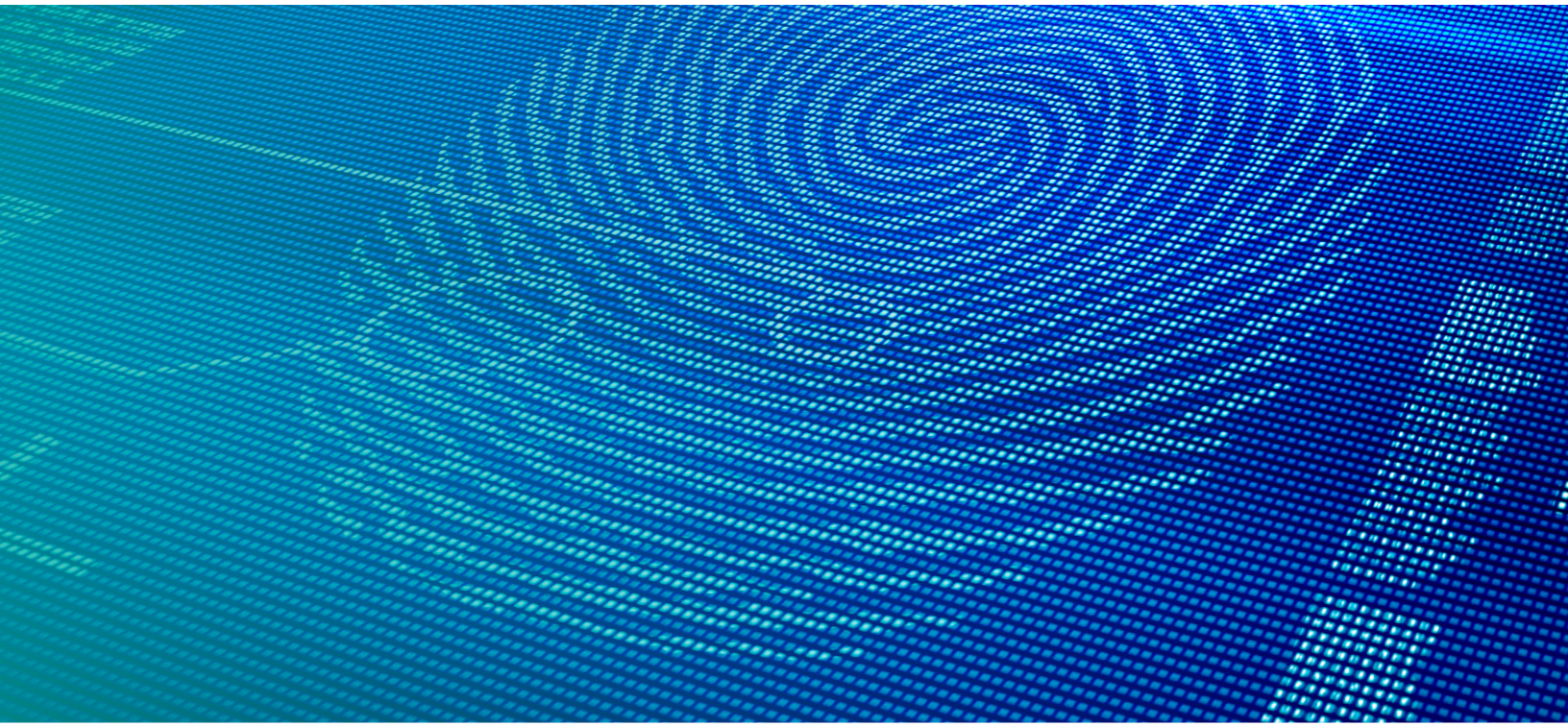
Self-Sovereign Identity and Distributed Ledger Technology: Framing the Legal Issues



JOSEPH CUTLER | PARTNER
+1.206.359.6104
JCutler@perkinscoie.com

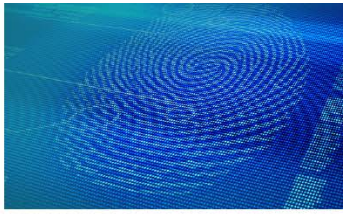
J. DAX HANSEN | PARTNER
+1.206.359.6324
DHansen@perkinscoie.com

CHARLYN HO | ASSOCIATE
+1.202.654.6341
CHo@perkinscoie.com

PerkinsCoie.com/Blockchain

Perkins Coie LLP | September 2018

PERKINSCOIE



About Perkins Coie's Blockchain Industry Group

Perkins Coie features the world's largest and leading Blockchain Technology & Digital Currency industry group. We were here when it all began. Our firm started advising clients about tokenization and bitcoin, and has since expanded to helping our clients pioneer numerous and diverse uses of blockchain technology.

LEADER, NOT A FOLLOWER

Established in May 2013, this industry group emergence was more of an evolution than a genesis. Through its Electronic Financial Services group, Perkins Coie has a long history representing technology companies that provide consumer and financial services, including: mobile payments, tokenized in-game assets, e-commerce services, and marketplace payment services. Naturally, when the first Bitcoin and other decentralized virtual currency companies emerged, Perkins Coie was uniquely situated to launch an industry group focused specifically on blockchain technology and digital currency that now has more than 40 lawyers advising clients across a range of issues. This group has helped more than 200 clients reconcile complex regulatory compliance questions, assess intellectual property opportunities, negotiate with regulators, and educate the greater population about the promises and complexities of blockchain technology.

