BLOCKCHAIN IN CALIFORNIA: A ROADMAP

CALIFORNIA
BLOCKCHAIN WORKING GROUP

July 1, 2020

California Blockchain Working Group
Members

Chair of the Blockchain Working Group

Camille Crittenden,
CITRIS and the Banatao Institute, University of California

Three appointees from the technology industry

Brian Behlendorf, Linux Foundation
Audrey Chaing, Blockchaing
David Tennenhouse, VMware

Three appointees from the non-technology-related industry

Ben Bartlett, Berkeley City Councilmember
Meredith Lee, West Big Data Innovation Hub
Anne Neville-Bonilla, California State Library

Three appointees with a background in law chosen in consultation with the Judicial Council

Jason Albert, Workday
Liz Chien, Ripple Labs Inc.
Michele Neitz, Golden Gate University School of Law

Two appointees from privacy organizations

Arshad Noor, StrongKey
Sheila Warren, World Economic Forum

Two appointees from consumer organizations*

Radhika Iyengar-Emens, DoubleNova Group

The State Chief Information Officer

Amy Tong, California Department of Technology

The Director of Finance

Keely Bosler, Department of Finance
Ted Ryan, designee

The Chief Information Officers of three other state agencies

Benjamin Bonte, Department of Industrial Relations
Sergio Gutierrez, California Environmental Protection Agency
Kem Musgrove, Franchise Tax Board

One member of the Senate

Senator Robert M. Hertzberg
Freddie Quintana, Office of Senator Robert M. Hertzberg
Cynthia Castillo, Office of Senator Robert M. Hertzberg
Charles Loudon, Office of Senator Robert M. Hertzberg

One member of the Assembly

Assemblymember Ian Calderon
Voleck Taing, Office of Assemblymember Ian Calderon
Michael Magee, Office of Assemblymember Ian Calderon

*Contributions were provided by Kai Stinchcombe who withdrew before the completion of this report.

Table of Contents

Introductory Letter

To the Members of the California Legislature:

As Chair of the Blockchain Working Group, it is my pleasure to submit the Group's report for your review. The report fulfills the charge established by AB 2658 (Calderon) and represents a significant step in analyzing the potential uses, risks and benefits of blockchain technology in state government and for businesses operating in California.

It was my privilege to lead a diverse 21-member group representing multiple disciplines, which developed a comprehensive report that includes feedback from many stakeholders, including industry groups, academic experts, public sector leaders, and the broader public. The Working Group investigated a range of topics and potential applications, from public vital records and personal health records to supply chain and educational credentials. Although leaders throughout California State government were consulted and the Government Operations Agency championed the process and provided logistical support, the Working Group operated as an independent body. The ideas contained in the report are those of the Working Group and do not necessarily reflect administration policies. Any consideration of adopting blockchain by government entities in California should include conversations about the risks and benefits of blockchain to the people of California—not just government—and ensure that clear communications about benefits, such as privacy and control over personal data, are communicated clearly as well as any risks.

After a year of research and discussions, the Working Group has identified three recommended pilots for your consideration:

Department of Motor Vehicles
The Department of Motor Vehicles (DMV) identified three candidates for pilots in which blockchain technology could improve its current processes. These included creating a digital wallet for individual identification, building a common blockchain platform for tracking a vehicle's lifecycle, and creating a fine-grained security structure for sharing driver records across states. For the moment, DMV has put this project on hold to focus on the State's response to the COVID-19 pandemic.

The Department of Food and Agriculture

The California Department of Food and Agriculture could pilot the use of blockchain technology to more quickly trace the source of food-borne contamination by collecting and organizing data from growers, transporters, wholesalers and retailers to locate products in the distribution system to speed recall and consumer notification. Leaders from this office (CDFA) have expressed interest in developing a pilot, working with the agricultural industry, to increase transparency in the food supply using blockchain.

The Secretary of State's State Archives Division

The California Legislature could work with the Secretary of State leadership to determine how best to move the State Archives online with blockchain technology. A blockchain platform would increase accessibility and storage capacity for the hundreds of documents State agencies generate each year that the State Archives are charged with preserving. This use case provides for a relatively low-risk pilot project with large potential benefits.

In accordance with its charge, the Working Group established a definition of blockchain that will clarify discussions about it and its uses as decision makers explore various potential applications of this new technology:

> Blockchain is a domain of technology used to build decentralized systems that increase the verifiability of data shared among a group of participants that may not have a pre-existing trust relationship.
>
> Any such system must include one or more "distributed ledgers," specialized datastores that provide a mathematically verifiable ordering of transactions recorded in the datastore. It may also include "smart contracts," that allow participants to automate pre-agreed business processes. These smart contracts are implemented by embedding software in transactions recorded in the datastore.

Finally, the report discusses considerations for the appropriate application of blockchain, including a decision matrix to assess whether the technology is a good fit for a given problem, taking into account technology considerations and ethical dimensions. The Working Group evaluates and provides recommendations on potential application areas for blockchain deployment and the role that state government should consider.

Blockchain technology is not without its skeptics, some of whom shared their views with the Working Group. The technology will have to prove itself in rigorous evaluations of its application, and for government agencies to adopt it at any real scale, demonstrate its superiority to existing technology. State dollars, representing taxpayer money, are scarce, and development of new platforms must provide a clear return on investment.

Thank you for your time and consideration of these recommendations. On behalf of the blockchain working group, we are pleased to support California's leadership to create effective policy and guidelines for the development of this emerging technology.

Sincerely,

Camille Crittenden

Camille Crittenden, PhD
Chair, Blockchain Working Group

I. Executive Summary + Recommendations

I. Executive Summary and Recommendations

Blockchain technology has captured the attention of individuals far beyond the circles of computer scientists and cryptocurrency enthusiasts that initially sparked its development. The themes of distributed authority, decentralized governance, self-sovereign identity, and data privacy appeal to those who favor reducing hierarchy and increasing personal agency. The field has evolved in recent years to explore applications in the public sector and in private enterprise where regulation is a consideration.

As a state that is home to many innovative technology companies both big and small, as well as progressive voters and their representatives, California is well suited to investigate this intersecting space between new technology like blockchain and its potential application in the public sector.

Assemblymember Ian Calderon set out to do just that when he introduced Assembly Bill 2658, which established the Blockchain Working Group and its charge:

1. Define the term blockchain
2. Evaluate blockchain uses, risks, benefits, legal implications, and best practices
3. Recommend amendments to other statutes that may be affected by the deployment of blockchain

Three pilot projects have emerged as near-term opportunities for testing the effectiveness of blockchain applications within California State government.

Department of Motor Vehicles

The Department of Motor Vehicles (DMV) identified three candidates for pilots in which blockchain technology potentially could improve its current processes. These included creating a digital wallet as a persistent form of digital identification, building a common blockchain platform for tracking a vehicle's lifecycle and creating a fine-grained security structure around sharing driver records across states. For the moment, DMV has put this research on hold to focus on the State's response to the COVID-19 pandemic but will be well positioned and eager to resume discussions about a potential use case in the near future.

