# IV. Considerations for Appropriate Application

## IV.A. A Framework for Assessing the Fitness of Blockchain Technology

### Introduction

The framework contained in this document is intended to support initial analysis by the State of California of whether blockchain technology might be a useful tool to help solve an identified problem. A rudimentary knowledge of blockchain is assumed, consistent with the completion of any of the multitude of "Blockchain 101" courses that are widely available; however, the framework is specifically intended for use by policymakers, not technical experts, and as such, elides certain technical details as necessary to promote comprehension.[1]

Blockchain adoption is first and foremost a business decision, rather than a technical one. Good use cases must solve real problems for organizations. Great use cases solve real problems at a cost that is significantly lower than the benefits the adoption brings. Blockchain can be a precursor to, and in some cases require, the redefinition of associated processes. Thus, it should be analyzed holistically, rather than strictly through a technical lens.

### Decision Tree Approach

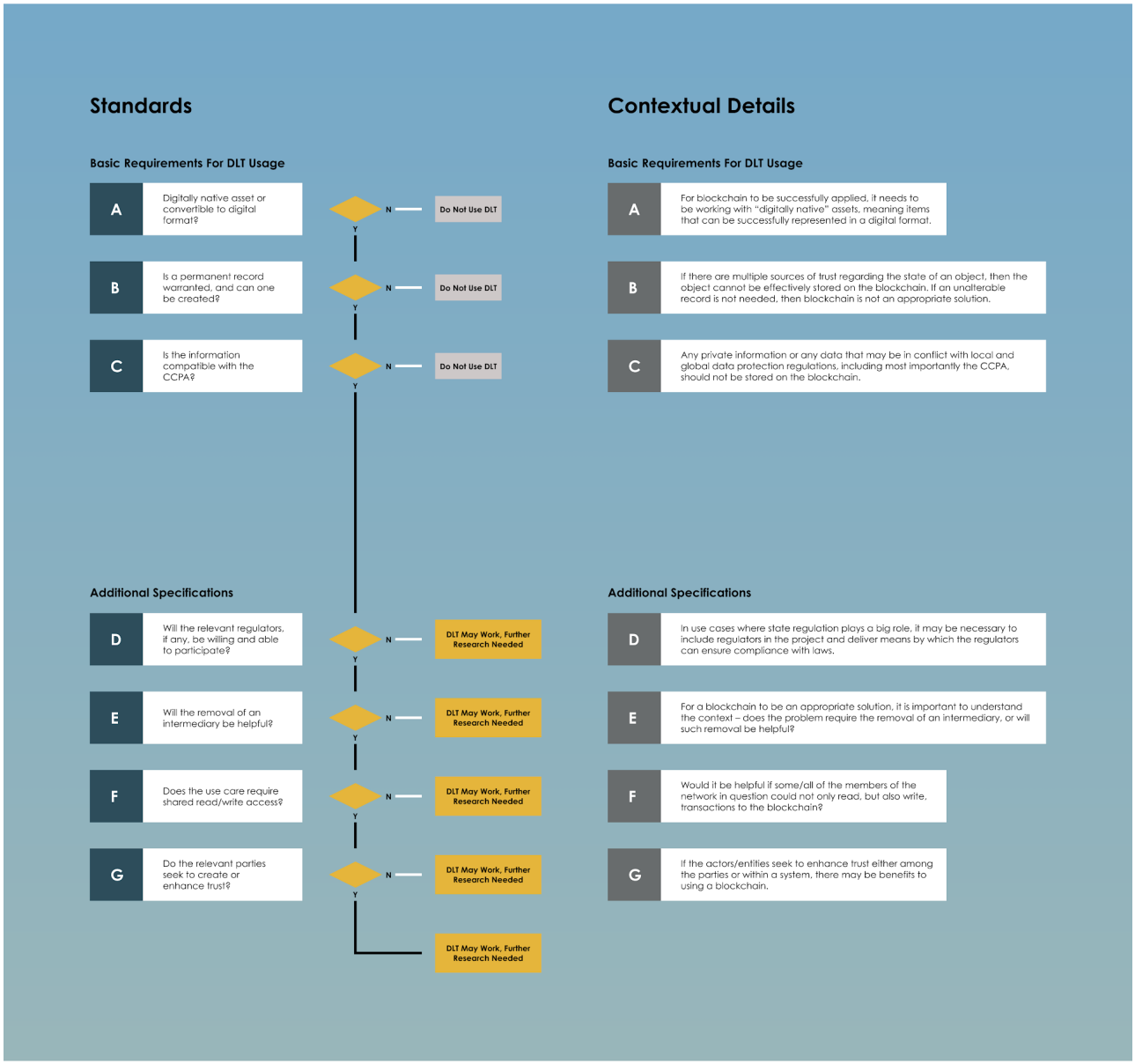
This tool is intended to enable rapid initial analysis of whether blockchain could be an appropriate solution for a defined problem. It is not intended to provide a final authoritative answer, but instead to assist senior decision makers in evaluating whether to deploy resources into exploring a blockchain-based solution to a given problem space, and if so, at what scale. The hope is that shifting focus to the problem, and away from a particular solution, will encourage a practical approach while reducing the risk of ill-advised experimentation.