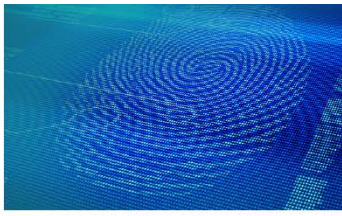
WE ARE HELPING SHAPE THE INDUSTRY

Our team participates as advisors to the Uniform Law Commission Study Committee in its drafting of a model Regulation of Virtual Currency Businesses Act. We serve as institutional members of The Chamber of Digital Commerce, the world's leading trade association representing the digital asset and blockchain industry, and are founding participants in many of the Chamber's initiatives including The Digital Assets Accounting Consortium, a resource for companies with operations involving digital assets, such as bitcoin; The Smart Contracts Alliance, an authoritative resource for smart contracts helping shape how smart contracts are understood, developed and adopted; the State Working Group, focused on tracking and influencing the various state regulatory and legal approaches to digital currency and blockchain technology; and the DC Blockchain Center, a strategic partnership between the Chamber and global technology incubator 1776.

YOUR LEGAL PARTNER IN INNOVATION

Our multidisciplinary group is on the front lines, helping clients address the complex legal issues faced by digital currency, blockchain, and other distributed ledger companies who are pioneering new solutions to many of today's market challenges. We provide regulatory compliance counseling, litigation support, consumer protection counseling, intellectual property support, corporate formation and maintenance, initial coin offering counseling, and business transaction assistance for a range of cryptocurrency and distributed ledger systems, services and products. Our clients include industry associations, digital currency exchanges, payment processors, investors, and blockchain innovators, both large and small, who are tackling a wide range of industry dilemmas such as digital identity, logistics, supply chain, and digital rights management.

We counsel our financial services clients regarding a range of regulatory issues, including compliance with the Bank Secrecy Act, FinCEN regulations, and securities and commodities laws and regulations. We help them draft anti-money laundering policies and organize their internal policies and practices for compliance. We have also assisted these clients to respond to inquiries and investigations by federal and state law enforcement and regulatory agencies. Our experienced Investigations and White Collar Defense group regularly defends corporate clients and individuals against criminal and civil allegations of fraud, money laundering, and other misconduct. Our defense practice includes particular experience in defending clients and property against government asset seizures and forfeitures.



Purpose

Distributed ledger technology ("DLT"), including the use of blockchain technology, has been touted as a way to create and validate digital identities that serve many of the same purposes that physical forms of identification (such as a passport or driver's license) do today. This summary describes the development of DLT as a means for creating a **decentralized**, **portable**, **secure**, privacy-respecting, and entirely **user-controlled** online identity system, often referred to as **self-sovereign identity** ("SSI"), and outlines the high-level legal issues and technological challenges that must be addressed ahead of mass adoption.

BACKGROUND AND HISTORY OF DIGITAL IDENTITY

- Today, a person's digital identity is fragmented across the numerous providers of services that rely on all or part of the person's identity to deliver services. For example, while one social network requires new users' to provide email address, birthdates, and passwords to create an account, another collects different information: full names, phone numbers, and passwords. The growing number of personalized services and Internet-connected devices that leverage, collect, or share information about people often require personalized interaction with the services and/or devices through means such as username/password gates and other forms of authentication (such as biometric data-based authentication). For obvious reasons, people often use the same usernames and passwords for many different services and devices, which is inherently insecure. Even though some service providers offer a single-sign on feature that allows users to utilize the same authentication information to log in to multiple services, this method has certain privacy drawbacks that are discussed in more detail below. Even then, for protection of both the user and the service, most services still require creation of a separate account that can be accessed only with a username and password. The process of constantly logging in to services is cumbersome and causes friction in the consumer experience.

- In addition to digital identity fragmentation, users do not have control over their digital identities as their digital identity is always "given to them" by a service provider stored on that service provider's servers, and subject to authentication and/or revocation by that service provider. For example, major social networks allow a person to build a digital identity by allowing that person to use his or her login credentials for their services as a proxy to log in to other services. Yet, if that social media platform deactivates the person's account, he or she not only loses the identity created on that social media platform, he or she loses access to all of the other parties, services, and sites that relied on that identity to establish access to the user.[1] Social media profiles may not yet be synonymous with a person's identity, but as the use of social media platforms becomes more ubiquitous, the potential harm to an individual when his or her social media account is deactivated or suspended can be significant. As an illustration, a letter from more than two dozen international human rights organizations to the United Nations regarding U.S. border agents allegedly demanding access to devices and social media accounts and permitting or denying entry based on the content on those devices and social media accounts alleges that "suspicionless access" to a person's "digital life" by force or coercion is a violation of international human rights law, including the fundamental right to privacy.[2] It is not inconceivable that in future cultural norms, international law, and even national governments/courts may deem involuntary termination of a person's access to his or her social media accounts to be a violation of a fundamental human right.