The Department of Food and Agriculture

The California Department of Food and Agriculture (CDFA) could pilot the use of blockchain technology to more quickly trace the source of food-borne contamination by collecting and organizing data from growers, transporters, wholesalers and retailers to find where the products are in the distribution system to speed recall and consumer notification. Leaders from this office have expressed interest in developing a pilot, working with the agricultural industry, to increase transparency in the food supply using blockchain.

The Secretary of State's State Archives Division

The California Legislature could work with the Secretary of State leadership to determine how best to move the State Archives online with blockchain technology. A blockchain platform would increase accessibility and storage capacity for the hundreds of documents State agencies generate each year that the State Archives are charged with preserving. This use case provides for a relatively low-risk pilot project with large potential benefits.

Below is a summary of the Blockchain Working Group's key recommendations. Full analyses and explanations of the recommendations are provided in the report.

Blockchain Definition

"Blockchain" is a domain of technology used to build decentralized systems that increase the verifiability of data shared among a group of participants that may not necessarily have a pre-existing trust relationship.

Any such system must include one or more "distributed ledgers," specialized datastores that provide a mathematically verifiable ordering of transactions recorded in the datastore. It may also include "smart contracts" that allow participants to automate pre-agreed business processes. These smart contracts are implemented by embedding software in transactions recorded in the datastore.

Evaluation of Blockchain and Appropriate Uses

A Framework for Assessing the Fitness of Blockchain Technology

REC IV.A.1. The Working Group recommends the use of a decision matrix to evaluate the suitability of blockchain for a given application by considering the questions provided in the diagram in Chapter IV. Special attention is given to ethical considerations, digital identity, cybersecurity, and privacy.

Ethical Considerations

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.

Digital Identity

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**. 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 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.

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.

Cybersecurity and Risk Management

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 **Blockchain Advisory Groups** across relevant State Agencies composed of experts from academia and industry.

REC IV.D.5. Consider establishing a **Security Review Board**.

REC IV.D.6. Require publication of **Data Breach Forensic Reports**, as needed.

Privacy Infrastructure

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.

Potential Application Areas

Working Group members considered the potential for blockchain application across multiple government functions including vital and health records, supply chain, property and titles, utilities and natural resources, finance, and education and workforce.

Vital Records

REC V.A.1. The State should consider using blockchain technology to create and verify tamper-resistant digital certificates of **government-issued documents**.

REC V.A.2. New legislation should be considered to amend the **Health and Safety Code** sections 102400, 102430, and 103525 to include blockchain application.

Health Records

REC V.B.1 **Engage** with patient advocacy groups, health consortia, health systems, hospital CIOs, executives at payers, and blockchain-for-healthcare platforms to understand the viewpoints and technical considerations of all stakeholders. Such conversations should also include government agencies and related entities including the California Health & Human Services Agency, school districts and organizations that review immunization records, Centers for Disease Control, Immigration & Customs Enforcement, and the California Department of Food and Agriculture.

REC V.B.2 Develop a framework for providing patient identity and data operability. This will better equip those who want to address challenges of data fragmentation and silos, lack of cohesive patient identity and privacy, security vulnerabilities and a one-size-fits-all approach to health care delivery.

Supply Chain

REC V.C.1. Tracking Food Contamination. Work with the California Department of Food and Agriculture to establish a pilot to use blockchain technology, based on the successful experiences of IBM and Walmart, to collect and organize data from growers, transporters, wholesalers and retailers to more quickly trace the source of food-borne contamination and where the products are in the distribution system to speed recall and consumer notification. Explore the possibility of federal grant funding to support a California-based pilot.

REC V.C.2. Food Freshness. Explore the use of blockchain combined with IoT sensors and artificial intelligence to help growers better estimate product shelf life and optimize transportation and logistics to ensure that produce can be delivered to destinations within the shelf-life periods.

REC V.C.3. Small Farms. California policymakers could support small farms in their exploration of the use of blockchain technology by identifying opportunities for pilots for California's specialty crops and organic produce where "tip-the-farmer" initiatives could help increase margins and sustainability. California policymakers could also expand oversight of agricultural co-ops and evaluate opportunities to revise their accounting practices and operations using blockchain technology.

REC V.C.4. Cannabis Supply Chain. California policymakers could direct the California cannabis licensing authorities to accept blockchain-based verification and reporting mechanisms for the cannabis supply chain. This might require certifying specific blockchain projects that pass a set of standards for operation and authenticity. California policymakers also could consider authorizing participants in the cannabis supply chain to use payment mechanisms that implement stringent industry "know your customer" processes but also accommodate U.S. regulatory concerns.

REC V.C.5. Pharmaceuticals. Develop a pilot program that brings together a broad group of California partners, including state government, pharma manufacturers, distributors, retail pharmacies, technology companies, healthcare providers and payers, patient advocacy groups, universities and other research facilities. Similar to other consortia like MediLedger, it is recommended that a "California Pharma Consortium" includes distributors and retail pharmacies, to ensure that the "last mile" in the pharma supply chains are secured.

Property

REC V.D.1. Real Estate: Titling. Continue to monitor ongoing efforts for potential applications in land titling.

REC V.D.2. Real Estate: Licenses. Explore issuing real estate licenses on a blockchain system while continuing to run the existing process in parallel until a new system is proven.

REC V.D.3. Real Estate: Fraud Detection, Efficiencies. To the extent that emerging technologies have the potential to make title search, record validation, or detection of error or fraud cheaper, faster, or more accurate, encourage counties to consider blockchain technologies and to be forthcoming in providing technologists the data they need; encourage lenders, title insurers, and other private-sector actors to adopt efficient new technologies; encourage new players to enter the space; encourage governments and regulators to provide a level playing field and remove barriers; and encourage all parties to pass savings on to the end user.

REC V.D.4. Real Estate: Vendors and Procurement. Allow vendors to describe the system they can build and the costs, let them choose the underlying technologies to employ, and let the State's procurement officials select the most competitive bid.

REC V.D.5. Vehicles and Parts. Further investigation is needed to identify whether there are specific regulatory barriers to applying blockchain technology to use cases in vehicles and parts. None are known at this time.

REC V.D.6. Vehicles and Parts: License Registration. Discussions with the Department of Motor Vehicles should continue to determine whether registration of motor vehicle operators is an appropriate use case for blockchain technology.

REC V.D.7. Property Insurance. Since streamlining insurer operations could have significant benefits for constituents in terms of pricing, access, and convenience, the state should encourage private industry to adopt blockchain technology as appropriate. California should also keep an open dialogue with industry to advance legislation and policies that might encourage and enable benefits to the consumer while minimizing potential risks such as potential loss of privacy.

REC V.D.8. Firearms. Although blockchain technology may find applications in firearms-related data in California, no opportunities have presented themselves at this time.

