California Blockchain Working Group
Digital Identity
Radhika Iyengar and Jason Albert

March 27, 2020

I. California Context

The State of California is a major provider of identity for individuals. The most prominent identity service that the state provides is drivers licenses and state identity cards. These are used daily by individuals for everything from age verification for alcohol purchases to identity verification for boarding airplanes to filing taxes.

But this isn't the only identity service California provides. California licenses a number of professions, including lawyers, doctors, nurses, engineers, and so on, as more fully documented in the section on Education and Workforce *[insert cross-reference].* While we think of these occupational licenses as permissions to engage in a particular profession, they also are aspects of the identity of the individuals who are licensed.

California is also a significant consumer of digital identity. Whenever an individual interacts with the government, whether applying for a license, obtaining benefits, seeking redress, etc., they need to verify their identity. Currently, that is done through various paper documents, such as birth certificates, drivers licenses, passports, utility bills (to prove residence) and so on.

Digital identity is critical to the modern economy. We already use digital identities in various ways, such as using Facebook to log into a service. However, existing digital identity solutions have limitations. Specifically, many forms of digital identity are vulnerable to hacking and compromise, require trusting third parties with an individual's data, and verification of identity and claims is limited. To quote the famous New Yorker cartoon, "On the Internet nobody knows you're a dog."

As this Techcrunch article notes:

> *Your digital identity is more than your login credentials. This is merely the authentication that connects you with the digital you. Your digital identity consists of thousands of data points that make up a profile of who you are and your preferences. Today, your digital identity is scattered all over the internet, where Facebook owns our social identity, retailers own our shopping patterns, credit agencies hold our creditworthiness, Google knows what we have been curious of since the dawn of the internet and your bank owns your payment history.*

II. How Did We Get Here? (portions of Sections II – XIII adapted from the book *Enterprise Blockchain Has Arrived* by Radhika Iyengar and Jorden Woods, copyright May 2019)

Today it is clear that trust and security are being challenged, and some would contend it is broken, in the online world:

- Every day, armies of cybercriminals break into various businesses and steal valuable records.

- People's online identities and information are routinely accumulated, misappropriated, and mined by trusted intermediaries.
- Billions of dollars in fraudulent online credit card transactions are made annually.
- The world is awash in fake news and disinformation that is falsely portrayed as trustworthy.

How did we get here? To put it simply, we are here because the Internet and the Web lack foundational layers of identity, security and trust. Instead, online identity has been generated by web sites and web/mobile applications that issue username/password credentials to everyone. Trust and security are seemingly generated by large online players that provide services to millions of users.

The foundational layers of the Internet are TCP/IP (the Internet protocol suite), which are a family of network messaging protocols. TCP/IP has created a powerful and low-cost medium for sending and receiving digital messages and information nearly instantaneously from one location or person to another. Building on this foundation applications have enabled the worldwide growth of now ubiquitous online communications like chat, email, photo-sharing, and VoIP. But TCP/IP as a messaging protocol was never conceived to address security, privacy, or identity.

III. Key Elements of Digital Identity

We need a form of digital identity that meets several design criteria. First and foremost, it must be secure. Second, it needs to be reliable and verified. Third, the individual needs to be in control—something often referred to as self-sovereignty. Let's dive into each of these a bit more:

- *Secure.* Security is important to ensure digital identity isn't compromised. The more we rely on digital identity, the more we need to be able to protect it. Fortunately, with cryptographic techniques like private keys we can enable a high degree of security beyond username and password or even two-factor authentication.

- *Reliable and Verified.* Digital identity is valuable only if others are willing to rely on it. Identity isn't part of our persona; rather it exists to be shared to establish some set of rights or obligations or attributes in the real world. So while self-reported facts like those on LinkedIn or Facebook are interesting, increasingly people will want and expect third-party verification of claims.

- *Individual Control.* Control of identity is perhaps the most promising aspect of digital identity. Right now our identity is in the hands of others. The government issues our passport; the state issues our driver's license; our employer verifies our employment; and so on. As noted before, all of these are important as verifiers of aspects of our identity, but they shouldn't be in control of it. Self-sovereign identity solutions based on blockchains can put the individual in control of their identity and how it is shared.

IV. The Role of Blockchain

Blockchain creates a secure source of truth and is the foundation for online trust. Identity in the real world is based on a foundation of trust, but it also fundamentally based on self-determination and is something that is owned by an individual. However, no individual or business today owns its identity or data online.