[1] Andrew Tobin & Drummond Reed, *The Inevitable Rise of Self-Sovereign Identity* 4, Sovrin Foundation (Sept. 29, 2016), https://www.sovrin.org/The%20Inevitable%20Rise%20of%20Self-Sovereign%20Identity.pdf.
[2] Letter from Access Now et al. on U.S. Border Searches to Zeid Ra'ad Al Hussein, High Comm'r for Human Rights et al. (Feb.17, 2017) (on file with author).

- End users of services are not the only ones affected by the challenges posed by the current identity models. Businesses that have a vested interest, business need, or statutory obligation (such as banks, money service businesses, health care providers, etc.) spend significant time and money verifying people's identities (for example, through bank Customer Identification Programs ("CIP") and/or Know Your Customer ("KYC") processes). Unfortunately, existing identity verification systems and processes are inefficient, cumbersome, and often overly invasive to the individual by collecting more information than is necessary. Current CIP and KYC processes also involve the centralization of troves of personal information about people without any meaningful promises that the businesses will (or even can) keep those people's identities secure from tampering or theft. Streamlining identification processes in a digital world would not only reduce and mitigate the effect of these security and privacy concerns, but also help spur innovation in sensitive areas like financial services and health care.

- Verifying and managing identities online is difficult because the Internet operates through protocols that identify technological endpoints (e.g., IP addresses) and not people, organizations, or other legal entities. To identify these legal entities, applications and websites rely on user registrations, typically protected by usernames and passwords, that are sometimes cross-checked against public records databases or biometric data.[3] Aside from being increasingly untenable and insecure (especially given the rising sophistication of hacking methods and value of the personal data they take), the username/password framework does not truly equate to digital identification because a username/password combination does not verify that a user is the person that he or she claims to be. Solving that problem requires the exchange of verifiable digital credentials (called "verifiable claims" in the industry) that are the digital equivalent of the credentials we use to verify identity in the real world today (passports, driver's licenses, birth certificates, school degrees, professional certificates, etc.).

- People have grappled with identity issues since the inception of the Internet, and the concept of online identity has evolved over the years, with the ultimate goal being SSI. In his article, "The Path to Self-Sovereign Identity,"[4] Christopher Allen identifies the following four phases in the evolution of digital identity:

    - PHASE 1—CENTRALIZED: Most online identities are currently centralized, which means that they are controlled by a single entity (like an online service or website owner). This model results in identity data being siloed and fragmented across disparate online services, websites, and applications. Additionally, in the Centralized model of digital identity, a user does not own his or her digital identity, and exercises little control over how his or her digital identity is used or with whom his or her data is shared.

    - PHASE 2—FEDERATED: This model allows a person to use the same credentials to log in to multiple services. However, this model did not resolve the underlying issue that a person's digital identity is still controlled by, and can be revoked by, the service provider that created that person's account, which then can result in a user losing access to other services that rely on the federated identity maintained by that service provider. This can be especially problematic for users as more and more services rely fully on federated identity services.

[3] Tobin & Reed, *supra* note 1, at 4.
[4] Christopher Allen, *The Path to Self-Sovereign Identity*, CoinDesk (Apr. 27, 2016, 5:02 PM), http://www.coindesk.com/path-self-sovereign-identity/.

- PHASE 3—USER-CENTRIC: The idea of a fully portable, user-controlled, secure digital identity is not new. In fact, programmers sought to achieve this vision through methods such as OpenID (2005), OpenID 2.0 (2006), OpenID Connect (2014), OAuth (2010), and FIDO (2013). Unfortunately, these attempts fell short because even though people were not under the control of a service, application, or website provider, their digital identities were still maintained and controlled by the entities that provided the digital identity services.

- PHASE 4—SSI: With SSI, digital identity is progressing from a non-user controlled and centralized model to a fully user-controlled and decentralized[5] model of digital identity. An SSI is intended to fulfill three basic requirements:

  1. Control: People must have control over their identities, including control over who has access to what aspects of their identities. As discussed below, this enables businesses to reduce the amount of personal data they acquire from their users, which reduces their privacy compliance burden and shrinks the size of any vectors of attack that could be exploited to compromise data that they do hold about people.

  2. Security and Integrity: People's digital identities must be protected from unauthorized access, use, disclosure, or modification. Additionally, people must be able to trust that the integrity of their data is maintained throughout its lifecycle. In other words, people must have confidence that their data will remain accurate and not be modified or changed without their authorization.

  3. Portability and Sovereignty: People must be able to use their digital identities to identify themselves without seeking permission from, or being tied to, a service provider and must be able to transfer their digital identities freely.[6] Additionally, their digital identities must be "sovereign"; in other words, their digital identities cannot be taken away from them.

  An SSI can be thought of as a repository of identity data about a person, entity, or thing—often called an "identity container"—where data in that container offers proof of that person's, entity's, or thing's unique identity and can be added there by the identity owner or by others at the identity owner's request.[7] It should be noted that since entities and things (e.g., Internet of things devices) cannot independently verify their identities, their SSIs are ultimately under the control of a person or organization, sometimes referred to as a "guardian." In a world where SSIs and protocols that allow entities to exchange SSIs are widely adopted, businesses, service providers, governments, and other entities will be able to verify and authenticate people, entities, and things through their SSIs rather than having to establish, maintain, or rely upon their own proprietary or federated databases of user identity and authentication information.