The decision tree is composed of a number of questions that assist in defining whether a blockchain might be the correct approach for a particular problem or not.

[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. https://www.weforum.org/whitepapers/blockchain-beyond-the-hype

## Framework for Assessing the Fitness of Blockchain

DECISION MATRIX






**A.** For blockchain to be successfully applied, it needs to be working with "digitally native" assets, meaning items that can be successfully represented in a digital format.

**B.** Is a permanent record warranted and can one be created for the digital asset in question? This is perhaps the most critical question that needs to 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 that have responsibility for the state of the digital asset in question agree how state will be handled/managed in the new business process prior to any development occurring. Separately, is a permanent record even desirable? If an unalterable record is superfluous or counterproductive, for example, in a situation where the need to delete information is critical, then blockchain/DLT is not an appropriate solution. As an example, it would not make sense to store an ordinary grocery list on a blockchain.

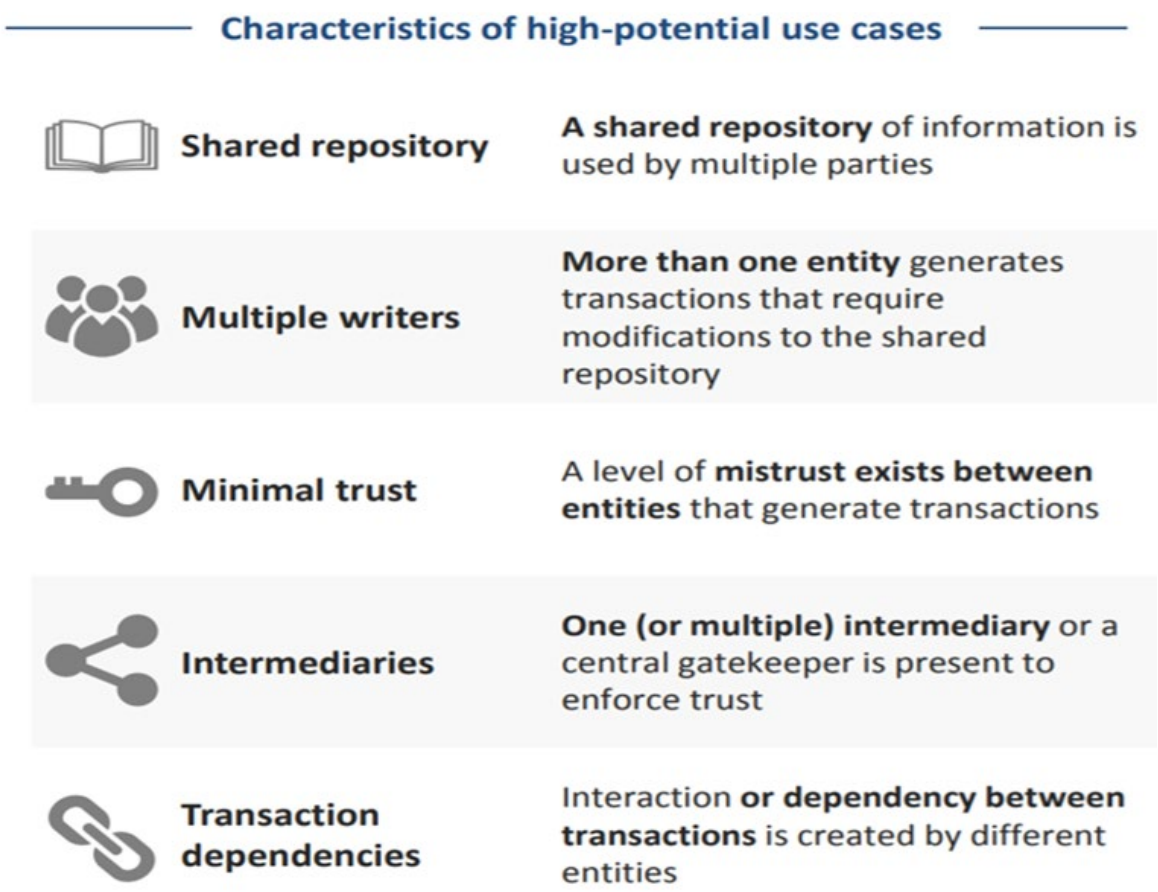
**C.** Any private information or any data that may be in conflict with local and global data protection regulations, including the California Consumer Privacy Act, should not be stored on the blockchain.

**D.** In use cases where state regulation plays a big role, it may be necessary to include regulators in the project and deliver means by which the regulators can ensure compliance with laws. This engagement will be a critical piece that needs to be addressed for many use cases and may throw up administrative or other roadblocks.

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

**F.** Does the use case require shared read/write access? That is, would it be helpful if some/all of the members of the network in question could not only read, but also write, transactions to the blockchain?

**G.** If the actors/entities seek to enhance trust either among the parties or within a system, there may be benefits to using a blockchain.