Utilities and Natural Resources

REC V.E.1. Energy Sector. Additional discussion and research are required to determine whether the concept of a "regulatory sandbox" is feasible in California

REC V.E.2. Water Sector. The State should evaluate the opportunity for blockchain-based technology to support a more efficient framework that further leverages the momentum from recent California water data efforts. Addressing the needs of different stakeholders to control and monitor how they responsibly share water data could enhance the efficiency of regulatory efforts, support more transparent decision-making, and ultimately, increase trust among stakeholders.

Finance, Payments, and Commercial Business

REC V.F.1. Welfare and Entitlement Programs. Any pilots should be done at a small scale that will not negatively affect vulnerable populations who rely on these services. To our knowledge, blockchain has not yet been used for entitlements, welfare, or social benefits by any government in the United States.

REC V.F.2. Taxes and Revenue. Evaluate and study the potential for blockchain application to better administer, collect, and detect fraud related to sales and use taxes.

REC V.F.3. Bonds and Public Finance. Research blockchain-based digital municipal bond issuance programs and the creation of a consortium to manage negotiation of bond issuance fees for the State of California. These universal fees would be implemented via blockchain.

REC V.F.4. Public Banking. The State of California should monitor developments in public banking and potential opportunities to integrate blockchain technology.

REC V.F.5. Digital Asset Banks. Define a framework for Special Purpose Depository Institutions (SPDI), and subsequently grant existing banks a charter to bank Digital Assets would enable greater monetization and overall growth of these new technologies.

REC V.F.6. Cannabis and Banking. California should explore the use of 1) public banks; 2) digital asset deposit and custodial institutions; and 3) a regulatory sandbox for blockchain and cannabis innovators.

REC V.F.7. Government Role in Remittances. The State has a limited role in the remittance market; no recommendations at this time.

Civic Participation

REC V.G.1. State Archives. The Secretary of State's State Archives Division would be an effective first blockchain pilot project. The Division should gather input from stakeholders and consider issuing a Request for Information to help outline the scope of the project and required budget. If indicated, the California legislature should work with the Secretary of State leadership to determine how best to move the State Archives online with blockchain technology.

REC V.G.2. Business Programs. The Secretary of State's business programs section may be a potential use case in the future, as the Secretary of State's employees deploy a new technology when developing future modules for the new portal.

REC V.G.3. Internet Voting. Security experts generally agree that internet-based implementations of voting systems, blockchain or otherwise, have not overcome security challenges. In applications to date, blockchain-based systems rely on factors other than blockchain, such as centralized voter databases, facial ID or postal delivery, cryptographic mixing, dual-device vote validation, etc., to solve these problems. Those experimenting with new voting technologies in California are encouraged to evaluate the quality of these solutions as a whole, rather than rely on a specific technology.

Education and Workforce

REC V.H.1. California should emphasize **interoperability, security, and scalability** when piloting the use of blockchain for education and workforce records.

REC V.H.2. The **Future of Work Commission** should adopt recommendations on skills-based hiring and credentials, ensuring workers have the means to control and electronically share credentials in a secure and verifiable manner.

REC V.H.3. The State should enable and facilitate a results-focused **forum for technology demonstrations** that advance public sector applications, leveraging opportunities to re-use, re-purpose, and build upon existing efforts.

REC V.H.4. The State should develop a framework of **key questions, considerations, and paths forward** for groups interacting with the California public school system and public service. Such a framework could help stakeholders identify blockchain-based pilot projects and serve as a public resource.

REC V.H.5. The State could encourage creative **"cross-pollination" from other sectors** and application areas by incentivizing and providing a safe space for transparent discussion of lessons learned and best practices. Illustrating the different phases of technology adoption, and encouraging discussion of risks, benefits, and "readiness levels" needed along the way will provide clarity for technology developers, policy writers, and solution adopters moving forward.

The Role of State Government

Working Group members considered the role of state government in ensuring appropriate application of blockchain to promote State government effectiveness, efficiency, and transparency.

REC VI.1. Consider establishing a **Blockchain Innovation Zone** to incentivize and provide safe harbor to blockchain companies working to solve California's most pressing problems.

REC VI.2. Foster collaboration through supporting a multi-stakeholder advisory group to promote best practices that would include government regulatory agencies, consumer advocacy groups and other industry stakeholders.

REC VI.3. Create a unit within the **California Department of Technology** to monitor developments in the blockchain industry. Possible responsibilities for this unit include:

i. Monitoring and reporting any consumer protection issues.

ii. Train the IT workforce within government agencies.

iii. Working with the state legislature and local governments to create flexible and adaptive regulations.

iv. Attending or hosting conferences to encourage responsible blockchain business development in California.

v. Arranging community education programs to teach more Californians about consumer protective measures related to blockchain and ensure that laws are adaptive to changes in the industry.

REC VI.4. Blockchain definition. The Legislature should adopt an accurate, concise definition of blockchain, such as that proposed in this report. With this agreement, policymakers can turn to two questions: 1) How can blockchain be used to increase efficiency? and 2) What changes to state laws and regulations will be needed to implement the new technology?

REC VI.5. Neutral terminology. Adopt technology-neutral terminology to expand use cases for blockchain.

II. Legislative Charge + Working Group Process

II. Introduction

Legislative Charge and Statement of Need

Blockchain has been a topic of discussion among state governments searching for technologies that will increase government efficiency and boost transparency. Advocates have touted blockchain as a means to save money, accelerate processes and increase security. Although blockchain is often associated with cryptocurrencies such as Bitcoin, its potential reaches beyond financial technologies to applications of "smart contracts" or other use cases requiring authenticated distributed records, including title and property records, identity authentication, supply chains, international remittances and more.

Amid growing interest for potential use cases from the public and private sector, California began to explore the use and regulation of blockchain technology for California government transactions, its businesses and residents. **Assembly Bill 2658 (Calderon)** established the Blockchain Working Group and charged its members with submitting a report to the Legislature by July 2020. The report includes policy recommendations and evaluates potential uses, risks and benefits to state government and California-based business as well as amendments to existing law that may be affected by the deployment of blockchain technology.

Working Group Process

The California Government Operations Agency (GovOps) created an internal advisory group to establish a process for soliciting nominations (including self-nominations) and to review and consider candidates who had applied or been nominated. Several categories of representatives were established in the legislation, to ensure a group balanced among representatives from the private sector, privacy advocates, government IT leaders and others. The advisory group sought to assemble a group that would offer diverse backgrounds, expertise, and opinions with a balanced range of perspectives. The Governor's Office provided additional advice and feedback during this selection process.

The 21-member Working Group represents members from multiple disciplines.

Experts in technology, business, law, government, public policy and information security were key in conducting a comprehensive evaluation.

California State University, Sacramento (CSUS) - Consensus and Collaboration Program was contracted by GovOps to provide facilitation support for the Working Group.

