IV. Considerations for Appropriate Application

A Framework for Assessing the Fitness of Blockchain Technology

Introduction

The framework contained in this document is intended to support analysis by the State of California of whether blockchain technology might be a useful tool to help solve an identified problem in the public or private sector. A rudimentary knowledge of blockchain is assumed; however, the framework is intended for use by policymakers, business professionals and the general public, not technical experts.[1]

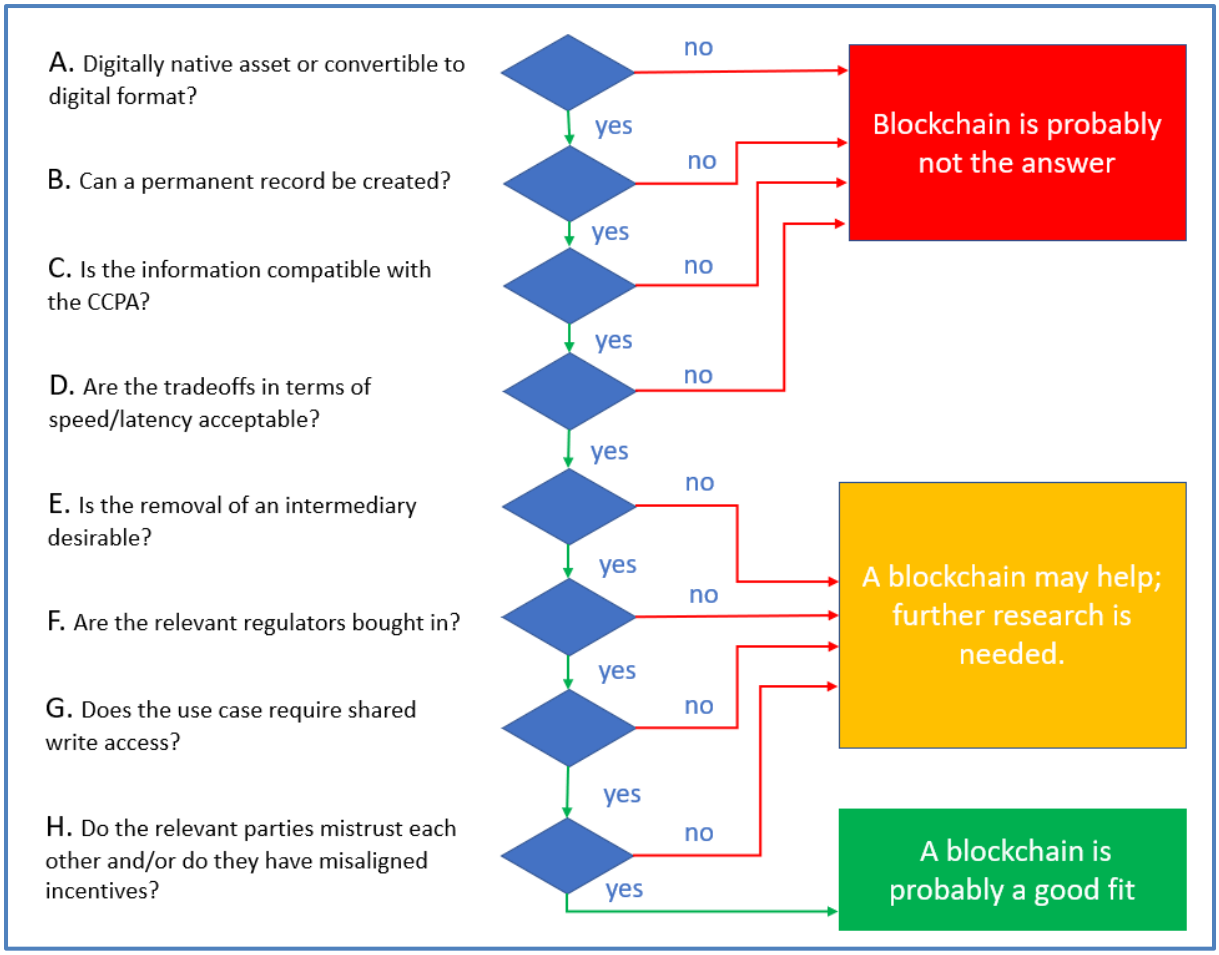
Blockchain adoption is primarily a business decision rather than a technical one. Appropriate use cases must solve real problems for organizations. Blockchain implementation can be a precursor to, and in some cases require, revising associated business processes. Thus, its potential should be analyzed holistically rather than strictly through a technical lens.

Decision Tree Approach

The tool illustrated below is intended to help decision-makers make a preliminary analysis of whether blockchain is an appropriate solution for a defined problem, not to provide a final authoritative answer. By shifting focus to the problem and away from a particular solution, the tool will encourage a practical approach while reducing the risk of ill-advised experimentation.

The decision tree is composed of questions that assist in defining whether a blockchain is the correct approach for a particular problem.

[1] This framework was articulated in the whitepaper Blockchain Beyond the Hype: A Practical Framework for Business Leaders, published by the World Economic Forum in April 2018, by Catherine Mulligan, Jennifer Zhu Scott, Sheila Warren, JP Rangaswami.



A. **Digitally native assets or convertible to digital format?** For blockchain to be successfully applied, it needs to be working with "digitally native" assets, meaning assets that can be successfully represented in a digital format. While this may sound complex, it is actually relatively straightforward; if an asset has a physical representation that can change form, then it is difficult to effectively manage that asset on a blockchain. An example of this is tracking and tracing food on the blockchain – if a company wishes to track and trace wheat across the entire supply chain as it becomes bread, then it is difficult to use blockchain to manage its transition from wheat, to flour, to bread.

B. **Can a permanent record be created?** This is perhaps the most critical question that must be answered, since a blockchain needs to be the source of trust. If there are multiple sources of trust regarding the state of an object, then the object cannot be effectively stored on the blockchain. In those instances where a permanent record can be created, it is important that all parties with responsibility for the state of the digital asset in question agree how its state will be handled or managed in the new business process *prior* to any development. If an unalterable record is superfluous or counterproductive, for example, in a situation where the need to delete information is critical, then blockchain or distributed ledger technology (DLT) is

not an appropriate solution. For example, it would not make sense to store an ordinary grocery list on a blockchain.

C. **Is the information compatible with the California Consumer Privacy Act (CCPA)?** Is any private information or data stored that may be in conflict with local and global data protection regulations, including most importantly the CCPA? These should not be stored on the blockchain.

D. **Are the tradeoffs in terms of speed/latency acceptable?** It is appropriate to assess the speed required *for the business process* in question. Blockchains can increasingly handle fast processing times, but tradeoffs in terms of energy consumption and other factors may not be advisable.

E. **Is the removal of an intermediary desirable?** For a blockchain to be an appropriate solution, it is important to understand the context – does the problem require the removal of an intermediary? For example, would it be cheaper to collaborate directly rather than use a broker?