## IV.B. Ethical Considerations

### Key Recommendations

**REC IV.B.1.** Consider how best to **educate** Californians about blockchain, to ensure a basic understanding as the technology is introduced in the public and private sector.

**REC IV.B.2.** Encourage **environmental sustainability** as use cases are being developed by offering incentives to blockchain companies that have an environmental sustainability plan or impact statement. 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 the risks associated with imposing a set of top-down rules on blockchain designers and developers, who 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 than a "culture of compliance."[2]

## Essential Elements of Ethical Considerations

Blockchain technology may eventually 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. Ethical issues related to the potential social impact of blockchain are fairness, equity, accessibility, trust and transparency, and sustainability.

**1) Fairness**. The concept of fairness assumes that blockchain technology will not perpetuate bias or discrimination.[3] Human bias can be either explicit, such as overtly racist comments, or implicit. Implicit biases operate through our subconscious minds, and we are often not even aware of our implicitly biased beliefs.[4] For example, what are the potential biases of the core developers influencing decisions on a permissionless blockchain? Alternatively, are corporate executive biases affecting the design and implementation of enterprise blockchains?

Technology can also have implicit values.[5] Blockchain technologists should implement processes to test for potential biases and seek to remediate their effects in the technology's design.

Any type of bias, whether explicit or implicit, can lead to discrimination. It is incumbent upon blockchain proponents, including legislators, industry

[2] Beard, Matt and Longstaff, Simon, "Ethical Principles for Technology," *The Ethics Centre, Sydney (11),* 2018. https://ethics.org.au/ethical-by-design/
[3] Beard and Longstaff, "Ethical Principles for Technology" (2018).
[4] World Economic Forum White Paper, "AI Governance: A Holistic Approach to Implementing Ethics Into AI" 9 (2019). https://www.weforum.org/whitepapers/ai-governance-a-holistic-approach-to-implement-ethics-into-ai
[5] Beard and Longstaff, "Ethical Principles for Technology" (2018).

leaders, and academics, to ensure that we are creating an industry that is free from discriminatory actions and/or inadvertent discriminatory effects.

**2) 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 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 narrow 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.

**3) 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.[6] 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.

At this time, a blockchain entrepreneur does not need an advanced degree in computer science to start a blockchain company. One way the legislature

[6] Mone, Gregory. "Bias in Technology." *Communications of the ACM*, 60(1), 2017. https://perma.cc/44UD-H8LC

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. Moreover, California's legislature and industry leaders should work to create "a culture of cooperation and engagement between stakeholders."[7]

**Community education:** A second accessibility consideration involves the high learning curve required to understand this technology. As 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 intersect with important areas of their daily lives?

**4) Trust and transparency.** Blockchain's architecture facilitates increased trust and transparency by its very nature. In the sense of ethical principles, the system exemplifies a culture of cooperation and engagement between stakeholders and one that demonstrably behaves as intended. Its functions should be explained (i.e., should be able to know how the blockchain platform or its functions were executed), and if it causes harm, it should be possible to know why.

**5) Sustainability.** Blockchain use cases have the potential to either further the goal of sustainability or diminish it. Sustainability concerns are most prevalent in permissionless blockchains, such as those that rely upon proof of work consensus and require high energy consumption. These issues are less concerning with permissioned/enterprise blockchains.

California, as a leader in environmental sustainability policies, can offer incentives to blockchain companies that align with these goals. 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.

Moreover, this technology can assist consumers and other sustainability advocates in creative ways. For example, on a supply chain, enterprise blockchains could enable ordinary consumers to identify the origins of any

[7] Mone, "Bias in Technology."

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.[8]

## Implementers of Ethical Considerations

**Developers**. Blockchain developers and designers should consider how the ethical principles affect their design choices. For example, those designing user interfaces should follow best practices for accessibility. 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 ensuring that blockchain applications are consonant with privacy considerations and regulation, as mentioned in the decision tree above.

**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.[9] 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."[10] When assessing the ethical implications of blockchain technology, California should abide by the following three principles:

### 1. Address key ethical design goals

1. Seek societal benefit: Maximize good and minimize bad.
2. Equity: Does this benefit all Californians, or only a few?

[8] LeBlanc, Rick. "How Blockchain Will Transform Supply Chain Sustainability." *Small Business*, 2020. https://www.thebalancesmb.com/blockchain-and-supply-chain-sustainability-4129740
[9] *See, e.g.,* "SEC Charges Issuer With Conducting $100 Million Unregistered ICO" (2019). https://www.sec.gov/news/press-release/2019-87
[10] Beard and Longstaff, "Ethical Principles for Technology."

3. Efficiency and effectiveness: How can we achieve ethical design and use cases without slowing innovation?

**2. Consider ethical uses of blockchain technology**

1. Fairness: Is this technology designed and deployed in a fair, non-discriminatory manner?
2. Accessibility: Design to include the most vulnerable user.
3. Responsibility: Anticipate and design for all possible uses.
4. Sustainability: Create technology to advance sustainability, public health, and corporate social responsibility.