Assessment interviews. The CSUS facilitator conducted 1-hour phone interviews with each of the Working Group members and chairperson to gather information on the following:

1. Members' perspective and expectations regarding their participation, decision-making process, and overall engagement.

2. Members' initial thoughts on blockchain definition, criteria for identifying appropriate applications, and potential use cases for further research and analysis.

Information gathered through the interviews informed the Working Group meeting agendas and the development of the report's topics.

Working Group meetings. The full Working Group met seven times between September 2019 and June 2020. Members volunteered to conduct research and present information on each of the report topics. During the Working Group meetings key issues were discussed to refine the content and inform the recommendations found in this report.

Subcommittee meetings. The Working Group voted to form two subcommittees (1) the finance subcommittee and (2) the regulatory subcommittee, recognizing the complexity of these two topics. The finance subcommittee met twice and the regulatory met once to discuss related topics and then reported their conclusions and recommendations to the Working Group for further discussion.

Public comment. As part of the Working Group process, members of the public were invited to provide input and feedback on topics discussed during the Working Group meetings. Members of the public provided information and additional resources to advance the conversation on blockchain technology, promising regulatory guidelines, and considerations related to potential risks, benefits and uses in state government. Over 150 public comments were received via Zoom Chat/phone (85), in-person (19), emails to GovOps staff (20), and through a website survey (32).

The website survey invited public comment on the following questions:

1. What opportunities or constraints should policymakers keep in mind when crafting legislation regarding blockchain? Perspectives could address technical, economic, social, environmental or other concerns.

2. Considering potential application areas, which sectors or cross-cutting applications may be well suited to adopt blockchain solutions? Which areas will need further technological or infrastructure development or regulatory changes before a blockchain framework could be implemented? Which, if any, sectors should NOT be considered for incorporating blockchain technology?

3. How can the state improve civic literacy regarding blockchain technology? What examples of successful user interfaces should the Working Group consider as models?

4. Provide contact information for follow-up as needed.

A summary of comments provided through the website public survey is provided in Appendix VIII.

Information Technology staff survey. The Blockchain Working Group, in coordination with the California Department of Technology, sent a survey in January 2020 to state employees working in information technology (IT) to gain a better understanding of their familiarity with blockchain technology and assess interest for potential use cases. A summary of responses to the survey is provided in Chapter 4 of this report (Considerations for Appropriate Applications).

III. Blockchain: Defining Characteristics

III. A Definition of Blockchain and its Defining Characteristics

Part of the charge of the founding legislation for the Blockchain Working Group (AB 2658) is to establish a definition of blockchain. The Working Group agreed it was important to define "blockchain" in such a way that it helps the State make policy with clarity and precision. It should focus policymakers and the public on the most unique value that the technology can deliver. It should be accessible to and understandable by the public, and yet technically specific enough to ensure that the State can reap maximum benefit. At the same time, it does not need to be adopted wholesale but rather can be considered a starting point to be customized as needed in specific contexts, such as when drafting legislation.

After much discussion, the Working Group arrived at the following definition:

> "Blockchain" is a domain of technology used to build decentralized systems that increase the verifiability of data shared among a group of participants that may not necessarily have a pre-existing trust relationship.
>
> Any such system must include one or more "distributed ledgers," specialized datastores that provide a mathematically verifiable ordering of transactions recorded in the datastore. It may also include "smart contracts" that allow participants to automate pre-agreed business processes. These smart contracts are implemented by embedding software in transactions recorded in the datastore.

Blockchain technology is the most widely recognized approach to building co-operative, auditable, multi-stakeholder information systems that avoid the need for a single organization to operate and own the center of the datastore. The intent of this is to bring increased trust, transparency and/or disintermediation in the overall system. This has positive implications for government roles in market regulation, permit issuance processes, identity management, and many more use cases. Through blockchain technology, California can pursue a highly agile approach to enabling California's businesses and residents to participate in the digital economy.

The literature on blockchain technology is vast and growing. The Working Group chose to focus on a functional description, in order to recognize and empower a wide array of implementation paths.

As in most technology policy domains, but particularly in the application of this technology, it is crucial to avoid vendor lock-in. As in these other domains, the use of open standards and/or open-source software is preferred wherever available and suitable. Fortunately, these are widespread characteristics in the blockchain ecosystem.

We recognize that nearly any use case for blockchain technology can be implemented using a centralized datastore. And by most objective technical metrics—speed, throughput, cost, ease of update—a centralized data store will be superior to using a blockchain to store the same data. But the unstated assumption in any such comparison is that a central data store can be trusted, that it can be operated by an organization or human beyond reproach, perfect in their ability to resist the temptation to adjust the ledger or provide access in unequal ways. The only reason to use blockchain technology to solve a problem is to avoid that dependency on single organizations or individuals to keep the system of record honest and accountable. This is especially important within a business context, where participants are likely to be highly competitive and constantly looking for arbitrage opportunities that centralization brings. The definition above is designed to reflect that essential advantage of blockchain technology.

This does not mean that all data written to a blockchain is “true,” trustworthy, or immediately verifiable. If someone writes to a blockchain ledger that the temperature on March 14 in Sacramento was 102 degrees, nothing about blockchain technology leads to a conclusion that this is the truth. However, the blockchain ledger will show us, verifiably, who recorded that temperature, when they recorded it, everyone else who recorded a temperature, and any retraction of the statement, all in ways that provide high confidence that this history has not been corrupted. Whether the temperature in Sacramento was actually 102 degrees on March 14, this verification and complete history is important.

The social costs and security risks implied with centralized systems in social networking, ride-hailing, food delivery, e-commerce, and other applications become increasingly clear every day. Meanwhile our collective trust in institutions, corporations, and government to operate efficiently and in the interests of citizens is declining, as per the Edelman Trust Barometer. Blockchain technology cannot solve this by itself, but its appropriate application by the State of California has the potential for substantial positive impact.

Blockchain Technical Standards

There are a variety of organizations that have attempted to create standards for blockchain technologies or blockchain identity standards. We list a few of these blockchain standards associations below, though this list is not necessarily comprehensive. In addition, these standards change quickly, and developers should consult with experts to make sure they are utilizing the most up-to-date and methodologically sound protocols.

Bitcoin Improvement Proposals (BIP): BIPs are directly connected to current Bitcoin implementation. BIPs are open-source specifications where developers can propose changes to the Bitcoin protocol. These include consensus critical changes or process changes. BIPs can be accessed through GitHub.[1]

Ethereum Improvement Proposal (EIP): Similar to BIPs, EIPs are open-source proposals that are directly connected to current Ethereum implementation. EIPs describe standards for the Ethereum platform. Proposals can include core protocol specifications, client application program interfaces (APIs), and contract standards. EIPs can also be accessed through GitHub or through a website.[2]

The Enterprise Ethereum Alliance: The Enterprise Ethereum Alliance (EEA) is a member-driven standards organization whose charter is to develop blockchain standards that drive interoperability. The website includes the latest versions of their technical specifications.[3]

Decentralized Identity Foundation: The Decentralized Identity Foundation is a group of experts who are creating an open, standards-based, decentralized

[1] See https://en.bitcoinwiki.org/wiki/Bitcoin_Improvement_Proposals and https://github.com/bitcoin/bips.