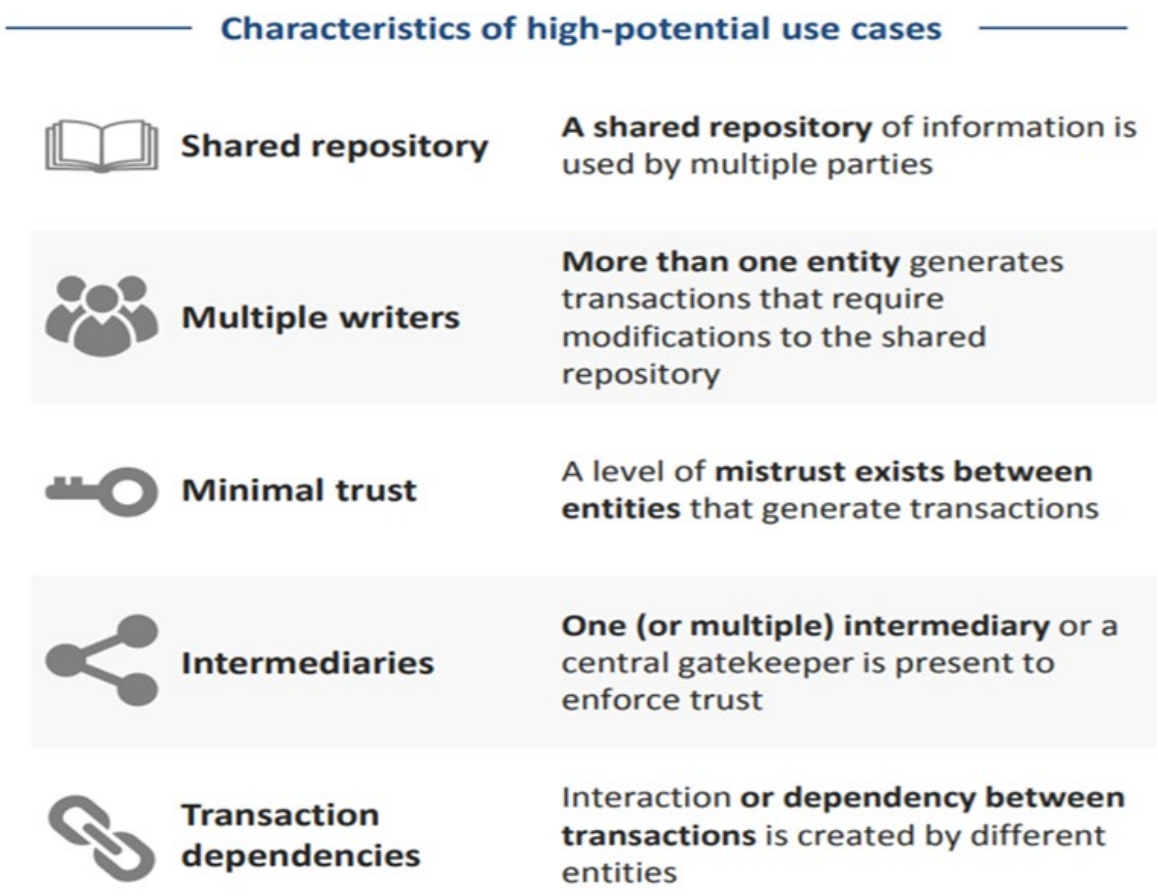
F. **Are the relevant regulators bought in?** Engagement by relevant regulatory bodies may be a limiting factor. In use cases where state regulation plays a role, it may be necessary to include regulators in the project and provide means by which regulators can ensure compliance. This engagement will be critical for many use cases and may throw up administrative or other roadblocks.

G. **Does the use case require shared write access?** In other words, do some or all of the members of the network in question need to be able to write transactions to the blockchain? If the use case does not require such shared write access, then another technology may provide a better solution.

H. **What is the current level of trust?** If the actors or entities already know and trust one another, blockchain is probably not needed. If they do not know or trust one another and/or have misaligned interests, there may be a good reason to use blockchain.

I. **How is blockchain functionality determined?** If the ability to change the functionality on a blockchain (e.g., node distribution, permissioning, engagement rules, etc.) without having a detailed discussion across the large open source forums for blockchain is desirable, then a PRIVATE, PERMISSIONED blockchain is a better alternative.

J. **How is privacy maintained?** If transactions need to be kept private, then a PRIVATE, PERMISSIONED blockchain is appropriate. If NOT, then a PUBLIC, PERMISSIONLESS blockchain may be used.



IV.B. ETHICAL CONSIDERATIONS

Key recommendations:

- Consider how best to educate Californians about blockchain, to ensure a base-level understanding as the technology is introduced in the public and private sector.
- Encourage environmental sustainability as use cases are being developed by offering incentives to blockchain companies. For example, tax incentives and penalties could serve as motivators to promote sustainability goals. California could also prioritize sustainable practices in evaluating vendors for government contracts related to blockchain technology.

MAKING THE CASE FOR BLOCKCHAIN ETHICAL FRAMEWORK

Special considerations must be addressed to ensure that blockchain technology serves as a force for good in California while protecting our communities, our most vulnerable citizens, and the environment from unintended consequences related to this technology. The ethical framework described below provides guidance for collective decision-making while recognizing that there are risks associated with imposing a set of top-down rules on blockchain technologists in California as

designers and developers may choose to leave the state in order to avoid such rules. A key principle to ethical guidance should be promoting a "culture of genuine responsibility" rather a "culture of compliance." [5]

THREE PILLARS OF ETHICAL CONSIDERATIONS

Blockchain technology may touch various aspects of the everyday lives of Californians. As with other new technologies, the potential positive and negative effects of blockchain technology remain unclear. Three specific ethical issues related to the potential social impact of blockchain are equity, accessibility, and sustainability.

Equity

More Californians will ultimately be users of this technology rather than its designers or developers. It is therefore incumbent upon its creators to consider whether their designs are inclusive and advance the goal of equity among all California residents.

A debate is already underway about improving the user experience for blockchain applications, and companies are working toward that goal. However, for the purpose of California legislators, the goal of equity encompasses more than just a user experience.

Blockchain designers and developers should consider questions such as: how will this technology affect low-income populations, such as the unbanked? Will disabled or senior Californians be offered an equal opportunity to use this technology, particularly when it comes to civic rights? Does this technology close or increase the gaps between rural and urban populations? Does this technology uniformly protect the privacy rights of all Californians?

Identifying equity as a stated goal of blockchain legislation would be an important step toward cultivating an inclusive approach to this technology.

Accessibility

Developer diversity. In considering blockchain technology's accessibility, it is important to consider who is developing the technology. How are diverse perspectives (such as gender, racial, and ethnic identities, and sexual orientation) incorporated during development phases of blockchain application? This issue has been researched more generally as it relates to the need for a more diverse workforce in the tech industry. [8] Many of the factors identified as responsible for the imbalances in the general tech industry also apply to blockchain technology. Blockchain technology, however, is not yet dominated by few large companies and is currently a remarkably open field which provides a greater opportunity for diverse representation.

Currently a blockchain entrepreneur does not need an advanced degree in computer science to start a blockchain company. One way the legislature could maintain accessibility in this industry is through careful consideration of any certificate requirements. The legislature should balance the need to protect members of the public from potential malicious actors with potential inequities related to imposing certificate requirements which generally favor the wealthy and educated.

Trust and basic understanding of blockchain technology. A second accessibility consideration involves the high learning curve required to understand this technology. Since blockchain has the potential to affect many different areas of the lives of Californians, we must ensure that the blockchain industry represents a variety of perspectives and technical expertise. How can the State ensure that people are properly informed about the technology as its implementation begins to affect important areas of their daily lives? It will be difficult to secure buy-in for the various blockchain areas identified in this report if the average Californian does not have a basic understanding of the technology itself.

Sustainability

Blockchain use cases have the potential to either further the goal of sustainability or diminish it. On a supply chain, enterprise blockchains could enable ordinary consumers to identify the origins of any retail item. This would allow a purchaser in a California store to know where, when, and under what conditions a particular item was produced, promoting corporate social responsibility. [10]

IMPLEMENTERS OF ETHICAL CONSIDERATIONS

Developers. Blockchain developers should consider the ethical principles, while making any ethical concerns or issues accessible to everyday consumers. Consumers should not "stick their heads in the sand" and use technology mindlessly without consideration of its consequences.