Ironically, even though the paradigm for today's online world is centralized, from a user perspective identity and data are distributed and fragmented. There is no one master identity for each user and so

there is no identity layer. With no identity layer, there can also be no real trust layer, since any user's identity in the online world can be compromised.

To remedy this problem, digital identity is based on two important concepts, self-sovereign identity (SSI) and decentralized identifiers (DIDs). SSI is the concept that individuals and entities should own and control their identity and data, independent of any central authority. By its nature, SSI is about the individual and so requires a decentralized foundation. DIDs are unique, global identifiers that provide this foundation for individual identity. These might seem to be novel concepts for the online world, but let's compare them with identity in the physical world.

In the physical world, businesses and individuals are the arbiters and protectors of their identity and assets. Consider that we typically carry our identity information around in our physical wallet. Inside this physical wallet are important cards that prove our identity (i.e. a driver's license or photo ID) and provide information about our trusted relationships (i.e. insurance, banks, credit, schools, etc.). If we are asked to prove our identity, we show our identity cards. If we are asked for insurance information or use credit to make a purchase, we present or carry out a transaction with the appropriate card.

Like in the physical world, identity information and confidential data will be stored in a digital wallet. In our digital wallet will be credentials and information tied to our identity and our trusted relationships. Since the wallet is digital, it is much more powerful and can control significantly more information than a physical wallet that we are accustomed to carrying personally.

For example, a digital banking "card' would be issued by a bank and would serve as the credential, along with a biometric, for access to the bank account. These credentials, issued by each entity, but 'owned' by the user, would streamline access and the processing of all transactions. Since the wallet would also be involved in all banking transactions, it would store all transactions on its own blockchain ledger which would be accessible independently of the banking entity.

Unlike the physical world, however, our digital wallet and credentials will be keyed to our DID and protected by public key cryptography. SSI means that only we will have the master keys (private key) and be able to authenticate to gain access to our digital identity and associated data.

V. Collaboration and Standards

Cross-entity collaboration will definitely be needed. The Digital Identity Foundation and the World Wide Web consortium have been working to make sure that digital credentials have standard formatting and are interoperable. There will be a variety of different platforms and individuals need to be able to share and recognize aspects of their identity across them. It is important that the industry—both issuers and consumers of aspects of digital identity—participate in this work. Common standards will accelerate adoption, making digital identity solutions more widely available.

SSI relies on DIDs and decentralized public-key cryptography. A DID is provided to an individual or entity typically by a public utility, and once issued it is owned only by the individual or entity. In addition to being global and universal, it is also portable, private, and persistent; with persistence being guaranteed by the immutable blockchain ledger. DIDs grant a unique private key to the owner, who then has exclusive access to the private key and can generate public keys to give to others to carry out transactions. An individual or entity can have multiple DIDs in order to represent a range of personas, entities and contexts

A universal DID specification is being developed by the Decentralized Identity Foundation (DIF). DIF is an ecosystem of the top blockchain platforms and SSI community globally, and includes the following well-known members: IBM, Microsoft, Hyperledger, ConsenSys, Accenture, Aetna, Mastercard, and SecureKey, among others.

Taken together, the combination of SSI, DID, and blockchain can create an identity layer in the online world. With this identity layer, all members of the online community can be certain that an entity's online identity is really that entity, that all actions and information are recorded accurately, and that each entity has full control over its data. The identity layer therefore creates a trust layer. This is very different from the current online world in which identities can be easily 'spoofed' (one entity masquerading as another), falsified accounts (often bots) disperse false information and fake news, and where identity theft is commonplace.

To be widely adopted, this identity layer must be both highly secure and convenient to use. Since blockchains can create the most secure networks known today, the data will be immutable and well protected. This still leaves an open issue around convenient user authentication for accessing the private key.

VI. Self-Sovereign Identity & Trust

To address this, there has been a rise in the concept of self-sovereign identity. The idea is that one's identity isn't in the hands of a third party—be it Facebook on the Internet or the DMV in the offline world. Rather, information about one's identity is in the individual's hands, for him or her to share as he or she wishes.

Blockchain is a key enabler of self-sovereign identity. Importantly, this isn't because personal data (aspects of identity) are stored on the blockchain. Rather, the value of blockchain, as pointed out in this IBM blog, is that it "provides a transparent, immutable, reliable and auditable way to address the seamless and secure exchange of cryptographic keys." In many digital identity solutions, the key elements stored on the blockchain are the individual's public key, the credential issuer's public key, and revocation information. These allow verifiers of credentials to tell that they are signed by the issuer's private key and the individual's private key—proving that they were validly issued and shared by the person to whom the credential relates. The credential itself is not stored on the blockchain, but somewhere else, such as the individual's mobile device.