[2] See https://eips.ethereum.org/ and https://github.com/ethereum/EIPs.

[3] See https://entethalliance.org/.

identity ecosystem. Their working groups are scoped by function areas, and include areas such as identifiers and discovery, and authentication.[4]

International Organization for Standardization: The International Organization for Standardization (ISO) is an international standards-setting body composed of representatives from various national organizations. It is currently developing standards for blockchain and distributed ledger technologies through the TC307 protocol.[5]

World Wide Web Consortium: The World Wide Web Consortium (W3C) is an international standards organization for the World Wide Web. It has been active in defining underlying blockchain technology standards. For example, the Decentralized Identifier model specifies a common data model and set of operations for decentralized identifiers.[6] The Verifiable Credentials model provides a standard way to express verifiable credentials on the Web in a manner that is secure, privacy-respecting, and machine-verifiable. [7]

GS1: GS1 is a non-profit that develops global standards for business and communication. Though they do not create blockchain-specific standards, they have been adapting their non-blockchain standards to be used in blockchain applications.

Global Legal Entity Identifier Foundation: The Global Legal Entity Identifier Foundation (GLEIF) provides trusted services and open, reliable data for unique legal entity identification. Like GSI1, GLEIF does not create blockchain-specific standards, but they have been adopting their non-blockchain standards for blockchain applications.

IEEE: The IEEE Standards Association, a globally recognized professional association that publishes technical standards on various technologies, has been actively pursuing blockchain standardization across various sectors.[8] However, as of the writing of this report, these standards have been developed in the absence of actual blockchain deployment.

[4] See https://identity.foundation/.

[5] See https://www.iso.org/committee/6266604.html.

[6] See https://www.w3.org/TR/did-core/.

[7] See https://www.w3.org/TR/vc-data-model/.

[8] "Standards," IEEE, Blockchain. https://blockchain.ieee.org/standards.

National Institute of Standards and Technology (NIST): An agency within the U.S. Department of Commerce, NIST has also begun standardization efforts. Similar to IEEE, these standards have been developed in the absence of actual blockchain deployment.[9]

Other organizations: A variety of other organizations have been involved in developing general guidelines or developing source code for blockchain use. This, for example, includes Hyperledger, which has published blockchain source code and software.[10]

[9] "Blockchain," National Institute for Standards and Technology. https://www.nist.gov/topics/blockchain. See also this report: Dylan Yaga et al. "Blockchain Technology Overview," NIST, October 2018. https://csrc.nist.gov/publications/detail/nistir/8202/final. And "Blockchain for Industrial Applications Community of Interest," NIST, November 2019. https://www.nist.gov/el/systems-integration-division-73400/blockchain-industrial-applications-community-interest.

[10] See https://www.hyperledger.org/join-a-group for more information on each of the working groups and special interest groups.

IV. Considerations for Appropriate Application

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.

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.

Standards

Basic Requirements For Using Digital Ledger Technology (DLT)

A Digitally native asset or convertible to digital format?

B Is a permanent record warranted, and can one be created?

C Is the information compatible with prevailing privacy regulations?

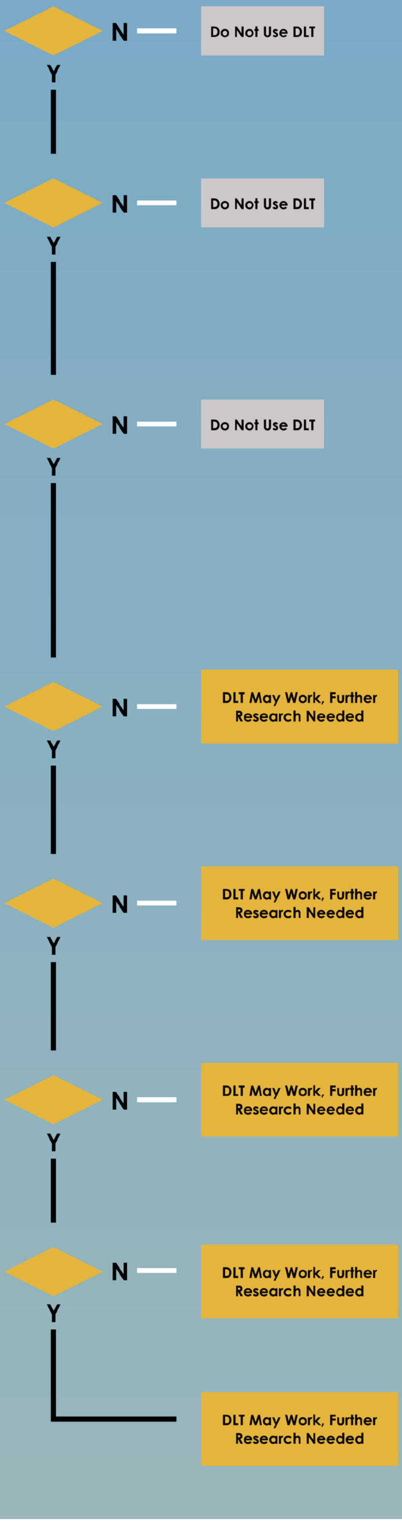
Additional Specifications

D Will the relevant regulators, if any, be willing and able to participate?

E Will the removal of an intermediary be helpful?

F Does the use case require shared read/write access?

G Do the relevant parties seek to create or enhance trust?



A: N — Do Not Use DLT; Y

B: N — Do Not Use DLT; Y

C: N — Do Not Use DLT; Y

D: N — DLT May Work, Further Research Needed; Y

E: N — DLT May Work, Further Research Needed; Y

F: N — DLT May Work, Further Research Needed; Y

G: N — DLT May Work, Further Research Needed; Y — DLT May Work, Further Research Needed

Contextual Details

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 If there are conflicting sources of trust regarding the state of an object, then the object cannot be effectively stored on the blockchain. If an unalterable record is not needed, then blockchain is not an appropriate solution.

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.

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?

F 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.

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 differing or conflicting 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. They must agree how the 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.[1]

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 an Ethical Blockchain 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.[2] A key principle to ethical guidance should be promoting a "culture of genuine responsibility" rather than a "culture of compliance."[3]

[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.

[2] For a discussion of risks, see Michele Benedetto Neitz, "The Influencers: Facebook's Libra, Pub-lic Blockchains, and the Ethical Considerations of Centralization," 21 *N.C.J.L & Tech* 27 (2019).

[3] Beard, Matt and Longstaff, Simon, "Ethical Principles for Technology," The Ethics Centre, Sydney (11), 2018. https://ethics.org.au/ethical-by-design/.