Legislators. Legislators bear the responsibility of ensuring this balance in a particular jurisdiction. For example, legislators can incentivize the ethical use of technology on the part of designers. Legislators can also lead the discussion around new technologies, identifying concerns early and fostering a culture of ethical innovation.

Law enforcement. Law enforcement serves as the backstop, as we have seen with the SEC's recent enforcement of securities laws against companies issuing digital asset tokens.[6] Law enforcement can act reactively, such as identifying violators of the law and imposing consequences. Law enforcement can also act proactively, by announcing increased enforcement of specific laws and thereby sending a message to potential violators.

ETHICAL FRAMEWORK FOR THE ADOPTION OF BLOCKCHAIN TECHNOLOGY

The concept of ethics "requires us to consider the broader impact of our activities."[14] When assessing the ethical implications of blockchain technology, California should abide by the following three principles:

1. Address key ethical design goals

a. Seek societal benefit: maximize good and minimize bad
b. Equity: does this benefit all Californians, or only a few?
c. Expediency: how can we achieve ethical design and use cases without slowing innovation?

2. Consider ethical uses of blockchain technology

a. Accessibility: Design to include the most vulnerable user
b. Responsibility: Anticipate and design for all possible uses
c. Sustainability: Create technology to advance sustainability, public health, and corporate social responsibility

3. Minimize unintended consequences

a. Are there unintended biases or conflicts in the design or use of this technology?
b. Are any populations being unintentionally harmed by the way this technology is developing?
c. Does this technology promote violations of local, national, or international law?

California is the first state in the nation to consider ethical issues at this early state of blockchain technology regulation. Our state aims to strike a balance between innovative technology and its potential effects. With an ethical framework in place as regulation moves forward, California will serve as a model for the development of ethical blockchain technology.

ENDNOTES

[1] Michele Benedetto Neitz, *The Influencers: Facebook's Libra, Public Blockchains, and the Ethical Considerations of Centralization*, 21 N.C.J.L & Tech 1 (2019).

[2] See, e.g., Silk Road Seller Pleads Guilty to Money Laundering, Tracing Illegal Activity Though the Blockchain to Combat Cryptocurrency-Related Crimes.

[3] Beard, M. and Longstaff, S.A., *Ethical Principles for Technology*, 9 The Ethics Centre, Sydney (2018).

[4] World Economic Forum White Paper, AI Governance: A Holistic Approach to Implementing Ethics Into AI 9 (2019).

[5] Beard, M. and Longstaff, S.A., *Ethical Principles for Technology*, 11 The Ethics Centre, Sydney (2018).

[6] *See, e.g.,* SEC Charges Issuer With Conducting $100 Million Unregistered ICO

[7] The European Commission's Group on Ethics in Science and New Technologies created a list of ethical concerns, including some not discussed herein (such as human dignity, autonomy, and democracy). *See* World Economic Forum White Paper, AI Governance: A Holistic Approach to Implementing Ethics Into AI 11 (2019).

[8] Gregory Mone, Bias in Technology (discussing the lack of diversity in the tech workforce).

[9] Congress enacted the CAN-SPAM Act in 2003, a law that "sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have [commercial users] stop emailing them, and spells out tough penalties for violations." Federal Trade Commission, CAN-Spam Act: A Compliance Guide for Business.

[10] See Rick LeBlanc, How Blockchain Will Transform Supply Chain Sustainability.

[11] Jorden Woods and Radhika Iyengar-Emens, Enterprise Blockchain Has Arrived: Real Deployments. Real Value (2019).

[12] Id.

[13] For further discussion, *see* George Nicholson, Blockchain Will Reshape the Future of Sustainability.

[14] Beard, M. and Longstaff, S.A, *Ethical Principles for Technology* 35, The Ethics Centre, Sydney (2018).

[15] Id. at 25.

IV.C. Considerations for Appropriate Application

Digital Identity

Key Recommendations

- Current technology solutions are available to address digital identity challenges and data sovereignty.
- Recommendations, likely related to pilot projects, for how to promote blockchain-based digital identity solutions to come.

Introduction - California Context

The State of California is a major provider of identity verification for individuals. The most prominent identity service that the state provides is driver's 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.

California also licenses a number of professions, including lawyers, doctors, nurses, engineers, and the like, 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 must 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, and require trusted third parties with an individual's data; the ability to verify 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.

KEY ELEMENTS OF DIGITAL IDENTITY

An effective, trustworthy digital identity must meet several design criteria. First and foremost, it must be secure. Second, it must be reliable and verified. Third, the individual whose identity it represents must be in control—often referred to as self-sovereignty.

- ***Secure.*** Security is important to ensure that one's digital identity is not compromised. The more we rely on digital identity, the more we need to be able to protect it. Cryptographic techniques like private keys 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 is not an inherent part of our persona; rather it exists to be shared to establish a set of rights, obligations or attributes in the real world. So while self-reported facts like those on social media profiles are useful in their way, 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. As noted before, all of these are important as verifiers of aspects of our identity, but they should not control it. Self-sovereign identity solutions based on blockchains can put individuals in control of their identity and how it is shared.

THE ROLE OF BLOCKCHAIN

No single master identity exists for each online entity. Without such an identity layer, trust can falter, since any user's identity in the online world can be compromised. To remedy this problem, digital identity is based on two 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 requires a decentralized foundation. DIDs are unique, global identifiers that provide this foundation for individual identity. These may seem like novel concepts for the online world, but they have parallels 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 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 carry on our person.

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.

Collaboration and Standards

Cross-entity collaboration will be needed. The Digital Identity Foundation and the World Wide Web consortium have been working to ensure that digital credentials have standard formatting and are interoperable. A variety of platforms and individuals will 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 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 key and can generate public keys to give 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 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 true, that all actions and information are recorded accurately, and that each entity has full control over its data. The identity layer thus 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 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 regarding convenient user authentication for accessing the private key.

SELF-SOVEREIGN IDENTITY & TRUST

To address the issue of trust, the concept of self-sovereign identity has gained ground. The idea is that responsibility for an individual's identity rests in their hands rather than with a third party, whether an online social media company or a government office offline.

Blockchain is a key enabler of self-sovereign identity, but not because personal data (aspects of identity) are stored on the blockchain. Rather, the value of blockchain, as pointed out in an 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 be assured that they are signed by the issuer's private key and the individual's private key—proving they were validly issued and shared by the person to whom the credential relates. The credential itself is not stored on the blockchain but elsewhere, 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 its use based on "breach of terms," attaching fees for use, etc.

In addition to placing restrictions on use or reuse, entities and individuals will be able to fine-tune control over how information is disseminated to third parties. This is also a form of selective disclosure. This capability enables entities to share only the minimum amount of information required (i.e., verifiable claims) for the transaction. Alternatively, 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) are 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.

In the next few years new concepts like SSI and ZKP will further mature and usher in practices that can positively affect areas of commerce and society.

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 gradually store only the information most relevant to their operations. Centralized data stores will be reduced, leading to a likely decrease in significant data breaches. This will take place as honeypots, "single points of failure," and centralized authorities are replaced with decentralized systems and data systems that are more difficult to penetrate and provide smaller, lower value targets.

One of the major barriers to system interoperability, both internally within an enterprise 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 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 aspects of their businesses such as customers, suppliers, partners, and products. In each case, it will be possible to create digital passports to 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.

How Does Self-Sovereign Identity Enhance Consumer Privacy?

A key benefit of self-sovereign identity is enhanced privacy. Currently, many aspects of our identities are tied to our Social Security Numbers. This piece of information may be tied to others to build a profile. Social media companies also allow a complete picture of individual interests to be drawn across the web. Putting individuals in control of their identity and allowing them to determine what to share, and with whom, can help make greater control a reality.