Under a system of SSI, each individual or entity controls its online identity and associated data. As a result, access to this information will require the individual's or entity's permission. No other entity can provide this information and no other entity will have rights to store identity information and its affiliated data without explicit permission. Additionally, the individual or entity can place conditions on the permission, for example making it time-limited, restricting reuse, revoking use based on 'breach of terms', attaching fees for use, etc.

In addition to placing restrictions on use or reuse, entities and individuals will also be able to use fine-tuned control on how information is disseminated to third parties. This is also a form of selective disclosure. This capability enables the sharing of only the minimum amount of information required (i.e. verifiable claims) for the transaction. Alternately, selective disclosure can be set to bar specific third parties from any access.

Currently, privacy mechanisms based on cryptography such a zero-knowledge proof (ZKP) is currently used in permissioned platforms to obfuscate the identities of users in a transaction and/or the values and parameters associated with the transaction. Since blockchains typically make all transactions within the network visible and transparent to the members of the network, ZKP enables selective disclosure to only the parties involved in the transaction. All other parties are aware a transaction took place, and they might know selectively a few parameters associated with it, but they will typically not be aware of who was involved, and all values associated with the transaction.

Blockchain has the potential to revolutionize trust, security, and each entity's relationship with its digital identity and online data. In the next few years radically new concepts like SSI and ZKP will further mature and usher in a new era that can positively impact all areas of commerce and society.

VII. What Does this mean for California businesses?

The decentralization of trust and the creation of online identity and trust layers will have significant benefits for California businesses. As users take control of their data, businesses will generally only store the most relevant information to their operations, rather than all user data. This will lead to a downsizing of centralized data stores and most likely a significant decrease in data breaches. This will take place as honeypots, 'single points of failure', and centralized authorities are replaced with decentralized systems and data that are more difficult to penetrate and that provide smaller, lower value targets.

One of the major barriers to system interoperability both internally to a business across as well as externally across businesses, has been the use of different identifiers for the same customer or vendor. The adoption of DIDs will enable businesses to become more internally and externally interoperable since customer data will be tagged with the same set of identifiers globally. This will have major implications in industries such as healthcare, especially in combination with SSI, since patients will now be able to aggregate their own medical records and share them with providers to improve healthcare outcomes.

DIDs will also enable businesses to more easily and readily share information with each other about many other aspects of their businesses such as about customers, suppliers, partners, and products. In each case, it will be possible to create digital passports that will provide historical data that can streamline administrative overhead in areas such as customer authentication, customer and vendor onboarding, supplier vetting, product evaluation, supply chain management, and process tuning. The use of digital twins in combination with AI can add higher levels of sophistication enabling process optimization and process automation across companies.

VIII. How Does Self-Sovereign Identify Enhance Consumer Privacy

One key benefit of self-sovereign identity is enhanced privacy. Currently, lots of aspects of our identities are tied to our Social Security Numbers. So if you learn some things about me, it might be possible to tie others and build a profile. Even something like Facebook allows a complete picture of what I am interested in across the web. Putting individuals in control of their identity and allowing them to determine what to share, and with whom, can help make this a reality.

Importantly, self-sovereign identity doesn't mean unverified identity. While the individual is in control of his or her identity elements, those can be verified by the employer, the DMV, etc. And the individual benefits from verification, because it will lead to broader acceptance of the particular identity aspect that is being shared for a given purpose (e.g., age to get into a bar, salary for a bank loan).

Individuals will embrace digital identity when they see the benefits it brings to them. One simple example is a credential that proves I'm over 21 (not that anyone would question that) when I go to a bar, without having to turn over a driver's license with my full name, birthdate, height and weight, etc. Another example is applying for a loan, where my employer could issue a credential saying I earn over a certain amount without disclosing my exact compensation—and do it in a seamless, paperless way that reduces friction and lowers cost. Or as a recovering attorney, I'd welcome being able to share my licensure information securely and instantly without waiting sometimes weeks for proof.

IX. Enterprise Case Studies

There are already a number of high profile deployed blockchain solutions that employ digital identity, DIDs, and in some cases SSI, to generate a tangible ROI and improved convenience through increased efficiency and new business models. The more prominent cases are summarized below.

- *CULedger* is a blockchain consortium that introduced its CU Pay application. CULedger has multiple blockchain initiatives and two others are identity-focused. The first to launch (February 2018) was developed with Evernym and is called MyCUID which is a true digital DID provided by the Sovrin Identity Network. With MyCUID credit union customers can authenticate securely from their mobile devices, authenticating with a biometric, and protect themselves from financial fraud and identity theft. MyCUID also employs SSI, so customers can use selective disclosure to control specifically which data is shared in each context.