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.[4] 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.[5] 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.[6] 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 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.

[4] Beard and Longstaff, "Ethical Principles for Technology" (2018).

[5] 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.

[6] Beard and Longstaff, "Ethical Principles for Technology" (2018).

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.[7] 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 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

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

should work to create "a culture of cooperation and engagement between stakeholders."[8]

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 sustainability advocates in creative ways. For example, on a supply chain, enterprise blockchains could

[8] Mone, "Bias in Technology."

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 an item was produced, promoting corporate social responsibility.[9]

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.[10] 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."[11] When assessing the ethical implications of blockchain technology, California should abide by the following three principles:

[9] Rick LeBlanc, "How Blockchain Will Transform Supply Chain Sustainability," *Small Business*, 2020. https://www.thebalancesmb.com/blockchain-and-supply-chain-sustainability-4129740.

[10] See, e.g., "SEC Charges Issuer With Conducting $100 Million Unregistered ICO" (2019). https://www.sec.gov/news/press-release/2019-87.

[11] Beard and Longstaff, "Ethical Principles for Technology."

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?
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.

1. 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.[12]

2. 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 individuals interact with the government, whether applying for a license,

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

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.

Digital identity is critical not only for social benefits but also for many business transactions. However, many existing 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, many of which are provided by blockchain and are worth further study. 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.

1. **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.

2. **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.

3. **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[13]

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

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.

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

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.[14] 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

Self-sovereign identity based on blockchain is one promising digital identity approach. Blockchain is a key enabler of self-sovereign identity, but not because personal data (aspects of identity) are stored on the blockchain.[15] 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."[16] 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

[14] Decentralized Identity Foundation, available at https://identity.foundation/, and Decentralized Identifiers (DIDs) v1.0, available at https://www.w3.org/TR/did-core/.

[15] Alex Preukschat, "Self-Sovereign Identity—a guide to privacy for your digital identity with Blockchain," 2018. https://medium.com/@AlexPreukschat/self-sovereign-identity-a-guide-to-pri-vacy-for-your-digital-identity-5b9e95677778.

[16] Dan Gisolfi, "Self-sovereign identity: Why blockchain?" IBM, 2018. https://www.ibm.com/blogs/blockchain/2018/06/self-sovereign-identity-why-blockchain/.

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.

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.[17] 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 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.[18] 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.[19] 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.

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

[18] Verified.me: https://verified.me/.

[19] Trust Your Supplier: https://www.trustyoursupplier.com/.

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.[20] 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.[21] 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.

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.

[20] ID2020 Digital Identity Alliance: https://id2020.org/.

[21] Workday Credentials, Cloud Credentialing Management: https://www.workday.com/en-us/applications/credentials.html.

REC IV.D.4. Convene Blockchain Advisory Groups across relevant State Agencies composed of experts from academia and industry.

REC IV.D.5. Consider establishing a Security Review Board.

REC IV.D.6. Require publication of Data Breach Forensic Reports, as needed.

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.

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

5. Consider establishing a Security Review Board. A Security Review Board, comprising practicing application security experts, will help to establish guardrails for future blockchain development to highlight potential security vulnerabilities and learn from past breaches. Its mandate would be limited to applications of blockchain in the State of California and would complement but not replace the jurisdiction of civil or criminal courts. It 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.

6. Require publication of Data Breach Forensic Reports. 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, within California government agencies.

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, reduce the friction typically encountered in distributed database designs, and, because of the redundancy in the system, increase 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.

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.[22] 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).[23] 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).[24]

Literature Review

Quite a bit has been written on blockchain and privacy. With respect to the

[22] 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.

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

[24] Jason Albert, "U.S. Privacy Law: A Short History," Self-Published, 2018. https://www.linkedin.com/pulse/us-privacy- law-short-history-jason-albert/.

ability of blockchains to comply with GDPR, the two main reports are the EU Blockchain Observatory's report *Blockchain and the GDPR*[25] 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.*[26] Important critiques of the state of privacy compliance of blockchain solutions have also been published.[27]

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."[28] 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.

[25] "Blockchain and the GDPR," European Union Blockchain Observatory and Forum, 2018. https://www.eublockchainforum.eu/reports.

[26] "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.

[27] Elizabeth Reneiris, "Forget erasure: why blockchain is really incompatible with the GDPR," Medium, 2019. https://medium.com/berkman-klein-center/forget-erasure-why-blockchain-is-re-ally-incompatible-with-the-gdpr.

[28] Reneiris, "Forget erasure," Medium, 2019.

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.

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. As described above in the Digital Identity section, generally the only personal data that should be written to the blockchain is an individual's public key as part of their Decentralized Identifier. In that case, there are two ways to break the link between the individual and any personal data stored elsewhere. First, the individual 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. Alternatively, it might be possible to hash or encrypt the data rather than deleting it.

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." 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.[29] 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.[30] 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 by using multiple identifiers but with confirmation that they tie 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.

[29] 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).

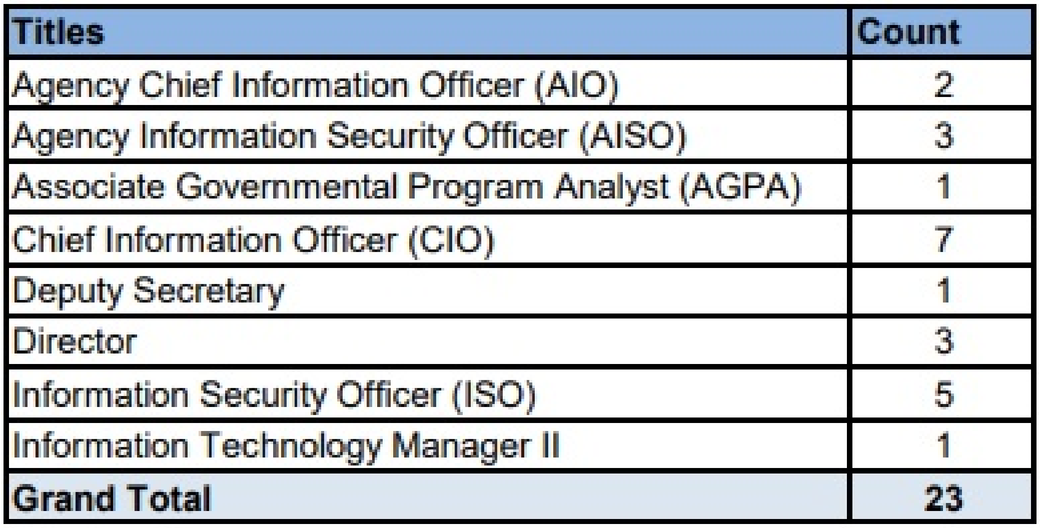
[30] Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (2010/87/EU).

IV.F. State Information Technology Staff Perspective on Blockchain

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 sought to address a specific problem rather than considering the technology and then identifying the problems it may be applied to.