Self-sovereign identity does not 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. The individual benefits from verification, because it will lead to broader acceptance of the particular identity aspect being shared for a given purpose (e.g., age to purchase alcohol, salary for a bank loan). For example, a credential could prove an individual's age to gain admission to a bar, without having to turn over a driver's license with full name, birthdate, height and weight, and the like.

Another example is applying for a loan, where an employer could issue a credential confirming the employee earns more than a given amount without disclosing the exact compensation—and do it in a seamless, paperless way that reduces friction and lowers cost. Or licensure information could be shared securely and instantly without waiting sometimes weeks for proof.

PILOT AND RELATED CASE STUDIES

A number of high-profile blockchain solutions have been piloted that employ digital identity, DIDs, and in some cases SSI, to generate a tangible return on investment and improved convenience through increased efficiency and new business models. Several examples are summarized below.

CULedger. CULedger is a blockchain consortium with multiple initiatives including CU Pay and two other identity-focused applications. The first to launch, in February 2018, MyCUID is a true digital DID developed with Evernym, provided by the Sovrin Identity Network. With MyCUID credit union customers can authenticate securely from their mobile devices 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, it will offer a self-sovereign identity in order for customers to control their data. The initiative will improve compliance with Know Your Customer (KYC) and identity authentication, and will enable credit unions to collaborate in offering new services. Both CULedger identity initiatives aim to increase the ease of access to credit union services and enhance 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. Verified.me is a blockchain-based digital identity network developed by SecureKey, in partnership with a set of large Canadian banks plus Canadian and U.S. government offices. It was built with the IBM Blockchain Platform on Hyperledger Fabric. The system provides individuals with a digital identity 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, bank account information could be shared with an insurance company or lender, or credit score information could be shared with the user or another verified member of the network. The platform launched in May 2019 and is supported by seven 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 launched in late 2019 that introduced a solution for streamlining the onboarding process for suppliers in a supply chain and provides 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, suppliers need not 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.

ID2020 Alliance. A number of companies have banded together to form the ID2020 Alliance, 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. Workday has established 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 as they wish and do so granularly,

credential by credential. Verification is secured 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 has not 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.

IDENTITY MANAGEMENT

Proving one's identity is a daily activity. For example, many online applications require a login enabling each user to access their account. The username and password are intended to prove the identity and right of the user to the account assets, services and information. Access to the device itself, such as a phone, PC, or tablet, may also require some type of passcode, password or biometric identity.

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

- Passing through customs at international borders
- Passing through security at an airport
- Cashing a check
- Opening a bank account
- Purchasing a product on credit
- Opening a brokerage account
- 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 one's identity.

Legal documents often require notarization of signatures attesting to the identity of the signer. The notary records the number of a government document, 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 identity are based on a person's official birth certificate. In the U.S. birth certificates are issued by State-based Vital Records departments. In other countries, birth certificates are generally issued by individual cities (Europe) or districts.

Blockchain Challenges

The challenge with most government documents is that they can be easily falsified and few tests can reliably differentiate real documents from fake ones. For example, many high school students in the U.S. have fake driver's licenses that show an older age so they can drink alcohol. At the same time, some older children obtain fake birth certificates so they can play with younger players in competitive sports leagues. Nefarious actors could also hold many passports fraudulently attesting to their nationality, name, address, and age.

In some countries, corrupt government officials will modify government documents for a fee. This could be to make a person older or younger, to enable entering a school, getting married, avoiding military service, or other age-limited activities. So although it might be difficult to modify a physical document, it is possible to pay or bribe an official to falsify a document so that the legal version has incorrect information.

Another serious global challenge is with vulnerable populations such as the homeless, about 150 million homeless people worldwide and 550,000 in the U.S., many of whom may have lost their identity documents. Without an official ID, they are ineligible for government assistance, employment, or public services like healthcare.

Blockchain Opportunities

Blockchain technology provides three 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 lost or stolen records, as described below:

- **Fake documents** — identity would be verified via a biometric scan to access official records found in a blockchain ledger, thus virtually eliminating the need for documents
- **Corruptible officials** — vital records data is immutable and cannot be modified once made so officials become powerless to make changes
- **Lost or stolen records** — because the data is digital and stored in a decentralized ledger, 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.

A leading provider of self-sovereign identity (SSI) in the blockchain world is the Sovrin Foundation. Former CEO Heather C. Dahl notes:

> 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.

CYBERSECURITY & RISK MANAGEMENT

Key Recommendations

Rec 1 – Evaluate blockchain appropriateness based on the specific use

Rec 2 – Government regulations have an important role in addressing security problems.

Rec 3 – The State of California should regulate the practice of certifying and/or licensing blockchain application developers who develop for or supply blockchain applications to the State of California.

Rec 4 – The State of California is encouraged to adopt the suggested Disruptive Defenses described in this section.

- Eliminate weak authentication technology

- Ensure the provenance of a transaction before it enters the blockchain
- Preserve the confidentiality of sensitive information within and outside the blockchain
- Preserve the integrity of transaction data even when outside the blockchain
- Use cryptographic hardware wherever cryptographic keys are used
- Ensure application access to cryptographic services remains within a secure zone

Rec 5 – Convene Agency-specific Blockchain Advisory Groups
Rec 6 – Convene Online Academic/Industry Security Advisory Group
Rec 7 - Publish Forensic Report of Data Breaches
Rec 8 - Use different blockchains for different application contexts to manage financial and operational risk
Rec 9 - Adopt an experimental period for blockchain application

INTRODUCTION – CALIFORNIA PERSPECTIVE

As the fifth largest economy in the world, the State of California has an extraordinary influence on almost every aspect of commerce. As a progressive state and the home of Silicon Valley, it leads the world on technology, including matters of data security and privacy. California was the first jurisdiction in the world to pass a law in 2002 mandating the disclosure of a data breach affecting Californians. It was also the first state in the U.S. to pass a privacy law in 2018, protecting the personal information of Californians. Any legislation on blockchain will have an effect on the California economy and beyond.

While Silicon Valley companies may have created some of the most useful computing technology to serve people, they have also been responsible for some of the largest data breaches in the world. While California might have a responsibility to serve its residents, it behooves the State to consider the impact of any technology related legislation when it might affect the lives of people around the world.

California's data breach disclosure law provides an extensive record of all publicly disclosed breaches since 2004. While this chronology does not offer guidance on how to prevent these breaches, it does provide a documented record of the types of problems government and private sector companies have failed to prevent.

In light of this, it is important that the State carefully consider the risks and vulnerabilities of blockchain, and design controls to ensure that all users of the

technology have mechanisms to reset blockchain transactions before they are deemed secure enough to replace current practices.

Pilots and Related Use Cases

Blockchain is a young technology. As such, practitioners have not yet identified best practices that can be applied to projects across the board. However, given that blockchain technology intersects fields of databases, network protocols and security, many relevant resources and research are available. Without a detailed understanding of each business application, its data model and the impact of business transactions on networks, it is difficult to make generalized recommendations in these areas.

Considerations and Opportunities for Blockchain Application

While it has always been possible to share business transactions securely among interested parties within an ecosystem, blockchain technology simplifies many aspects of this process and reduces the friction typically encountered in distributed database designs.

One strong benefit is in enabling transparency by making government data available to the public with little effort on the part of the agency. While this data-sharing must be subject to privacy regulations, it would be the equivalent of a permanent "freedom of information act" record available on the internet. It offers potential benefits to preserving democratic norms and holding the government accountable to its constituents.