**3. Minimize unintended consequences**

1. Are there unintended biases or conflicts in the design or use of this technology?
2. Are any populations being unintentionally harmed by the way this technology is developing?
3. 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 any potential negative effects. With an ethical framework in place as regulation moves forward, California will serve as a model for the development of ethical blockchain technology.

## IV.C. Digital Identity

### Key Recommendations

**REC IV.C.1.** The California Legislature should enact legislation that allows public entities to issue as authorized verifiable credentials the identification documents set forth in Section 1798.795(c) of the California Civil Code as verifiable credentials. Individuals would benefit from the ability to have these identification documents available in a secure and verifiable digital form under their control. Verifiable credentials would store no substantive personal information on the blockchain. Instead, decentralized

identifiers (DIDs) would be stored verifying that the document was validly issued and shared with the individual's consent.

**REC IV.C.2.** In a post-COVID California, two near-term opportunities present themselves for the state to pilot applications of digital identity and verifiable credentials: health records and driver's licenses.

i. The impact of COVID-19 heightens the necessity for trustworthy health records. Making them available as verifiable credentials will be vital to ensure seamless and immediate sharing with individuals' consent and to protect against forgery. Enactment of Assemblymember Ian Calderon's bill AB 2004, introduced in the 2019-2020 Regular Session, would enable this.[11]

ii. Driver's licenses are foundational identification documents for most California residents, and often must be shared as proof of identity or qualification. A pilot in this area would have wide applicability, enabling evaluation of use cases from basic identification to qualification to drive particular types of vehicles.

## INTRODUCTION

The State of California is a major provider of identity verification for individuals. The most prominent service 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. California also licenses a number of professions, including lawyers, doctors, nurses, engineers, and the like, as more fully documented in Section V.H. on Education and Workforce. While we think of these occupational licenses as permissions to engage in a particular profession, they also verify the identity of the individuals who are licensed.

California is also a significant potential 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, this requires various paper documents, such as birth certificates, drivers licenses, passports, utility bills (to prove residence) and so on.

[11] Medical test results: verification credentials, Assembly Bill 2004, 2019-2020 Reg. Sess. (Cal. 2020).

Digital identity is critical to the modern economy. We already use digital identities in various ways, such as using social media credentials to log into a service. However, existing digital identity solutions have limitations. Specifically, many forms of digital ID are vulnerable to hacking and compromise, and require individuals to entrust their data to third parties; 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."

## 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 to whom it pertains 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 proof of 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 credentials and how they are shared.

### The Role of Blockchain[12]

Digital identity is based on two concepts: self-sovereign identity (SSI) and decentralized identifiers (DIDs). SSI refers to the fact that individuals and

[12] This and following sections have largely been adapted from: Woods, Jorden and Radhika Iyengar. "Enterprise Blockchain Has Arrived: Real Deployments. Real Value." *Self-Published* (2019), 237-246.

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. Like in the physical world, identity information and confidential data will be stored in a wallet. In a digital wallet will be credentials and information tied to one's identity and trusted relationships. Since the wallet is digital, it is much more powerful and can control significantly more information than a physical wallet carried on our person. For example, a digital banking "card" would be issued by a bank and serve as the credential, along with biometric data, for access to the bank account. (Use of biometric data introduces its own privacy concerns, especially for use with vulnerable populations.) These credentials, issued by each entity, but 'owned' by the user, would streamline access and the processing of all transactions.

Unlike the physical world, however, our digital wallet and credentials will be keyed to our DID and protected using blockchain technology. This makes it secure, verifiable, and self-sovereign. Specifically, a DID will be stored on the blockchain, with a unique global identifier that includes an individual's public cryptographic key. When that person shares an aspect of their identity from their digital wallet, they will sign it with their associated private cryptographic key. The recipient will then know it relates to the individual. If the identity aspect is verified by a third party, such as, say, the DMV, it will also be signed by that entity, which has its own DID. An individual or entity can have multiple DIDs in order to represent a range of personas, entities and contexts. In short, only we will have the master keys (private key) and be able to authenticate to gain access to our digital identity and associated data, aspects of which can be verified by third parties.

Taken together, the combination of SSI, DID, and blockchain can create an identity layer in the online world that verifies 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.

**Collaboration and Standards**

Cross-entity collaboration will be needed. The Decentralized Identity Foundation (DIF)—an ecosystem of the top blockchain platforms and SSI community globally that includes IBM, Microsoft, Workday, Hyperledger, ConsenSys, Accenture, Aetna, Mastercard, and SecureKey—and the World Wide Web Consortium (W3C) have been working to ensure that digital credentials have standard formatting and are interoperable, including via universal DID specifications.[13] 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.

**Self-Sovereign Identity & Trust**

Blockchain is a key enabler of self-sovereign identity, but not because personal data (aspects of identity) are stored on the blockchain.[14] 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."[15] 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 both by the issuer's and individual's private key 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.