[5] As used in this summary, the term "centralized" means that power over a user's digital identity is concentrated in a single entity or a small group of entities, whereas the term "decentralized" means there is no centralized identity provider (i.e., no single entity or small group of entities can control a user's digital identity, as was the case in a centralized, federated, or user-centric identity systems), and the user controls his or her own digital identity.
[6] Tobin & Reed, *supra* note 1, at 6.
[7] *Id.* at 9.

DLT AND SSI

- DLT is generally well-suited to serve as the underlying technology for SSI because it offers a way to create a single source of identity that can be trusted by everyone, that is completely portable, but that no one entity owns or controls. In fact, Drummond Reed, the Chief Trust Officer of Evernym and a Trustee of the Sovrin Foundation, described an SSI powered by DLT as a "lifetime portable digital identity for any person, organization, or thing that does not depend on any centralized authority and can never be taken away."[8]

- DLTs consist of software that runs on a distributed network of computers or "nodes" around the world, where each node maintains an identical copy of an immutable,[9] verifiable, transparent ledger of records.[10] The ledger contains a history of every transaction made through DLT, and all copies of the ledger remain the same through a consensus mechanism operating across all the nodes rather than by utilizing a trusted third party. Transactions made through DLT are generally verified and secured through cryptographic public-private key pairs. The public key is transformed into or associated with an address that the user shares with the public (like an email address) and the private key allows that user (and only that user) to securely update the data held within the ledger entry identified by the public key (or address). Well-known instances of DLT include the Bitcoin blockchain, the Ripple network, Ethereum, and others.[11] Note that there are many variations in DLTs and therefore, this summary may not reflect how all DLTs function.

- Generally, a DLT can be either public or private and permissionless or permissioned. A permissionless DLT is used in this summary to refer to a DLT where anyone may operate a validator node, i.e., a node that participates in the consensus protocol to validate transactions. A permissioned DLT is used in this summary to refer to a DLT where permission from some governing entity is required to operate a validator node.[12] A public DLT is used in this summary to refer to a DLT that is "open to the public" for usage, i.e., anyone can create transactions on the ledger, whereas a private DLT is used in this summary to refer to a DLT where permissions to write entries to the ledger are restricted to a single centralized organization and read permissions can be either public or restricted.[13] The four main governance models for DLT as well as some examples of DLTs that utilize each governance model are summarized in the table below: [14]

[8] Drummond Reed, Chief Trust Officer, Evernym and Trustee, Sovrin Foundation, Self-Sovereign Identity (Apr. 10, 2017).
[9] As used in this summary, the term "immutable" means that the entries in the ledger are permanent and cannot be changed.
[10] Note that there are some DLTs in which data is not shared with all participants and only the participants that have a "need to know" have access to the data, e.g., Corda *See* Richard Gendal Brown, *Introducing R3 Corda: A Distributed Ledger Designed for Financial Services*, Thoughts on the Future of Finance (Apr. 5, 2016), https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/.
[11] Carla L. Reyes, *Conceptualizing Cryptolaw*, 96 Neb. L. Rev. __ (forthcoming 2017).
[12] Angela Walch, The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk, 18 NYU J. Legis. & Pub. Pol'y 837, 840 & n. 15 (2015).
[13] Vitalik Buterin, *On Public and Private Blockchains*, Aug. 7, 2015 https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/.
[14] Drummond Reed, Chief Trust Officer, Evernym and Trustee, Sovrin Foundation, Self-Sovereign Identity (Apr. 10, 2017).

Access	Validation: Permissionless	Validation: Permissioned
Public	Bitcoin Ethereum	Sovrin
Private	Hyperledger Sawtooth* *in permissionless mode	Hyperledger (Fabric, Sawtooth Lake, Iroha) R3 Corda

- One very powerful feature of some types of DLT (e.g., Ethereum) is that they can deploy automated code that can autonomously make updates to the decentralized ledger. These code modules are called "smart contracts." Nick Szabo describes smart contracts as "a set of promises, specified in digital form, including protocols within which the parties perform on these promises."[15] In other words, a smart contract is a computer protocol that can execute "promises" or a set of actions based on preprogrammed rules.[16] Smart contracts are very useful in the SSI context because they can act autonomously, self-execute, and even adapt to changing circumstances through predictive technology and machine-learning algorithms.

- Although the method used by various types of distributed ledgers differ, DLT can enable creation of a rich digital identity by allowing cryptographic linking of "attributes" to an SSI. Attributes (also referred to as "claims") are descriptors about a person, such as his or her name or birthdate. DLT also allows for other entities to verify a person's attributes—this is referred to as an "attestation" or a "verifiable claim." The verifying entity digitally signs the verification which then allows subsequent entities to rely on the claim, to the extent they choose to do so. For example, if a person's name and social security number have been attested by a bank, then a subsequent bank may choose to rely on that attestation without having to independently conduct the same verification.

- The SSI model is less susceptible to attack or failure than the user-centric model both because of the distributed nature of the ledger on which the identities are rooted and the use of public/private key cryptography. Because transactions and the accuracy of the ledger are verified by independent and distributed nodes on the protocol, the DLT structure makes it very hard (if not impossible) for a single entity to make changes to recorded transactions without the nodes on the network becoming aware of the change and rejecting it. And the use of public/private key cryptography means that management of each identity relies on strong public/private key cryptography and not weak, phishable usernames/passwords.