While blockchain has its benefits, it does not eliminate all problems:

- If multiple companies and government agencies must collaborate on transactions to complete business processes, they must agree on transaction protocols and the rules that regulate those transactions. This can be a simple or burdensome activity depending on the use-case.
- Implementers must handle physical technology problems independent of the blockchain: hardware failures, network outages, security vulnerabilities, and the like. Multiple copies of the blockchain make data always available, which is also true of traditional databases. However, these costs must be taken into account when designing blockchain applications.
- Unless open-source blockchain software implementations are used, licensing costs will be a factor.

- Given the newness of this technology, there is a tendency to equate all blockchain implementations with that of the "Bitcoin" blockchain. However, blockchain applications may be implemented in a variety of ways. State agencies should seek a thorough understanding of the use-case and the technical ramifications of the implementation.

Addressing vulnerabilities. The vast majority of data-breaches are caused by failures to protect data from known vulnerabilities; very few attacks are caused by "zero-day vulnerabilities," i.e., vulnerabilities that were never known until the attack and its methods were discovered.

Most vulnerabilities in any application can be addressed with stronger defenses. These defenses are not unproven new technologies, but are based on current industry standards that raise application security to much higher levels.

While the use of these defenses cannot unequivocally prevent an application from being compromised (since not all threats can be mitigated, or the cost of mitigating all threats will make it prohibitively expensive to implement the application), a compromise is more likely if one or more of these defenses are not incorporated.

KEY RECOMMENDATIONS:

Recommendation 1 - Application-specific evaluation. As with any new technology, blockchain's benefits and risks must be evaluated on a case-by-case basis until a body of knowledge establishes the most efficient designs. Every application will have differences that may require trade-offs.

Recommendation 2 - The role of regulations. Government regulation of some aspects of blockchain development may address security concerns. While regulation does not guarantee the elimination of security breaches, the absence of regulation will create an environment for continued systemic breaches, which may exacerbate losses to consumers.

Recommendation 3 - Certification of blockchain developers. It is recommended that the State of California regulate the practice of certifying and/or licensing blockchain application developers who develop for or supply blockchain applications to the State of California. This can be accomplished through a course of study, an examination, experience and certification much as the networking industry certifies network specialists or the security industry certifies security professionals. While such a "Certified Blockchain Application Developer" (CBAD)

course of study or certification exam does not yet exist and cannot guarantee that certified developers may not create faulty or vulnerable software, this is likely to establish a baseline level of knowledge, expertise and experience that mitigates the risk of catastrophic security failures. The State's educational systems – California State University and/or the University of California – should convene a panel of application development experts from academia and industry to define the curriculum and criteria for becoming a CBAD.

Arguments Against CBAD	Responses
It will stifle innovation and move blockchain investment out of California	California has been a leader in many regulations that have benefited its residents, America and the world; this has only propelled it to become the fifth largest economy in the world. California will, once again, show leadership by ensuring that blockchain applications are built by software developers who are certified to build secure applications that operate in secure environments.
It will be too expensive for some software developers to pay for the certification examination even if they have the knowledge and experience	Community colleges, the CSU and/or UC systems can be encouraged to structure certification exams that can be paid for in a variety of ways: scholarships, internships, apprenticeships, student loans, etc. The examination itself need not be expensive and will represent an insignificant portion of the CBAD's annual salary – perhaps, less than 1%.
It will be perceived as being discriminatory to people without access to higher education.	A college degree should not be a requirement to be a CBAD. However, possession of relevant knowledge and a demonstration of capability is essential. Both can be achieved through an examination and internships and/or apprenticeships prior to being certified.
It will be perceived as being discriminatory to minorities who are under-represented in the technology sector.	Community colleges, the CSU and/or UC systems can be encouraged to offer need-based free classes to help people get certified. Such programs can enable them to find internships and apprenticeships that will enable them to qualify to become CBADs.

It will be perceived as the "industry" blocking out individuals from certification	Much as other professions required certification to practice (e.g., electricians, lawyers, nurses, etc.), the State can make it possible for anyone with the appropriate knowledge and experience to become a CBAD. While the details will need to be defined separately, regulation can ensure the system is fair and open to anyone who chooses to become a CBAD.

Recommendation 4 - Disruptive Defenses. Below is a summary of six best practices for any modern application operating within complex networked systems. The State is strongly encouraged to evaluate potential blockchain applications with these in mind.

1. **Eliminate *weak authentication technology***: The use of *public-key cryptography* authentication will eliminate authentication secrets in applications, thus eliminating the attack vector on target systems. Combining this with cryptographic hardware to protect cryptographic keys will prevent compromises of the user's credential. Invented three decades ago, public-key cryptography is used to protect the most sensitive systems around the world. Expensive and complex in the past, industry standard protocols from the FIDO Alliance and the World Wide Web Consortium, reduce this cost and complexity dramatically. NIST rates FIDO standards at Authenticator Assurance Level 3, its highest assurance level for authentication, which provide "*very high confidence that the claimant controls authenticator(s) bound to the subscriber's account.*"

   Objection: The use of public-key cryptography with cryptographic hardware will be expensive and not provide the level of desired security due to advances in quantum computing (which have the potential to "brute-force" compromise public-key cryptography).

   Response: The FIDO2 protocol has been standardized at this time of writing across operating system platforms (Windows, Android, iOS, OS-X) and all modern browsers (except Internet Explorer). Additionally, cryptographic hardware which support the FIDO2 protocol are now standard components in modern business desktops, laptops and mobile devices. As such, the burden of Californians adopting this authentication technology is reduced to web-applications supporting the use of FIDO2 to authenticate users. Login.gov is a

US Federal website that supports this authentication protocol, and aims to become the gateway to all Federal applications for consumers.

NIST and its contemporaries are aware of the threat to public-key cryptography by quantum computing. However, NIST has been conducting a program to standardize "post-quantum safe" cryptographic algorithms. It is this author's professional opinion that the next 3-5 years will see post-quantum safe cryptographic algorithms incorporated into FIDO/W3C protocols for strong-authentication.

2. **Ensure the *provenance* of a transaction before it enters the blockchain**: Applications almost universally assume that data received by a server is the same data input by the user. This cannot be taken for granted due to inherent vulnerabilities. This is true even when the application uses the Transport Layer Security (TLS) protocol to secure data transmission. There are two vulnerabilities that TLS cannot protect from: i) the theft of a stolen user credential, such as username/password; and ii) the compromise of data within the user's computer after it is submitted by the legitimate user and before it enters the TLS channel, possible if the computer system on which the user is executing the transaction has been compromised.

   A *digitally signed* blockchain transaction before it is submitted by the user will mitigate this risk. However, it is essential to protect the cryptographic key performing the digital signature. This is typically accomplished using cryptographic hardware to secure the *signing key*. With a digitally signed transaction, i) the attacker will not be able to submit a spurious transaction because he will not have possession of the user's *signing key*; and ii) any modifications of the signed transaction by the attacker will alert the application through a failed verification of the user's signature. The FIDO2 protocol, which can strongly authenticate users, also includes specifications for *Transaction Confirmation* that delivers this capability.

3. **Preserve the confidentiality of sensitive information within and outside the blockchain**: The California Consumer Privacy Act (CCPA) requires protection, as do many laws around the world. Encryption is the industry standard for preserving the confidentiality of sensitive information.

   The cryptographic operation (encryption/decryption) must not be delegated to general-purpose elements of the blockchain application, including the blockchain itself. It is imperative that sensitive data be encrypted before it gets on the blockchain so its confidentiality is not compromised.