[13] Decentralized Identity Foundation, available at https://identity.foundation/, and Decentralized Identifiers (DIDs) v1.0, available at https://www.w3.org/TR/did-core/.
[14] Preukschat, Alex. "SelfSovereign Identity—a guide to privacy for your digital identity with Blockchain." 2018. https://medium.com/@AlexPreukschat/self-sovereign-identity-a-guide-to-privacy-for-your-digital-identity-5b9e95677778.
[15] Gisolfi, Dan. "Self-sovereign identity: Why blockchain?" *IBM,* 2018. https://www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-why-blockchain/.

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 as zero-knowledge proof (ZKP), are used in various blockchain 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, potentially leading to a decrease in significant data breaches.

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 linked with 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 information 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, eliminating lengthy delays waiting 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 developed specifically for credit unions.[16] In February 2018, CULedger launched MyCUID enabling credit union customers to authenticate securely from their mobile devices with a biometric credential and protect themselves from financial fraud and

[16] CULedger: https://www.culedger.com/.

identity theft. MyCUID also employs SSI, so customers can use selective disclosure to control specifically which data is shared in each context.

**Verified.me.** Verified.me is a blockchain-based digital identity network developed by SecureKey, that launched in May 2019 in partnership with a set of large Canadian banks plus Canadian and U.S. government offices.[17] The system provides individuals with a digital identity stored as a private key on the user's mobile device. The user can authorize personal information stored with one provider to be shared securely and privately with another.

**Trust Your Supplier (TYS).** 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.[18] 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.

**ID2020 Digital Identity Alliance.** The ID2020 initiative is an alliance of major global organizations, designed to enable digital identity that provides political, economic, and social opportunity.[19] The focus has been on creating a digital ID that is private, portable, persistent, and personal. The effort is designed in fulfillment of the United Nations' 2030 Sustainable Development Goals, including the commitment to "provide legal identity for all, including birth registration" by 2030.

**Workday Credentials**. Workday Credentials enables employers, training programs, and others to issue credentials to individuals; these credentials then live on the individual's phone in the WayTo app, allowing the individual to share them with a fine degree of granularity.[20] Verification is secured via a blockchain backbone, so that the verifier of a credential can have confidence that the issuer issued the credential, it relates to the person who shared it, and the credential has not been revoked.



[17] Verified.me: https://verified.me/.
[18] Trust Your Supplier: https://www.trustyoursupplier.com/.
[19] ID2020 Digital Identity Alliance: https://id2020.org/.
[20] Workday Credentials, Cloud Credentialing Management: https://www.workday.com/en-us/applications/credentials.html.

## IV.D. Cybersecurity & Risk Management

### Key Recommendations

**REC IV.D.1.** Evaluate blockchain appropriateness based on the specific use case, considering financial and operational risk.

**REC IV.D.2.** To establish a new baseline of security and adequately trained workforce for this emerging technology, the State of California should encourage training for (and potential certification and licensing of) application developers who develop or supply blockchain platforms to the State of California.

**REC IV.D.3.** The State of California should create policies and standards to govern the use and control of blockchain utilizing industry expertise and other worldwide standards.

**REC IV.D.4.** Convene a Blockchain Advisory Group composed of experts from academia and industry.

### Introduction

As the fifth largest economy in the world, the State of California has an extraordinary influence on almost every aspect of commerce. 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 and was 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.

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 such breaches, it does provide a record of the types of problems government and private sector companies have failed to prevent.

In light of this, the State must carefully consider the risks and vulnerabilities of blockchain, and design controls to ensure that all users of the technology have mechanisms to appeal blockchain transactions in which the State is a participant until they are deemed secure enough to replace current practices. To the extent it is commercially reasonable to do so, operators of

applications serving the private sector should be encouraged to have similar appeal mechanisms.

### DETAILED RECOMMENDATIONS:

**1. Application-specific evaluation of risks and mitigations**. 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 and secure designs. Every class of application will present different priorities that may require trade-offs. The appropriate blockchain architectures should be used for different application contexts to manage financial and operational risk.

For example, 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 may be 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.

An important challenge will be striking the right balance between: (i) having sufficient diversity to limit the risk of a single large-scale security event; and (ii) keeping the total number of blockchains the State participates in manageable from a security perspective. The latter is an important consideration in an environment in which the pool of qualified personnel to provide security oversight, audit, and similar functions is limited.

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. 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 may create an environment for continued systemic breaches, which may exacerbate losses to consumers. An important consideration here is that any such regulation be introduced in a way that is *technology-neutral*, i.e., does not disadvantage blockchain technology relative to legacy technologies and thereby delay the introduction of this promising new technology. So, for example, if new security regulations are

enacted they should, to the extent feasible, apply equal to traditional database technologies and not only to blockchain.

Transparency, e.g., precipitating public disclosures of key information, is an alternative to traditional regulation that regulators have used to encourage desirable behaviours related to some aspects of the Internet industry. Where transparency of information serves a public good, government leaders must make considered decisions to find the right balance.

**2. Encourage training and potential certification of blockchain developers**. The State of CA should create training policies and standards to govern the use and control of blockchain utilizing industry expertise and other worldwide standards. The State of California should encourage certifying the workforce of blockchain developers through working with industry and academic partners to develop institution-based curricula or professional development programs. The State's educational systems should convene a panel of application development experts from academia and industry to define an appropriate curriculum and explore certification.