[15] Nick Szabo, *Smart Contracts: Building Blocks for Digital Markets* (1996).
[16] Digital Chamber of Commerce, *Smart Contracts: 12 Use Cases for Business & Beyond* 8 (2016).

COMPANIES OR FOUNDATIONS OFFERING DLT-BASED IDENTITY SOLUTIONS

- SOVRIN: The Sovrin Foundation was founded specifically to create an open public distributed ledger for the purpose of enabling SSI. Any person who has access to the Internet will be able to use a Sovrin-enabled app that talks to the Sovrin ledger to manage his or her SSI. Unlike the Bitcoin protocol (which is a public, permissionless distributed ledger), Sovrin offers a public, permissioned distributed ledger that allows public access to identity owners but allows only trusted institutions to serve as nodes on the network. On the Sovrin network, any identity owner can issue claims about themselves—for example, that they graduated from a certain college. However, for other parties to trust that this claim is true, it needs to be verifiable, i.e., digitally signed by the specific college that issued a transcript to the identity owner. Once the identity owner and the college set up a connection (e.g. put their Sovrin-enabled apps in touch with each other to request a verified transcript), each party receives a decentralized identifier (DID) registered on the Sovrin ledger. Each DID is then assigned to Sovrin software called an "agent" that exchanges any personal data necessary to verify the claim. Agents are run off-ledger (e.g., not on the blockchain) to preserve the security and privacy of the identity owner's data. Only DIDs and hashes or digital signatures of a verifiable claim are recorded onto the blockchain. More information can be found at https://www.sovrin.org/.

- UPORT: uPort is a system built on the Ethereum protocol that allows individuals, devices, entities, or institutions to have an SSI. A uPort identity can digitally sign and verify a claim, action, or transaction and can control cryptocurrencies or other tokenized assets. A uPort identity can also be linked to digital identities that are not on the blockchain (e.g., a social media identity) by using a smart contract to map a person's uPort SSI to that off-chain digital identity. More information can be found at https://www.uport.me/.

- CIVIC: Civic's Secure Identity Platform is built on blockchain technology and uses a verified identity for multi-factor authentication on web and mobile apps, including the use of biometrics, without the need for usernames, passwords, third party authenticators, or physical hardware tokens. Civic uses multiple identity validation service providers to authenticate an individual's identity and to detect and reduce the risk of fraud. Once validated by Civic, a person can use his or her digital identity with Civic partners for identity verification and authentication, and to receive alerts of potential identity theft. Civic's services can be used for many purposes, including by financial services and medical services providers to provide authorized access to financial and medical records and for identity verification, and by e-Commerce platforms to provide seamless integration into their payment portals. More information can be found at https://www.civic.com/secure-identity-platform.

- R3: R3 leads a consortium of over 80 financial institutions and regulators around the world to design and deliver DLT to global financial markets. In 2016, R3 and 10 of its consortium member banks developed a proof-of-concept for a KYC registry that operates on the R3 Corda platform and that is intended to allow identities (of both individuals and entities) to be managed by the identity owners. The identity owners can allow other participants of the Corda platform to access their digital identity for client onboarding and KYC purposes. Participants of the Corda platform can issue attestations of an identity owner's identity attributes. More information can be found at http://www.r3cev.com/.

- MOOTI: Mooti is a cryptographic identification and validation platform that can issue and validate identity claims on multiple public and private blockchains. Mooti's client software for receiving, validating, and sending identity information is available on iOS, Android, and Windows Phone devices, thereby allowing users to provide their identities using their smartphones. Mooti also allows businesses to verify claims about customers, such as their age, and then store cryptographic proofs on the blockchain instead of the actual personal data, thereby reducing the risk of losing the actual identity data to attack, which reduces the potential liability for data breach. More information can be found at http://mootipass.com/.

SSI AND THE LAW

PRIVACY LAWS

- Whenever sensitive or private data such as identity data is being stored or transmitted, compliance with domestic and international data privacy and security laws is always a concern. Developers of SSIs must build their systems with privacy and security in mind from the outset. Most companies or foundations that offer SSI solutions have determined that it is best practice to record only hashes of private data on the blockchain and not store any private data on the blockchain (even encrypted). Instead, all private data is stored off-ledger and is only exchanged "peer-to-peer," e.g., between the entities that need to exchange that personal data (which is often done through the SSI provider's application or via cloud-based agents or smart contracts). This ledger architecture reduces the risk that personal data will be breached because only non-personal data (e.g., DIDs and hashed digital signatures) are stored on-ledger. Of course, the process of storing and transmitting personal data off-ledger presents the same privacy risks inherent in the technology being utilized to store and transmit such off-ledger data, but with respect to the on-ledger data, at least, privacy and security risks are mitigated. As an example, if an identity owner makes a claim about himself or herself (e.g., I am licensed to practice medicine), that claim can be verified by a third-party entity (e.g., the medical licensing authority) if that third-party entity creates a "proof" of that verifiable claim (which can be done by digitally signing the verifiable claim or through a cryptographic hash). Only a cryptographic hash of the doctor's medical certification is recorded on the ledger for verification purposes.