4. **Preserve the integrity of transaction data even outside the blockchain**: While a user-submitted digitally signed transaction provides assurances about the *provenance* of the transaction, it cannot guarantee the integrity of transactions as that data changes over its lifetime. A digital signature must be applied on the transaction by the application each time the transaction undergoes a change; this ensures that the integrity of the transaction can be verified through its lifetime. The transaction must be signed before it gets on the blockchain so its integrity is preserved within and outside the blockchain.

5. **Use cryptographic hardware wherever cryptographic keys are used**: Cryptography is complex; application developers unaccustomed to working with cryptography underestimate the task and skimp on security controls regarding key-management (the discipline of managing the life-cycle of cryptographic keys). Even billion-dollar companies have been compromised because of this.

   Blockchain applications using cryptographic keys for encryption and signing must use certified cryptographic hardware solutions to secure cryptographic keys, in adherence to NIST guidelines and in keeping with best-practices of the industry

   Objections: The use of cryptographic hardware modules will be expensive and not provide the level of desired security based on recent discoveries of hardware vulnerabilities.

   Response: Specialized cryptographic hardware solutions were expensive. However, industry-standard security hardware is now available at very reasonable prices. Currently, every business-class laptop, desktop, server and mobile device come embedded with *secure elements* that are cryptographic hardware elements capable of sophisticated key-management functions when designed appropriately.

   In a recent breach, Intel's vulnerabilities were due to the optimization of the central processing unit (CPU) for faster operations, without taking into account potential vulnerabilities. A purpose-built cryptographic element is significantly less complex with fewer opportunities for compromise.

6. **Ensure application access to cryptographic services remains within a secure zone if a cloud provider is used:** Cloud computing presents many opportunities for alternative deployment strategies for IT systems, as well as challenges for traditional notions of data security. Companies have made the mistake of taking "on-premises" applications to the public cloud on the assumption that cloud service providers have better security controls to protect data. This may not necessarily be true.

Blockchain applications that use the public cloud must leverage an application architecture that defines a *secure zone* – distinct from the cloud's *public zone* – where the application has access to cryptographic services.

Recommendation 5 - Agency-specific Blockchain Advisory Groups. Given the paradigm shift that blockchain-based systems present for current systems, California agencies should establish Blockchain Advisory Groups representing the following categories of stakeholders:

- Business leaders
- Government representatives of existing systems-of-record (where public records are involved)
- Independent legal and privacy advisers
- Experienced regulators from other sectors such as construction, finance, utilities, etc.
- Experts proficient in systems, application and cryptographic security – not network security
- Representatives of the public who will be affected by the blockchain-based system

Recommendation 6 - Online Academic/Industry Security Advisory Group. The state should establish a public online forum and invite security and cryptography experts from academia and industry to review security designs for blockchain applications and provide their feedback. The proposed forum might work along the following lines:

1. California announces the forum publicly and invites security experts from academia and industry to provide voluntary feedback on proposed blockchain application security designs. The state defines the rules of engagement for the forum and has final authority for who is accepted; the general public may have read-only access to the forum.
2. California agencies proposing to build or implement blockchain applications post the security architecture, which must include a *threat model* of proposed application on the forum, and publish a *Request for Comments (RFC)*.
3. Academic experts on the forum should have the first opportunity to debate among themselves to arrive at a consensus opinion (if feasible).
4. Industry experts may provide their comments before the closing date of the specific RFC.
5. The agency's Blockchain Advisory Group reviews comments and makes a recommendation on the security design/architecture.
6. Final security design/architecture is published on the forum.

While this process may slow the implementation of an agency's blockchain application, the benefit is having the threat-model and security design reviewed by dozens of professional security experts. This process is similar to the process used by Internet Engineering Task Force (IETF) to define standards for the internet through its request for comments.

Recommendation 7 - Publishing Forensic Report of Data Breaches. California's data breach disclosure law of 2002 was bold for its time. However, it did not go far enough to have prevented the 11,000 publicly disclosed breaches that followed: it did not mandate that the company or government agency publish a standardized forensic report documenting the breach and the mechanics of how it occurred.

When a data breach occurs today, most cybersecurity professionals without access to the evidence must deduce (at best) or guess (at worst) how it occurred and what might have prevented it. The industry that creates technology products and universities that train new generations of technology professionals have limited ability to prevent these problems unless the US Cybersecurity and Infrastructure Security Agency (CISA) publishes an advisory of a vulnerability through a US-CERT alert.

The Data Breach Forensic Report should be made public so academia and the technology industry may learn from it and improve their designs and technology implementations.

Recommendation 8 - Private, Permissioned Blockchains. Different blockchain architectures should be used for different application contexts to manage financial and operational risk.

While a home and an automobile are both assets typically purchased by consumers and registered with the State of California, given the different ecosystems these asset classes operate in, two separate blockchain-based systems to track these assets is warranted. The same analogy applies to humans who participate in different ecosystems: healthcare, education, finance, government, employment, commerce, etc. Each ecosystem may deserve its own blockchain to support agency transactions within that ecosystem.

The desire for privacy is not inherently contradicted by the immutability of blockchains. The State should consider that neither a blanket privacy law nor a rush to implement blockchain is an optimal answer. Where transparency of information

serves a public good, government must make considered decisions to find the right balance.

Recommendation 9 - Experimental Period. The speculative nature of crypto-currencies and the dramatic events surrounding public blockchains, for example the collapse of Mt. Gox and the "hard fork" of the Ethereum blockchain, suggests that the State of California might consider defining an *experimental* period of perhaps 5-7 years, where implementations of blockchain-based applications are restricted to only private and/or permissioned blockchains, under the State's control, for use-cases that reflect public data. This does not imply that the State may not implement blockchain-based applications; merely that in the early phases of adoption, the State avoids the use of public, permission-less blockchains such as the Bitcoin blockchain, Ethereum or similar platforms where anyone may introduce transactions and/or process data without permission.

Initial applications might be in experimenting with a blockchain simulating the Registry of Births, Deaths and Marriages, or the registration of Business Entities, where information is public by law. This will enable the State to enter the field cautiously and learn from its experience before taking bolder steps. However, until such time computer security and the blockchain ecosystem can prove it can protect the average consumer or citizen, State agencies must run parallel systems to ensure that in the event of a conflict, existing systems-of-record will prevail over blockchain-based systems.

PRIVACY INFRASTRUCTURE

Key Recommendations:

- With CCPA enacted and CPRA on the horizon, California already has a strong privacy-protecting legal regime. Although blockchain is a new technological solution, it does not change the fundamental privacy rights to which individuals are entitled, set forth in the OECD Fair Information Principles. Ensuring those privacy rights is not incompatible with use of blockchain, whether under CCPA, GDPR, or other similar laws. At present California's privacy laws need not be amended to enable adoption of blockchain technologies and use cases. Still, it will be important for the legislature to monitor for potential new issues in blockchain applications related to protecting individuals' privacy that are not addressed by technical measures or the existing legislative framework.

- Additional education about how to use blockchain in a privacy-compliant and enhancing way is needed. The guidance from the European Blockchain Observatory and the Commission nationale de l'informatique et des libertés (CNIL) provide a good start but are obviously tailored to European law. If adopted, CCPA would establish a new California Privacy Protection Agency. If that comes to pass, the California Legislature should task the agency with issuing guidance for both the State and for private entities on how to deploy blockchain in a manner that complies with California privacy laws. In the event that the Agency is not created, the Attorney General, as lead enforcer of privacy laws in California, should issue such guidance and be provided the necessary resources to do so.

INTRODUCTION – CALIFORNIA PERSPECTIVE

California is a leader on privacy protections, having adopted the nation's first comprehensive privacy law, the California Consumer Privacy Act (CCPA). In addition, there likely will be a follow-on ballot initiative, the California Privacy and Enforcement Rights Act, this year.1 In addition to these landmark measures, California businesses are subject to a number of other privacy laws, depending on the type of data they process and where they do business.