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 employees working in information technology (IT) to gain a better understanding of their familiarity with blockchain technology and assess interest for potential use cases. Provided below is a list of the 23 participants who responded, according to job title:



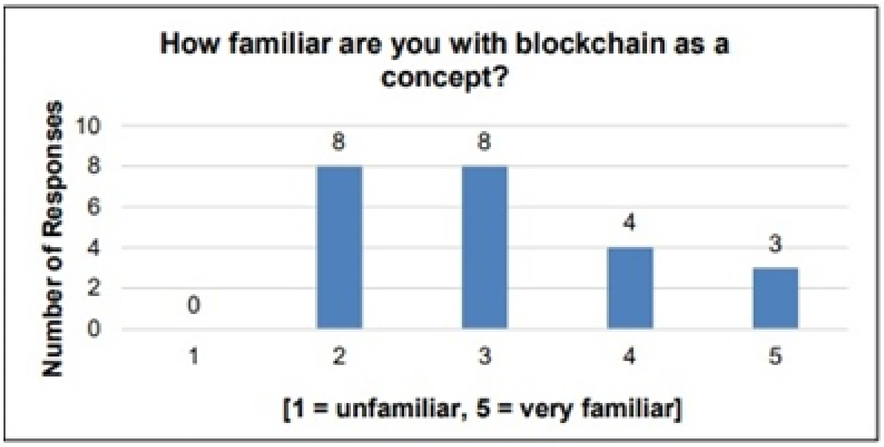
Titles	Count
Agency Chief Information Officer (AIO)	2
Agency Information Security Officer (AISO)	3
Associate Governmental Program Analyst (AGPA)	1
Chief Information Officer (CIO)	7
Deputy Secretary	1
Director	3
Information Security Officer (ISO)	5
Information Technology Manager II	1
Grand Total	**23**

Since respondents account for a small percentage of State IT employees, survey results may not be representative of overall understanding of blockchain technology and its potential application. The information below highlights some of the key findings on the State's readiness for blockchain deployment.

Familiarity with Blockchain Technology

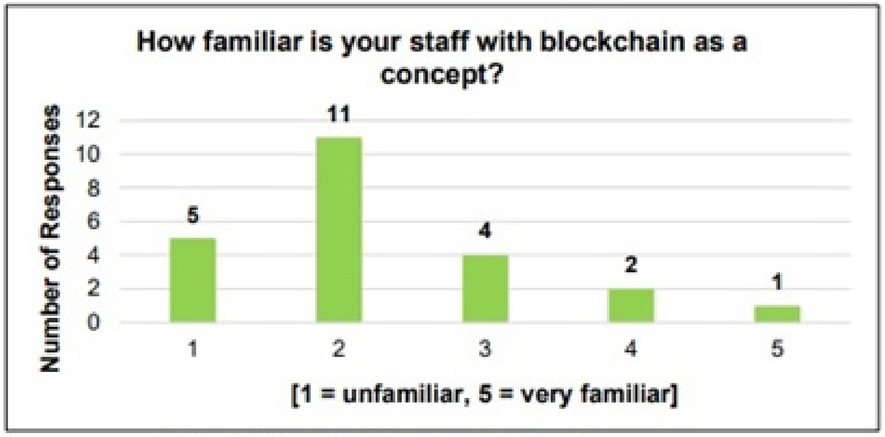
Most respondents reported having little familiarity with blockchain technology and acknowledged that their staff has limited familiarity with blockchain technology (Figure 1 and Figure 2).

Figure 1



Note: 23 Total Responses Recieved

Figure 2

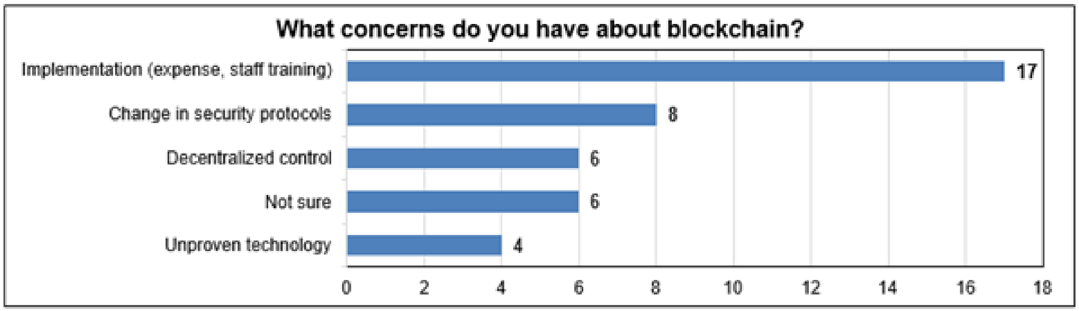


Note: 23 Total Responses Recieved

Key Concerns about Blockchain Technology

Respondents shared their key concerns about blockchain. A majority (17) listed implementation (including added expense and staff training) as their top concern when thinking about blockchain technology followed by change in security protocols. Responses are shown in Figure 3 below. Respondents had the option to select more than one answer.

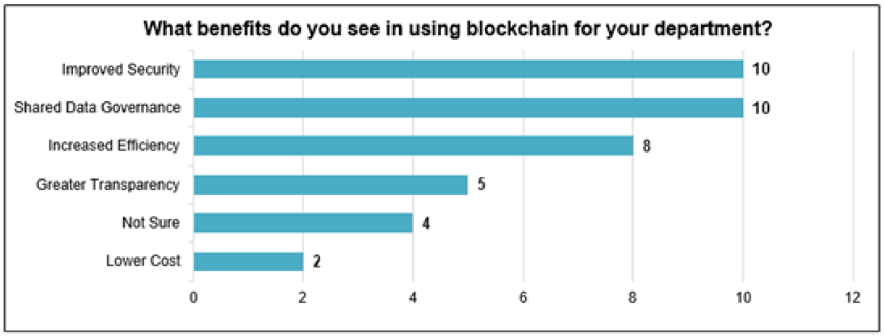
Figure 3



Potential Benefits of Blockchain Technology

Despite 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 could be a potential benefit of blockchain technology implementation. Responses are shown in Figure 4 below. Respondents had the option to select more than one answer.

Figure 4



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. Although blockchain technology is seen as an opportunity for improved security, shared data governance, and potential for increased efficiency, results suggest that additional resources, training, and funding are needed to be able to consider blockchain in State functions. 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 include 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.

V. Potential Application Areas

V. Potential Application Areas

V.A. Vital Records

Key Recommendations

REC V.A.1. The State should consider using blockchain technology to create and verify tamper-resistant digital certificates of government-issued documents.

REC V.A.2. New legislation should be considered to amend the Health and Safety Code sections 102400, 102430, and 103525 to include blockchain application.