- Zero knowledge proof cryptography further enhances privacy by allowing an identity owner to choose what identity information to reveal about himself or herself (often called "selective disclosure") and prove claims about himself or herself without revealing the underlying personal data.

- As DLT expands beyond the realm of decentralized cryptocurrencies and is adopted by regulated industries, some of its core features, such as its decentralized nature, may cause tension between this new technology and existing privacy laws. One such law is the recently enacted General Data Protection Regulation ("GDPR"), which applies to the processing of personal data by data controllers or data processers located in the EU or of data subjects in the EU.[17] The broad application of the GDPR means that it would apply to DLTs if any data is "processed"[18] on the ledger and is "personal data" (note that the definitions of "processing" and "personal data"[19] in the GDPR are extremely broad). At least two legal questions (and probably many more) must be answered before one can conclude that the GDPR applies and how it applies to a particular DLT: (1) is the data "processed" on the ledger "personal data" as such terms are defined in the GDPR and (2) who is the data controller (i.e., the person or entity who decides the purpose and means of processing the applicable personal data) and who is the data processor (i.e., the person or entity who processes the applicable personal data on behalf of the controller)? The answer to question 1 depends on the architecture of the applicable DLT and whether any personal data (as defined in the GDPR) is actually stored on the ledger, in other words, whether any data that is stored on the ledger is related to an identified or identifiable natural person (note: under the GDPR, to de-identify data such that no data subject is identifiable is a very high

[17] Regulation (EU) 2016/679, art. 3, O.J. (L 119) (hereinafter GDPR).
[18] "Processing" means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" *See* GDPR art. 4.
[19] "Personal data" means any "information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural Person" *See* GDPR, art. 4.

standard).[20] Therefore, even if a DLT stores only identification numbers that could be considered personal data under the GDPR if there is any way to tie that identification number back to a data subject.[21] The answer to question 2 is challenging because the GDPR contemplates that data controllers and processors are centralized entities. If the DLT at hand is a private ledger, a regulator would likely consider the centralized operator of the private DLT to be the data controller or data processor, as applicable, but if the DLT at hand is a public ledger, it is questionable which nodes—if any—would be considered the data processor or data controller given that every node may technically participate in processing the applicable data.[22] In this case, how would a regulator practically apply the GDPR to all nodes on the network, and does the outcome make sense? This summary does not propose to offer solutions to these questions, but conflicts like these between DLT and existing laws will need to be addressed as DLT is more widely adopted.

ANTI-MONEY LAUNDERING LAWS

- Anti-Money Laundering ("AML") laws such as the Bank Secrecy Act and USA PATRIOT Act require banks and other financial institutions to conduct KYC diligence to verify a customer's identity, or to maintain full-scale CIPs. Additionally, the USA PATRIOT Act requires enhanced due diligence for "high risk" customers.[23]

- According to KPMG, the global cost of complying with AML laws and regulations was estimated to be $10 billion in 2014 and is only expected to increase (although this may change with the new U.S. Presidential Administration).[24] Banks have shown great interest in DLT as a way of streamlining financial transactions and reducing the cost and time required to conduct KYC processes. A well-designed and privacy-respecting DLT could theoretically eliminate the siloing of information and duplication of efforts by banks, which would ultimately speed up the process and reduce costs of AML and KYC compliance. DLT could also be used to combat financial fraud and improve efficiencies by making transaction histories, identify verification instances, and compliance activities visible to other institutions (as long as the identity owner permitted such access). David Rutter, CEO of R3, said: "The growing complexity and cost of KYC compliance requirements presents a major challenge for banks on-boarding new clients and is having a negative impact on those client relationships. Distributed ledger technology can provide a unified view of clients whilst also significantly reducing costs and time spent verifying identity."[25]

- Despite the advantages that DLT and SSI may offer to the financial services industry, the question that remains to be answered is whether regulators will permit financial institutions to satisfy their AML and KYC obligations by relying on third-party attestations inherent in most DLT and SSI solutions.

[20] For a data subject not to be identifiable anymore requires that it be "absolutely impossible" to identify the data subject. Matthias Berberich and Malgorazata Steiner, *Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers?*, 2, EDPL, 422, 422-26 (2016)
[21] *Id.*
[22] *Id.*
[23] PricewaterhouseCoopers, *Anti-Money Laundering: Know Your Customer: Quick Reference Guide* 201-02 (Jan. 2014), http://www.pwc.com/gx/en/financial-services/publications/assets/pwc-anti-money-laundering-know-your-customer-quick-reference-guide.pdf.
[24] Teresa Pesce, *Global Anti-Money Laundering Survey 2014*, KPMG (Jan. 28, 2014), https://home.kpmg.com/xx/en/home/insights/2014/01/global-anti-money-laundering-survey.html.
[25] Ian Allison, *R3 develops proof-of-concept for shared KYC service with 10 global banks*, International Business Times (Nov. 10, 2016), http://www.ibtimes.co.uk/r3-develops-proof-concept-shared-kyc-service-10-global-banks-1590908.