  CULedger began another identity focused project with IBM in March 2019. This initiative leverages the Sovrin network and Hyperledger Fabric and will initially enable credit union customers to securely share their data across multiple credit unions and carry out transactions at any credit union in the CULedger network. As with MyCUID, customers will be in control of their data and so it will offer self-sovereign identity. The initiative will improve Know Your Customer (KYC) compliance, identity authentication, and will enable credit unions to collaborate in offering new services. Both CULedger identity initiatives have aims to increase the ease of access to credit union services and are thematically about financial inclusion. As CULedger is also working across multiple platforms, all initiatives are part of a network of networks strategy, in which they are helping to drive interoperability across the major platforms in the ecosystem.

- *Verified.me* is a blockchain-based digital identity network developed by SecureKey in partnership with a set of large Canadian banks plus Canadian and US government offices. It was built with the IBM Blockchain Platform on Hyperledger Fabric. On setup the system provides individuals with a digital identity that is stored as a private key on the user's mobile device. The user then connects to the network and can authorize that personal information stored with one provider be shared securely and privately with another. For example, that bank account information is shared with an insurance company or lender, or credit score information is shared with the user or another verified member of the network. The platform launched in May 2019 and is supported by 7 banks: Bank of Montreal (BMO), CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank and TD. Initial service providers include Sun Life for insurance, Notarius for document and signature authenticity, and Equifax for credit scores.

- *Trust Your Supplier (TYS)* is a blockchain consortium that introduced a solution for streamlining the onboarding process for suppliers in a supply chain plus providing buyers with trusted decentralized knowledge about the suppliers. The platform operates by creating a unique digital identity for each

supplier, which underpins a digital passport that stores an immutable history of interaction between the supplier and members of the network. Since the digital identity and passport create a single identifier, there is no need for suppliers to enter their data multiple times, and buyers have a trusted, decentralized source of information for evaluating suppliers. IBM Blockchain developed the platform on Hyperledger Fabric with Chainyard and is using it to onboard thousands of its suppliers. IBM has projected that by onboarding its suppliers with TYS it expects a 70-80% reduction in process time and 50% reduction in administrative costs. Founding members include Anheuser-Busch InBev, Cisco, Dun & Bradstreet, Ecovadis, GlaxoSmithKline (GSK), IBM, Lenovo, Nokia, RapidRatings, Schneider Electric, Flex and Vodafone. The network was launched in Q4 2019.

- *ID2020 Alliance.* A number of companies have banded together to form the ID2020 Alliance, which is designed to enable digital identity that provides political, economic, and social opportunity. The focus has been on creating a digital ID that is private, portable, persistent, and personal. Essentially, that means the digital ID is under the control of the individual, accessible anywhere, stays with them for their lifetime, and is unique to them. The effort is designed in fulfillment of the United Nation's 2030 Sustainable Development Goals, including the commitment to "provide legal identity for all, including birth registration" by 2030. The goal is to break down silos of information, particularly for refugees and low-income individuals, and its early pilot projects have focused on these populations.

- *Workday Credentials.* At Workday, we are working on aspects of this through Workday Credentials and the WayTo app. With Workday Credentials, individuals are empowered to accept various credentials offered by their employer, training programs, or others. Once they have these credentials, they own them: the credentials live on their phone in the WayTo app. They can then share them with others as they wish and do so granularly—credential by credential. There is strong security around verification via a blockchain backbone: recipients can have confidence that the issuer in fact issued the credential, the individual who shared it is the person in question, and that the credential hasn't been revoked. This concept fits with the WayTo app, which will collect credentials accepted by an individual and store them on the person's mobile device (with the option of encrypted cloud backup) and with fine-grained control over what is shared and with whom, enabling self-sovereign control.

X. Identity Management

Proving one's identity is a daily activity, but one that most people don't think about too deeply. For example, online, most sites require some type of login enabling each user to access their account. The username and password are credentials that are supposed to prove the identity and right of the user to the account assets, services and information. Access to a device that can provide online access, such as a phone, PC, or tablet, usually requires some type of passcode, password or biometric identity for access as well.

In all these cases, the foundation of *online* interactions begins with the authentication of digital identity. The basis of most fraud is improper authentication of digital identity. Real world examples of proof of identity moments can include:

- Passing through customs at borders.
- Passing through security at an airport.