**3. Create policies and standards in accordance with industry-wide practice.** To enable the State to make objective risk-management decisions with respect to blockchain application security, the State should be guided by best practices and guidance emerging from internationally recognized standards bodies.

The following may be considered for adoption:

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

> **A. Eliminate *weak authentication technology***: One possible solution is the use of public-key cryptography. 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.
>
> **B. 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. For example: 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.

**C. 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.

**D. 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. Reasonable efforts and industry practices should be taken to validate and preserve the accuracy of the data through all stages of importing, updating or deleting records on the blockchain.

**E. Consider using 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).

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

**F. Work with cloud computing providers, if appropriate, to ensure operational security.** Cloud computing presents many opportunities for alternative deployment strategies for IT systems, as well as challenges for traditional notions of data security. For example, if moving data and computing from "on-premises" applications to the cloud, ensure that

appropriate cryptographic controls are available and in place for blockchain applications.

**4. Convene Blockchain Advisory Groups** representing security experts from academia and industry to advise California agencies considering blockchain implementations. 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, independent legal and privacy advisers, experts from industry and academia proficient in systems, application and cryptographic security
- Government representatives of existing systems-of-record (where public records are involved)
- Experienced regulators from other sectors such as construction, finance, utilities, etc.
- Representatives of the public who will be affected by the blockchain-based system

The Advisory Groups could 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 through a formal process of Request for Comments or other procedure.

## CONSIDERATIONS AND OPPORTUNITIES FOR BLOCKCHAIN APPLICATION

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.

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

On blockchain systems government data will remain permanently available for the public record. 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 process can be simple or burdensome 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.
- Given the newness of this technology, there is a tendency to equate all blockchain implementations with "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 security compromise is more likely if one or more of these defenses are not incorporated.

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 similar future breaches.

The field would benefit from regularly published blockchain Data Breach Forensic Reports, so that academia and the technology industry may learn from them and improve their designs and technology implementations. The cognizant State entity responsible for administering the data breach disclosure law should take steps to encourage and, if necessary, require the disclosure of Forensic Reports for all significant data breaches covered by the law, including those in blockchain platforms.

**Adopt an experimental period** for permissionless blockchain applications**.** 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, when implementations of blockchain-based *systems of record* are restricted to only private and/or permissioned blockchains, under the State's authority, 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 avoid sole reliance on public, permissionless blockchains.

Initial experiments with permissionless blockchains might, for example, involve their use as secondary sources for validation of information in the Registry of Births, Deaths and Marriages, or the registration of Business Entities, where information is public by law. During such experimental periods the relevant State agencies would ensure that, in the event of a conflict, existing systems-of-record will be the primary authority. This will enable the State to enter the field cautiously and learn from its experience before taking bolder steps.

## IV.E. PRIVACY INFRASTRUCTURE

### KEY RECOMMENDATIONS

**REC IV.E.1.** In light of the California Consumer Privacy Act (CCPA) and pending California Privacy Rights Act (CPRA), California has a strong privacy-protecting legal regime and its privacy laws need not be amended to enable adoption of blockchain technologies and use cases. Although blockchain is a new technological solution, it does not change the fundamental privacy rights to which individuals are entitled.

**REC IV.E.2.** The legislature should continue to monitor pending legislation for potential new issues with blockchain applications related to protecting individuals' privacy that are not addressed by technical measures or the existing regulatory framework.

**REC IV.E.3.** Additional education about how to use blockchain in a privacy-compliant and enhancing way is needed. If adopted, CPRA would establish a new California Privacy Protection Agency. If that happens, 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. If 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 is a leader on privacy protections, having adopted the nation's first comprehensive privacy law, the California Consumer Privacy Act (CCPA). A ballot initiative to amend CCPA, the California Privacy and Enforcement Rights Act, will be on the November 2020 ballot.[21] 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

[21] 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.

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).[22] These Principles define the framework of modern privacy regulation not only in California but elsewhere around the world, most notably the European Union's General Data Protection Regulation (GDPR).[23]

**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[24] and the report from the French Commission Nationale de l'Informatique et des Libertés (CNIL, the French data protection authority), Solutions for a Responsible Use of the Blockchain in the Context of Personal Data.[25] Important critiques of the state of privacy compliance of blockchain solutions have also been published.[26]

**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



[22] "The OECD Privacy Framework." *Organisation for Economic Co-operation and Development*, 2013. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
[23] Albert, Jason. "U.S. Privacy Law: A Short History." *Self-Published,* 2018. https://www.linkedin.com/pulse/us-privacy- law-short-history-jason-albert/.
[24] "Blockchain and the GDPR." *European Union Blockchain Observatory and Forum*, 2018. https://www.eublockchainforum.eu/reports.
[25] "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*, 2018. https://www.cnil.fr/en/blockchain-and-gdpr- solutions-responsible-use-blockchain-context-personal-data.
[26] Reneiris, Elizabeth. "Forget erasure: why blockchain is really incompatible with the GDPR." *Medium,* 2019. https://medium.com/berkman-klein-center/forget-erasure-why-blockchain-is-really-incompatible-with-the-gdpr.