Thus, as the State of California and California businesses implement blockchain, they must do so in compliance with applicable privacy laws, as well as in cognizance of potential future privacy legislation at the Federal level, where several bills are pending. While privacy laws vary considerably in their specifics, most of them provide some combination of the rights embodied in Fair Information Principles developed by the Organisation for Economic Co-operation and Development (OECD) in 1980 (a revised version of these can be found in the OECD Privacy Framework).6 These Principles define the framework of modern privacy regulation.7

LITERATURE REVIEW

Quite a bit has been written on blockchain and privacy. With respect to the ability of blockchains to comply with GDPR, the two main reports are the EU Blockchain Observatory's report Blockchain and the GDPR[8] and the French Data Protection Authority's (CNIL) report Solutions for a Responsible Use of the Blockchain in the

Context of Personal Data.[9] Important critiques of the state of privacy compliance of blockchain solutions have also been published.[10]

Blockchain Compliance with Privacy Laws

Most of the privacy rights embodied in the OECD Fair Information Principles and the various laws pose no greater challenges for blockchain solutions than any other technology. For example, implementers of blockchain solutions must provide notice to individuals of what data they are collecting and the purposes for which the data will be used, must have a legitimate purpose for collecting and processing the data, not use the data for other purposes aside from those specified without consent, and must implement technical and organizational measures to protect the security of the personal data. In all these cases, blockchain either does not impede compliance or, as in the case of security, offers tools that can make compliance easier.

Still, these requirements cannot be ignored. As one author notes in connection with a permissible basis for collecting and processing personal data, "Most existing projects rely on 'consent' but do not effectively address the mechanism for obtaining adequate informed consent or its revocable nature." The article also suggests that it might be difficult to rely on GDPR's "legitimate interests" test given the automated nature of most blockchains, but that is probably overstating the case: many non-blockchain uses of personal data rely on the legitimate interests of the controller that are not outweighed by the rights of the individual without engaging in a person-by-person balancing test.

She further suggests that replication of the data on nodes may lack a legitimate purpose, unless there is a need for the data to be replicated across a blockchain network. She also argues that data replication runs afoul of data minimization requirements—that is, only the minimum data needed for a purpose for which it is processed be used. But fundamentally blockchain operates as a distributed ledger, and the distributed nature of that ledger provides enhanced security (by making the ledger more difficult to compromise) and enabling it to operate without a single master entity. These benefits should suffice to meet the "permissible purpose" and "data minimization" tests—for data replication is essential to realizing the benefits of application of blockchain in these uses.

Right of Rectification and Deletion

Most concerns about the ability to build a privacy-compliant blockchain solution relate to the rights of rectification and deletion. Under most privacy laws, individuals have the right for inaccurate data about them to be corrected, and for it to be deleted when no longer needed for the purpose for which it was collected. In addition, data controllers are obligated to delete data when it is no longer needed for the purpose for which it was collected. However, one of the features of blockchain is immutability—every transaction is tied to the preceding transaction cryptographically in a way that any subsequent alteration is detectable. This means that personal data, once written to a blockchain, remains there permanently.

Several commentators have suggested that this means blockchain is incompatible with laws such as GDPR that provide rights of rectification and deletion. However, it is possible to comply with GDPR's right to be forgotten, even though data stored on the blockchain is immutable, via several means. First, the recipient can delete his or her private key, breaking the association with the public key. Second, the data to which the public key relates (e.g., the credential) can be deleted, such that the public key serves no purpose. Indeed, it might be possible to hash or encrypt the data rather than deleting it.

The CNIL, the French data protection commissioner's office, has published a helpful paper on blockchain and privacy issues: "Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data." Fundamentally, blockchains are used to store public keys that identify individuals, but these can effectively be rendered anonymous by the individual by deleting his/her private key or via other measures.

As the CNIL guidance states, "…blockchain can contain two main categories of personal data: Identifiers of Participants and Miners [and Additional or "Payload" Data]. Each participant has an identifier, called a public key, consisting of a series of alphanumeric characters that seem random. This public key refers to a private key that is only known by one person."

Guidance thus far recognizes that it is not technically possible to "delete" information stored on the blockchain. Although definitive guidance would be helpful, alternative measures which obfuscate the information on the blockchain likely are "similar to effective erasure of data" according to the CNIL.

Deletion of the Private Key. The CNIL also stated that the deletion of the private key would make it impossible to prove what payload data had been associated with the public key and as such "would no longer pose a risk to confidentiality." The self-help approach where the user has control over their information through a portal or other technology is also supported by regulators.

Deletion of Underlying Data. Presumably, deletion of all the data on the centralized server that is linked to by the blockchain (so that the public key is merely a number without purpose) would satisfy the right to be forgotten.

Hashing or Encrypting Payload Data. While it does not go into specifics, the CNIL acknowledges that proper hashing or encryption techniques of payload data would be an acceptable method of erasure for blockchain technology.

Other Options. Over time, approaches may evolve that are recognized as acceptable but were not mentioned in the guidance, e.g., scrambling payload data, multiple public keys corresponding to specific personal data (like a new metadata approach) and other approaches.

CONTROLLER-PROCESSOR DISTINCTION

Beyond rectification and deletion, other privacy-related questions must be answered for blockchains. For example, many privacy laws distinguish between data controllers (those who determine the purposes and means of processing personal data) and data processors (those who process data on behalf of and pursuant to the instructions of a data controller).

Permissioned Blockchains. For a permissioned blockchain, the controller-processor issue can be resolved via the governing documents. In general, when a consortium operates the blockchain, it does so to provide a service to consortium members. Thus, each of them should be the controller of the personal data they write to the blockchain, with the consortium acting as a data processor. This is consistent with guidance issued by the CNIL. As consortium members use the blockchain for their own purposes, each will be a controller. However, if they write data to the blockchain for a common purpose, they could be considered joint controllers. It is possible for companies writing to the blockchain to designate a single entity to be the controller, per the CNIL guidance, if that entity makes decisions for the group. To achieve this controller-processor distinction, in most cases the consortium should be

a separate legal entity. If it isn't, then fundamentally every consortium member is a processor for every other consortium member—or they are joint controllers.

As the consortium will be a data processor, it will need to enter into data processing agreements with each controller that complies with the requirements of Article 28 of GDPR. These terms could be incorporated into the consortium agreement itself, as the consortium members will be the ones using the blockchain. Alternatively, each time a consortium member wanted to use the blockchain as part of a service, it could enter into a data processing agreement with the consortium. Either way, the relevant agreement will need to specify that the consortium member is the controller of personal data written to the blockchain and include instructions from that member to the consortium as to how that data should be processed.

Permissionless Blockchains. For permissionless or decentralized ledgers, the question of who is a controller poses more of an issue. As Renieris states, "Many blockchain or ledger-based projects argue that they are too "decentralized" to identify data controller(s) or take responsibility for giving effect to data subject rights." That won't work from a privacy compliance perspective, because it means that anyone operating part of the ledger—such as a node—may then be considered a co-controller, liable for all aspects of compliance.

Where good data privacy hygiene is observed, this should not be insurmountable. For many applications, the only personal data that needs to be written to the blockchain is a Digital Identity Document (DID), and the tie between that DID and an individual can be severed after the fact by various techniques (including simply having the individual destroy his or her private key). But on a permissionless blockchain, one cannot foreclose that someone may write additional personal data to the blockchain, and that the individual whose data is written there may have rights—whether under CCPA, GDPR, or another privacy law—to have that data deleted or to prevent it from being disclosed to others.