- Cashing a check.
- Opening a bank account.
- Purchasing a product on credit.
- Opening a brokerage account.
- Retrieving a car from a valet.
- Picking up mail from the post office.
- Entering a government or corporate facility.

In the cases listed, identity in-person is usually validated via government documents (i.e. driver license, passport). Most financial institutions are government regulated and require strict adherence to Know Your Customer (KYC) and anti-money laundering (AML) checks. As a result, banks and financial services companies require government-issued documents that attest to your identity.

Legal documents often require notarization of signatures attesting to the identity of the signer within a country. The notary often records the number of a government document (i.e. driver license, passport), photocopies the document, requests a signature, and takes a thumbprint to validate identity. Other instruments such as apostille, or Secretary of State authentication, are generally required to prove the authenticity of signatures for legal documents that cross borders.

The basic documents used to attest to your identity (driver license, passport) are in turn based on a person's official birth certificate. In the US birth certificates are issued by State-based Vital Records departments. In other countries, birth certificates are generally issued by individual cities (Europe) or districts.

XI. Challenges

The challenge with most government documents is that they can be easily falsified and there are few tests that can be done to differentiate real documents from fake ones. For example, many high school students in the US have fake driver licenses that show an older age so they can drink alcohol. At the same time, some older children obtain fake birth certificates so that they can play with younger players in competitive sports leagues. We've also seen many spy movies where individuals can have many passports fraudulently attesting to their nationality, name, address, and age.

In many countries it is not uncommon that corrupt government officials will modify government documents, for a fee, for various reasons. This could be to help make a person older or younger — to enable entering a school, getting married, avoiding military service, etc. So even if it might be difficult to modify a document, it is possible to pay or bribe an official to modify a document so that the legal version has incorrect information.

A serious global challenge is there are about 150 million homeless people (550,000 in the US), who may have lost their identity documents. Due to these circumstances, they are not eligible for government assistance, employment, or standard services, which creates hardship and societal imbalance.

XII. Blockchain Opportunity

Blockchain technology provides three special capabilities that enable it to provide a better foundation for identity than current systems. First, all data is recorded on the ledger via a consensus mechanism which enlists multiple parties to verify that the data is correct before it is written. Second, all transactions in the

ledger are immutable and digitally signed, which means the records are unchangeable and those who wrote the records are accountable for any issues. Third, the digital, immutable record can be linked to a biometric or set of biometrics (i.e. thumb print, facial scan, etc.) which means that it is unique, easily verifiable, and nearly indestructible.

Blockchain has the potential to solve the challenges section above — fake documents, corrupt officials, and destroyed records, as described below:

- **Fake documents** — identity would be verified via a biometric scan which would access official records found in a blockchain ledger which virtually eliminates the need for documents.
- **Corrupt officials** — the data about one's birth is immutable and cannot be modified once made so corrupt officials become powerless to make changes.
- **Destroyed records** — as the data is digital and stored in decentralized storage it can be considered virtually indestructible.

In the US, to help people and cities deal with the challenges of homelessness, the cities of Austin, Texas and Bronx, New York are turning to blockchain identity solutions. These solutions provide a unified digital identity, which enables individuals to access services such as food pantries, shelters, and banking more easily. It also enables cities to reduce administrative costs, provide better services (such as distributing mobile phones with apps), keep track of service usage, and minimize fraud.

XIII. Conclusion

Clearly there is a need to address the challenges we currently face in digital identity as current systems are not effective at solving the fundamental issues of broken trust, security and privacy. Today, there are technology solutions to help us address the digital identity challenges, and data sovereignty as a foundation provides the path forward.

A leading provider of self-sovereign identity (SSI) in the blockchain world is the Sovrin Foundation. The value of SSI cannot be overstated, and Heather C. Dahl, Former CEO of Sovrin Foundation, has these words of wisdom:

> "The Internet has reached a point where its limitations threaten its function, where the benefits it has brought have come with an increasingly stiff bill—loss of control of our data, and with it, our privacy and our security. Knowing these problems will only get worse, we need an evolutionary leap forward. That leap is taking control of our identity, and self-sovereign identity is the technology that will enable us to do just that.
>
> The critical thing is that everyone gains from self-sovereign identity. What's good for consumers is also good for businesses because when the consumer takes control of their data, they defuse the regulatory and security risks for business. It's a level playing field where people get to choose what they want to share and with whom.
>
> Trust and respect: these are our values and goals. Our digital selves need to be treated with dignity. When that happens, we all win."

[Note: Recommendations, likely related to pilot projects, for how to promote blockchain-based digital identity solutions to come.]