BIOMETRICS LAWS

- Biometric data is another way to identify people. One approach has been to collect biometric data such as fingerprints, palm scans, and iris scans directly into a centralized registry to identify citizens, undocumented immigrants and refugees—some of whom may live, work, and travel without any verifiable proof of identity. For example, the Unique Identification Authority of India has scanned the irises of millions of unregistered residents of India.[26] Biometrics work well as identifiers because they are physically tied to a person, and in the case of DNA and other similar physical markers, generally remain the same over a person's lifetime. However, just as usernames and passwords can be stolen, leading to potential breaches of sensitive information, biometric data may be even more prone to misuse. For example, if a person's DNA sequence is revealed, individuals and businesses can match it to existing databases of information to generate a profile for such person and use it for a variety of purposes, including extortion.[27] And unlike passwords, if a person's biometric data is stolen, it cannot be changed. This danger is reduced if the biometric data is collected and stored only on a local device under the control of the identity owner. This latter technique of verifying identity is now mainstream—according to Acuity Market Intelligence, 600 million smartphones with biometric capabilities are now in use, representing 28% of the installed base of smartphones globally.[28]

- However, what if there was a way to leverage existing biometric-based identity authentication protocols while reducing the associated privacy and security concerns through DLT? By hashing biometric data (so that only a representation of the data and not the data itself is stored) and recording such data onto a blockchain, it is theoretically possible to link a person's biometric data to his or her digital identity and protect his or her privacy at the same time.[29] However, it should be noted that there is significant debate in the industry whether storing even hashed biometric data is a good idea because if the raw biometric data used to produce the hash is ever leaked, the existence of that biometric data is forever immutable on a public blockchain, which can pose great privacy risks to the individual concerned.

- Not only can DLT be used to secure biometric data, but biometric data can be used to enhance the security of DLT. Rather than relying on a single private key to permit execution of transactions, multisignature blockchain functions may require multiple keys that each require a different method of authentication. One method of authentication can be biometric data.[30] For example, ConsenSys (the makers of uPort) has developed an application for iOS and Android whereby biometrics stored on the user's device are used to secure access to the private key that allows that user to interact with the Ethereum blockchain.

---

[26] Pooja Bhatia, *Biometric identification that goes beyond fingerprints*, USA Today (Apr. 19, 2014, 10:43 AM), http://www.usatoday.com/story/news/world/2014/04/19/ozy-biometric-identification/7904685/.
[27] Vinay Gupta, Tell Me Who You Are, ConsenSys (Dec. 23, 2015), https://medium.com/@ConsenSys/tell-me-who-you-are-258268bf3180#.30ppgqcc0.
[28] Stephen Mayhew, *Biometrics and online authentication, payments, fingerprint technology and MWC trending this week*, Biometric Update.com (Feb. 21, 2016), http://www.biometricupdate.com/201602/biometrics-and-online-authentication-payments-fingerprint-technology-and-mwc-trending-this-week.
[29] Christian Lundkvist & Andrew Keys, *The Identity Crisis*, ConsenSys (Nov. 25, 2015), https://medium.com/@ConsenSys/identity-is-defined-in-merriam-s-dictionary-as-who-someone-is-a3d6a69f5fa4#.ulo6wro35.
[30] Collin Thompson, *FinTech 2.0: Identity, and Unlocking the Transformative Power of the Blockchain for KYC and AML*, Intrepid Review (Dec. 16, 2015), https://medium.com/the-intrepid-review/fintech-2-0-e17491431103#.3j6kd8aq4.

- However, the convergence of DLT and biometric technology will undoubtedly bring legal challenges. A number of privacy laws in the United States specifically govern biometric data, and other, more broad privacy laws apply to biometric data. In the United States, the privacy laws that govern biometric data generally regulate third-party use and collection of biometric data. For example, the Illinois Biometric Information Privacy Act establishes rules governing businesses' collection and use of biometric data from Illinois residents. However, given that any biometric data that a person records onto a blockchain as part of his or her SSI is entirely self-driven and self-controlled and would likely be hashed, it is unclear whether the existing biometric data laws would apply. Therefore, it may be difficult for plaintiffs to have standing in any lawsuit alleging breach of privacy laws relating to their biometric data on the blockchain.

LAWS GOVERNING ONLINE IDENTITIES AT DEATH

- Only a few states govern how online accounts (like social media profiles) are handled after the owners of those accounts die. The Uniform Law Commission released the Uniform Fiduciary Access to Digital Assets Act ("UFADAA") in 2016 to supplement existing laws regarding probate, guardianship, trusts, and powers of attorney to allow fiduciaries to handle digital assets just as they would handle physical assets after a person's death. Many states are now trying to pass legislation that is substantially similar to the UFADAA. Additionally, service providers have begun to establish policies addressing how to handle the accounts of users that have died.[31] Several large social media companies permit a person authorized to act on a deceased individual's behalf to request deactivation of the applicable account.