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."[27] 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 may be 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.

The article 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. It 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.

[27] Reneiris, "Forget erasure," *Medium*, 2019.

Several commentators have suggested that this means blockchain is incompatible with laws such as GDPR that provide rights of rectification and deletion.[7] 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 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 technically impossible to "delete" information stored on the blockchain. Although definitive guidance would be helpful, the following 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 the 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, 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, whether participants are controllers or processors 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 would 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 CNIL. However, if the consortium members write data to the blockchain for a common purpose, they could be considered joint controllers. Also, per the CNIL guidance, it is possible for companies writing to the blockchain to designate a single entity to be the controller 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.

**Permissionless blockchains.** For permissionless or decentralized ledgers, the question of who is a controller poses more of an issue. In general, where good data privacy hygiene is observed, this issue 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 whether 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.[28] This clearly is the implication of the CNIL guidance.

**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 any consortium agreement.[29] 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

[28] 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).
[29] 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).

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.

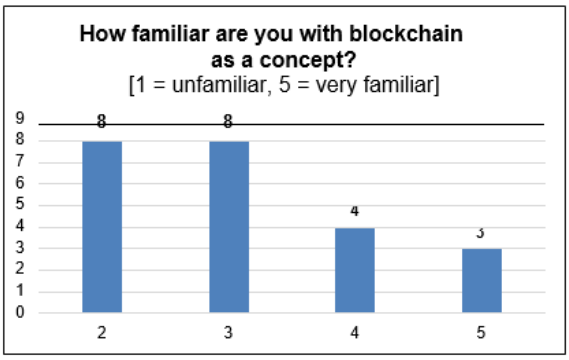
## IV.F. State Chief Information Officers' Perspective

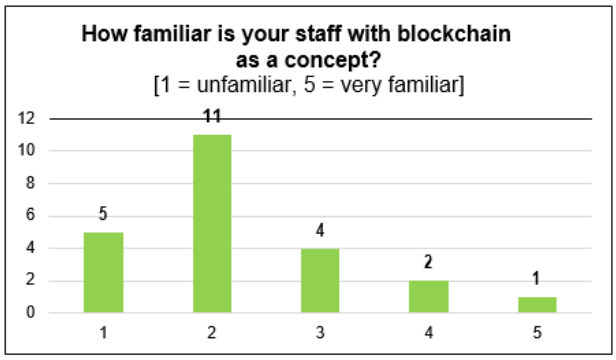
When thinking about adopting and maintaining new technology, the State of California carefully considers the application, how it will affect its end users, potential changes in policies and capacity to implement. Generally, technology is applied to a specific problem rather than considering an application first and then identifying the problems that it may solve.

### California Blockchain Technology Survey Results

The Blockchain Working Group, in coordination with the California Department of Technology, sent a survey in January 2020 to state Chief Information Officers to gain a better understanding of their familiarity with blockchain technology and assess interest for potential use cases. Twenty-three responses were received, and the information below highlights some of the key findings on the state's readiness for blockchain deployment.

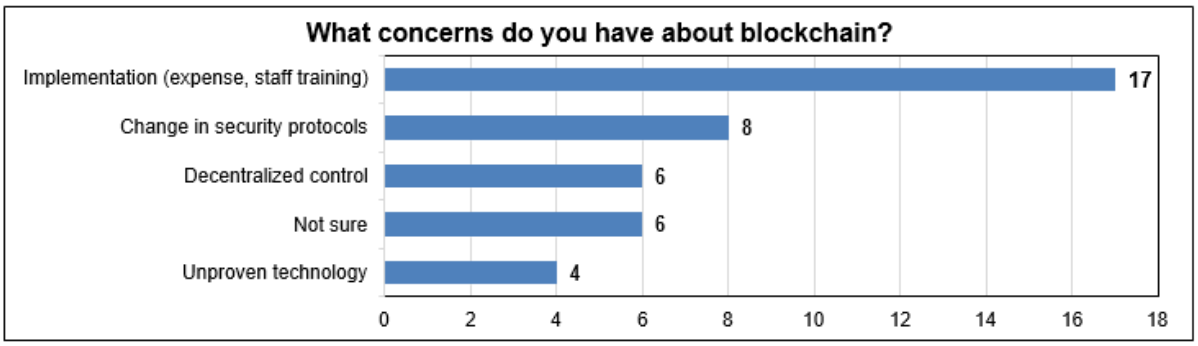
Most CIOs reported having little familiarity with blockchain technology:

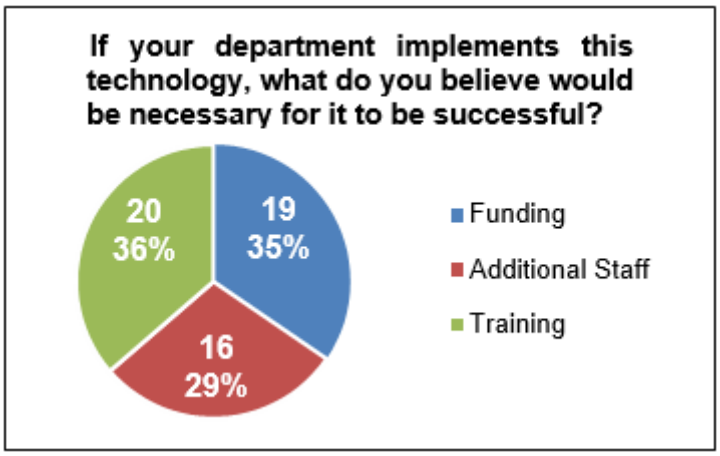


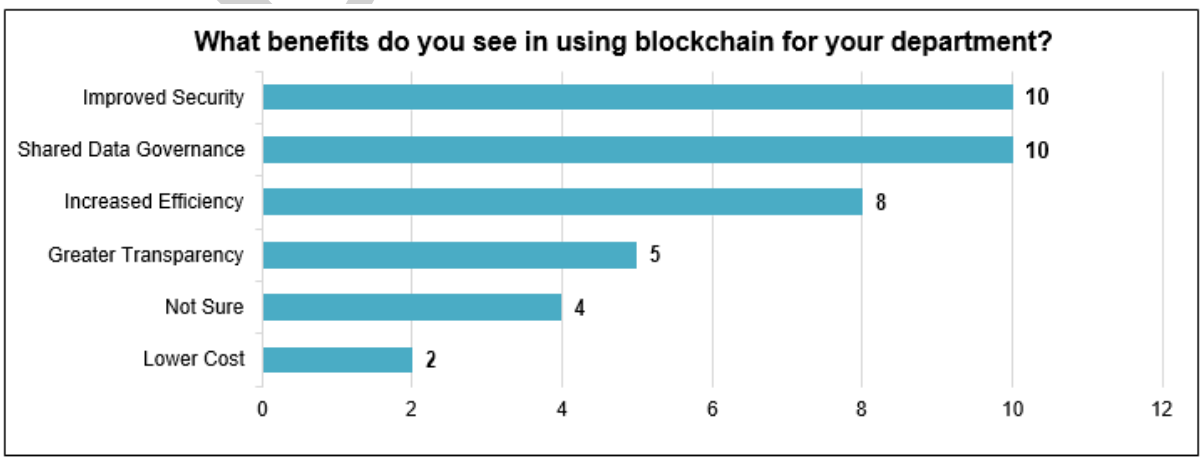

Respondents also shared what concerned them most about blockchain. A majority listed implementation as their top concern when thinking about

blockchain technology followed by change in security protocols. Implementation can include how expensive the process will be and the lack of resources available. Respondents stated that additional funding, staff and training would be necessary to successfully implement blockchain:




Despite these uncertainties, respondents have shown interest in exploring how blockchain could be used in their areas to improve current processes. Most agreed that improved security and shared data governance was an added benefit of blockchain technology.



Overall, the Blockchain Working Group learned that state agencies are not typically early adopters of new technology and prefer a cautious approach, especially when a new process has the potential to disrupt public services. Respondents have leaned toward seeking additional research on blockchain technology before moving forward.

**Considerations for Adoption**

In considering blockchain for adoption and use in State Government, as with any new technology, certain factors must be evaluated. Factors like procurement vehicles and overall cost; availability of training, knowledge and resources; compatibility with existing and future state architectures; ease of deployment and administration; security, data privacy and retention, and accessibility compliance; ability to meet established productive in-use requirements; as well as public and private support models and structures. These factors coupled with a well-defined business case outlining the need and potential advantages over existing solutions (more cost effective or efficient) will determine whether an application may be adopted in State Government.

**The Project Approval Lifecycle (PAL)**

State of California departments have adopted the California Department of Technology's Project Approval Lifecycle. The Project Approval Lifecycle (PAL) is intended to ensure projects are undertaken with clear business objectives, accurate costs and realistic schedules. PAL is a stage/gate model that focuses on four key areas: Business Analysis, IT Alternative Analysis, IT Solution Development, and Project Initiation/Approval.

Each stage consists of a set of prescribed, cross-functional, and parallel activities to develop deliverables used as the inputs for the next gate. The gates provide a series of "go/no go" decision points that request only the necessary and known information needed to make sound decisions for that particular point in time. As additional information is collected and refined through the lifecycle, cost estimates, schedules and business objectives will be progressively evaluated to determine if the project is still practical and if the investment should continue.

This stage/gate process assists departments in reducing project risk, ultimately leading to more successful projects. Risk tracking and reduction are key

components of the project approval lifecycle. Indeed, the likelihood of increased risk is a primary reason why State of California departments are not early adopters of technology. The preference when selecting technology improvements is for solutions that have been proven and previously used in similar business cases. Avoiding bleeding-edge technology until it has become mainstream allows departments to avoid missteps and pitfalls that at times accompany this type of technology. These potential missteps not only increase project risks but increase projects costs as well. As good stewards of California tax dollars the preference is for low-risk, low-cost, high-value solutions that have matured to the point that successful outcomes for our customers, stakeholders, and the public are likely.