In the case of CCPA, which applies to businesses, a business that chooses to write personal data in plain text to the blockchain will likely be in a position where it is unable to comply with the Act. Although it is unclear that a node operator falls under the Act, because it may not qualify as a business or a service provider, the mere writing of personal information to a permissionless blockchain would not necessarily put that blockchain in violation of CCPA. However, the situation with

respect to GDPR is likely different. There, the data protection rules apply to any entity that has data. In the absence of a permissioned system, where there is a data processing contract between the entity writing to the blockchain and each node operator, node operators are likely co-controllers, and responsible for complying with the privacy rights of individuals whose data is written to the blockchain. This clearly is the implication of the CNIL guidance.

Although there are successful decentralized ledgers—Bitcoin itself and Ethereum to name two—most commercial applications of blockchain appear to use permissioned ledgers, which helps address responsibility and accountability for compliance.

DATA TRANSFERS

Because the blockchain will consist of several nodes located around the world, it will be important that the EU's standard contractual clauses (SCCs)—specifically, the controller-to-processor clauses—be part of the consortium agreement.[11] That way, when consortium members operate nodes and data written to the blockchain is immediately replicated around the world on those nodes, it will be covered from a data transfer perspective. Likewise, any agreement between a consortium member and the consortium to write data to the blockchain will also need to include the SCCs.

BLOCKCHAIN AS A TOOL TO ENHANCE PRIVACY

The focus on the ability of blockchain solutions to comply with privacy laws should not diminish the fact that blockchain can help enhance privacy in many situations by enabling fine-grained control of access to personal data, along with strong security protections. In particular, blockchain-based digital identity solutions enable individuals to share only those aspects of their identity they wish to with others, and make correlation among different aspects of a person's identity more difficult. By removing the connection to a widely used identifier—such as a social security number or driver's license—and enabling the information to be shared granularly but with confirmation that it ties to the individual sharing it, blockchain enables greater privacy by avoiding links among different pieces of information about individuals that a third party can then aggregate.

ENDNOTES

[1] California Privacy Rights and Enforcement Act of 2020, as filed with the California Attorney General's office on November 4, 1999, available at https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf.

[2] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119 4.5.2016, p. 1).

[3] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-91, Title II.

[4] Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g.

[5] Financial Services Modernization Act of 1999, Pub. L. 106-102, 15 U.S.C. §§ 6801-6809.

[6] Organisation for Economic Co-operation and Development, The OECD Privacy Framework, 2013, available at http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[7] Jason Albert, "U.S. Privacy Law: A Short History," (June 28, 2018), available at https://www.linkedin.com/pulse/us-privacy- law-short-history-jason-albert/.

[8] Blockchain and the GDPR, European Union Blockchain Observatory and Forum (October 16, 2018), available at https://www.eublockchainforum.eu/reports.

9. Blockchain and the GDPR: Solutions for a responsible use of the blockchain in the context of personal data, Commission nationale de l'informatique et des libertés (November 6, 2018), available at https://www.cnil.fr/en/blockchain-and-gdpr- solutions-responsible-use-blockchain-context-personal-data.
10. Elizabeth M. Reneiris, "Forget erasure: why blockchain is really incompatible with the GDPR" (September 23, 2019), available at https://medium.com/berkman-klein-center/forget-erasure-why-blockchain-is-really-incompatible-with-the-gdpr.

11. Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU).

Appendix A

A Brief Background on Information Security

In an age where almost everyone in the developed world – and increasingly, people in the developing world – are connected to the internet, businesses are rapidly transforming themselves to transform how they manufacture products for, and how they deliver services to their customers. Every sector of the economy is affected by the new ways of conducting business over the internet. However, what is little recognized is that important elements of trust engendered over centuries of handwritten ledgers and record-keeping, are being eroded through this transition.

If we assume that consumers and markets had implicit trust in business transactions in the middle of the 20th century, when almost all record-keeping was manual and based on handwritten records, the introduction of mainframe computers did not erode this trust. Checks and balances, implemented during the days of manual record-keeping continued to verify that mainframes recorded and delivered the same results as manual ledgers. Additionally, given the cost of transitioning to computerized record-keeping was very high, enormous care was taken to ensure that data integrity was maintained. Data confidentiality was not questioned since even vast swaths of people within the company implementing such technology, were prevented from accessing such systems and data.

It can be said, that at the peak of mainframe and mini-computer usage for data-processing, computers were viewed to offer dramatic improvements in productivity to business transaction processing without the loss of data-authenticity, confidentiality or integrity. The advent of the Personal Computer (PC), Local Area Networks (LAN), the internet and eventually, the world-wide web (WWW) heralded the erosion of trust.

The cost of deploying PCs and LANs were insignificant compared to the cost of deploying a mainframe and/or mini-computers; as a result, the discipline inculcated

over years in managing mainframes and mini-computers were largely ignored as business processes transitioned to PCs and LANs. But, with the introduction of the internet and the WWW, businesses began to experience the consequences of ignoring security in the newly transitioned/created business processes that leveraged PCs, LANs and the WWW.

The outbreak of the Morris Worm in 1988, began a long slide that resulted in California passing the first regulation of its kind anywhere in the world in 2002. It mandated businesses to disclose data-breaches affecting California residents. Since the passage of this law, more than 10,000 publicly disclosed breaches and more than 11 billion breached data-records have been recorded with dozens of jurisdictions around the world passing new data-security and privacy regulations of which the most notable are the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA). [*NOTE: When this document is merged with other submissions in the final recommendation, please include a cross-reference to Jason Albert's Privacy related submissions, here. Thank you.*]

What this suggests is that while businesses have invested hundreds of billions of dollars – if not trillions over the last two decades – in building new business applications on the internet, there has been woeful attention paid to the security of data: ensuring its provenance, confidentiality and preserving its integrity.

Blockchain

Blockchain is touted to have many unprecedented business benefits, including security; but when dissected technically, there is only one unique benefit that blockchain offers: *the ability of multiple parties to participate in a distributed database system – a cost-effective shared ledger – where each party may view and verify each others' transactions, as well as participate in those transactions, without excessive friction.* All other stated benefits of blockchain have been feasible in the past but have remained unimplemented – or not implemented effectively enough to accrue benefits - for a variety of reasons.

For instance, the single most touted benefit of blockchain – *immutability of transactions* – has been possible within applications for over two decades with the use of digital signatures, a benefit of *asymmetric key cryptography* introduced as early as in the late '70s. *Distributed databases* across networks have been in use for over three decades. *All* applications currently in use are *permissioned* applications.

And, *multi-party trust* has also been in use for over two decades with the use of public key infrastructure (PKI). What blockchain has done is to demonstrate that these benefits can be combined together to provide, hitherto, unrealized benefits to businesses and government.

Given the above, the single most important consideration public and private organizations must undertake regarding the security of any proposed solution relying upon blockchain technologies is to make a commitment that security will not play a secondary role within the application, as has been so for the last few decades.

Blockchain heralds a movement to eliminate time-tested procedures of trust which were simple to understand by lay-people, and to replace them with cryptographic procedures transparent to only advanced professionals. While it might be argued that this is the natural evolution of science and technology, when it comes to human interactions with government and businesses, in order to preserve trust in institutions and an orderly society, it is imperative that every element of application security that can cast aspersions on the system be considered carefully before it can be deemed trustworthy.

This is analogous to a time when the construction industry could build homes without licenses, permits, building codes, inspections and certificates of occupancy. Many people paid a price with their lives, livelihoods and finances for such a *laissez-faire* mode of operations – some still do even in this 21st century despite the industry being heavily regulated in California. The global financial crisis of 2007-2008 occurred despite the banking and financial industry being the most regulated industry in the world.