- However, since a person's SSI is permanently recorded on a blockchain, how can a person's SSI be deactivated or deleted after he or she passes away? There are several ways that this issue can be addressed. People or institutions could issue attestations that this person is no longer alive or perhaps software can be programmed to deactivate digital identities after a certain period of time. Also, for DLTs that utilize the DID specification, control of the private keys for the digital identity of a dependent (i.e. an entity that cannot control its own private keys, such as a child, an object or a deceased person) can be vested in a guardian (i.e. a separate identity owner that serves as trustee for the dependent). In this way, the guardian (which can be the executor of a deceased person's estate) can control the deceased person's digital identity. In this model, however, it may be prudent to program a deceased person's wishes in some fashion onto the blockchain (e.g., through a smart contract) to prevent misuse of the deceased person's digital identity by the person's guardian. This outline does not explore all possible answers to this question, but the topic deserves attention as DLT continues to mature.

TRUST FRAMEWORKS

- Phil Windley, the Chair of the Sovrin Foundation, characterized SSI as "the Internet for Identity"[32] because SSI is meant to be accessible to everyone, anyone can improve it, and no one owns it. However, like the Internet, a governance structure (sometimes called a "trust framework") needs to be established that sets forth a protocol for SSI that is mutually agreed upon by the relevant stakeholders. A trust framework provides the structure necessary to establish trust in the distributed ledger that is the lynchpin of SSI. To foster widespread adoption of SSI, it is important to involve a diverse group of stakeholders in the creation and development of a trust framework, which may include technologists, lawyers, and the government. Therefore, a trust framework may be viewed as a technological, social, business and legal governance structure for SSI.

---

[31] Victoria Blachly, *Uniform Fiduciary Access to Digital Assets Act: What UFADAA Know*, A.B.A., Probate & Property Magazine Vol. 29 No. 04 (2015), http://www.americanbar.org/publications/probate_property_magazine_2012/2015/july_august_2015/2015_aba_rpte_pp_v29_3_article_blachly_uniform_fiduciary_access_to_digital_assets_act.html.

[32] Phil Windley, *An Internet for Identity*, Phil Windley's Technometria (Aug. 29, 2016), http://www.windley.com/archives/2016/08/an_internet_for_identity.shtml.

PRACTICAL CONSIDERATIONS FOR GOVERNMENTS CONSIDERING USING SSI

- First, it is important to clarify that the name "self-sovereign identity" does not imply that SSI systems are in any way opposed to or in competition with sovereign national electronic identification ("eID") systems such as India's Aadhaar or the EU's eIDAS. To the contrary, SSI architects maintain that SSI systems and governmental eID systems are in fact highly complementary and mutually reinforcing.[33]

- However, using DLT to implement legal processes such as issuing and recording national identifications may involve or demand changes to the law and the legal systems that interpret, create, and implement such legal processes. For example, if states began using a blockchain to record Uniform Commercial Code ("UCC") filings, current substantive law relating to defective filings, failed searches, and lapsed filings would become unnecessary.[34] In her article "Conceptualizing Cryptolaw," Carla Reyes predicts that a completely new type of jurisprudence will develop to govern "crypto-legal structures" or computer code built to implement law.[35] As a result, it may not be possible to predict all the legal challenges and issues that will arise when a government offers its citizens a way to create an SSI using DLT.

- Moreover, as discussed above, the development and deployment of SSIs may require the use of smart contracts programmed into the blockchain software. However, all computer code is susceptible to error, and given the complexity of smart contracts, it is more than likely that we will face many conundrums of erroneous application of law resulting from programming error and lack of foresight by the programmers creating these smart contracts. This will not be solely academic; as smart contracts roll out into the real world, errors, unforeseen consequences, and even intentional wrongs will cause damages and harm that will demand legal remedies.[36] Regarding the UCC, for example, what if a faulty smart contract resulted in a lien against property being released when it should not have been? Who would have standing to sue and who could be sued? Could the harmed party sue the developer of the smart contract, even though it was deployed in a system operated by the government?[37]

The law has not addressed these and many other similar questions, but as the technology advances and becomes standardized, legal practitioners will be forced to grapple with the intersection of DLT and the law to harmonize and rationalize just and equitable results.

---

[33] For example, at the Blockchain Roadmap for Austria conference held May 6-7, 2017 in Vienna, the recommendation of the Identity Working Group was for Austria to directly support the adoption of SSI by its citizens through the issuance of a digital Austrian Self-Sovereign Identity Card (in the form of a verifiable claim from the Austrian government). At the European Identity Conference the following week in Munich, the ability of SSI to enhance the German national ID card and the EU's eIDAS program was discussed in multiple conference sessions.

[34] Reyes, supra note 11.

[35] *Id.*

[36] As a case in point, the DAO which is a "decentralized autonomous organization," had a goal of operating an organization that was completely decentralized and was run by smart contracts. During the initial funding period during which people crowdfunded the DAO by purchasing tokens through an initial coin offering, the DAO raised over $150 million, making it the largest crowdfunding in history. Unfortunately, an attacker exploited certain errors in the smart contract code, stealing more than 3.6 million of ether worth about $50 million. Given the legal uncertainties of how to interpret smart contracts, and who is liable in the event of an attack caused by a faulty smart contract, it is unclear whether the investors in the DAO have any legal remedies against the creators of the DAO or the attacker, and if so, what legal remedies are available to them See David Siegel, *Understanding the DAO Attack*, CoinDesk (June 25, 2016, 16:00 BST), http://www.coindesk.com/understanding-dao-hack-journalists/.

[37] *Id.*