Introduction

Vital records, or government-issued documents that catalog life events, are used to validate the identity of a person in order to provide access to a benefit or service such as applying for credit, obtaining a passport, receiving a driver's license, receiving benefits, enrolling a child in school, and more. The three most common types of vital records are birth certificates, marriage certificates and death certificates. While these certificates are most commonly referred to as vital records, fingerprints and other genetic data or identifiers could also be considered as such.

In California, vital records are maintained by the local County Recorder's Office where the birth, marriage or death took place and then shared with the California Department of Public Health – Vital Records (CDPH-VR), which maintains birth, death, fetal death/stillbirth, marriage, and divorce records for the state. Local county recorder's offices are responsible for the intake and recording of information: the registration. During this process, birth, death, and fetal death certificate information is submitted to CDPH-VR electronically for state review, processing, and issuing certified copies. Marriage certificates are transmitted to CDPH-VR as paper documents and are subsequently reviewed and indexed to be stored as digital images for issuing certified copies. Services provided by CDPH-VR include issuing certified copies of California vital records, registering, and amending records.[1] Currently, marriage records are the only type submitted by counties that are not already digitized as part of the registration process. When a paper marriage record is received by CDPH, a staff member scans the document into the vital records database and conducts a key data entry exercise to make that scanned image searchable for issuance. This process is called "indexing."

Because of the range of uses, the validation of vital records is conducted by a multitude of federal, state and local entities that rely on certified copies. Certified copies of vital records are typically marked with a government seal that might be raised or embossed, and/or multicolored. In addition to an official seal, the certificate could include the signature of the state, county or city registrar.

Pilots and Related Case Studies

Washoe County Marriage Certificates: In April of 2018, Washoe County in northern Nevada created a pilot program to use blockchain technology to allow couples to receive digital marriage certificates directly to their email accounts. The program uses the Ethereum blockchain to create a hash* of a couple's physical marriage certificate.[2] The requestor receives a digital copy of the marriage certificate, which can be submitted to agencies to verify its authenticity. The pilot was a success: participating couples received their marriage certificates within 24 hours via email, instead of having to wait 7 to 10 business days.[3] This use of blockchain is both more secure than the current paper process and more expedient. The program has since expanded and is being fully implemented by the county.

** A hash is a unique identifier for a piece of of data (say, an idenitity record). All of the information in the identity record (name, date of birth, etc.) will be rolled together and a hash function will generate the hash. Hash functions guarantee that, if any of the information fed into it is different, then the output hash ID will be different.*

[1] SB373: County recorder: Vital records: Blockchain technology (Feb. 2019). http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200SB373.

[2] Ethereum definition: https://ethereum.org/what-is-ethereum/.

[3] Washoe County, "Digitally Certified Document Copies," https://www.washoecounty.us/recorder/blockchain.php.

Illinois Birth Certificates: The Illinois Blockchain Initiative (IBI) was launched in November 2016 as a collaborative effort by a number of state and county agencies to explore and assess the possibilities of applying blockchain technology in governance and public service delivery.[4] One of the pilot projects established through the initiative involved developing digital birth certificates using blockchain. IBI partnered with the blockchain technology company Evernym to develop a birth registration process that would allow residents access to digitized birth records without the time and expense of traditional record management models, which rely on filing paperwork.

Academic Certificates: Created by GovTech Singapore and the OpenCerts Consortium, the blockchain-based platform can issue and validate academic certificates. Educational institutions can create digital versions of academic credentials and publish them on a public ledger. Users can also validate their certificate by dragging the digital copy onto the OpenCerts portal. In real time, the website will compare the digital copy to what is stored on the blockchain and identify whether the certificate is valid.[5]

Austin MyPass: In February 2019, the city of Austin, Texas, created a pilot project that aims to use blockchain to help its growing unsheltered population. Several city agencies and other groups in Austin are testing a service they call MyPass, which aims to give unsheltered individuals who might not have valid identification the ability to store and notarize their vital records on a blockchain application they can access from any device. They can then use these digitized government documents to sign up for various government benefits.[6] The pilot is in early development stages, as Austin is still building the platform.

E-Estonia: In 2007, Estonia launched the e-Estonia initiative to digitize all governmental data concerning its citizens using blockchain. Most of Estonia's government services and functions, including taxation, citizen identification, voting, health, and public safety are fully digitized and many use blockchain technology. The initiative uses blockchain technology designed to ensure

[4] Young, Winowatan, and Verhulst. "Case Study: Registering Births," p.3. https://blockchan.ge/blockchange-birth-registration.pdf.

[5] OpenCerts: https://opencerts.io/faq.

[6] Daniel Fisher, "Austin Looks to Blockchain-Powered ID Management," *Government Technology*, 13 September 2018. https://www.govtech.com/products/Austin-Looks-to-Blockchain-Pow-ered-ID-Management.html.

networks, systems, and data are free from compromise, while retaining data privacy. Estonia claims digitization ensures its history cannot be rewritten by anyone and authenticity of the electronic data can be mathematically proven.[7]

Considerations and Opportunities for Blockchain Application

Validation: In context of the United States, the verification of a certified vital record is based on the physical appearance of an official seal. While embossed seals may have been tamper-proof in the past, advancements in technology have revealed vulnerabilities in relying solely on the visual appearance of a seal.

Permissioned vs. permissionless blockchain: When deciding to use blockchain in government processes, it is critical to consider the type of blockchain that best fits the use case. Generally, the types of blockchain can be categorized by their permission model, which determines who can maintain them. These permission models also interact with the public availability of the blockchain. The two main models to consider are Permissioned and Permissionless.

Improve vital recordkeeping: Current vital record management models across the state vary from county to county. In many instances, this information is kept using outdated technology, and some counties rely solely on paper filing systems. Blockchain has the potential to create uniformity across the state and promote access and protection of records, security, privacy, transparency and overall efficiency in the management of vital records.

Access and authentication: By using the distributed ledger function of blockchain and storing the hash of a digital file (which can correspond to any record), it is possible to assure third parties of the authenticity of the file without revealing the actual content of the record itself. Ensuring that individuals have immediate access to their information and the ability to confirm its authenticity can more quickly connect them to needed services. This allows for more efficient and secure interactions with government, which requires the proper forms of identification for verification.[8]

[7] Adnrew Young, Michelle Winowatan, and Stefaan Verhulst, "Case Study: Registering Births on the Blockchain in Illinois," *GovLab*, October 2018, p.4.

[8] Young, Winowatan, and Verhulst. "Case Study: Registering Births on the Blockchain in Illinois."

Security and privacy: The decentralized aspect of blockchain provides an additional layer of security, making hacking difficult because information cannot be gained or controlled from a single computer server.[9] In addition to security, blockchain provides potential privacy benefits. In contrast to a traditional system in which a central authority verifies transactions, network users validate the transactions in a blockchain, replacing the need for a single third-party institution to provide trust.

Transparency: Records kept on the ledger can be immutable, meaning they are permanent and cannot be altered. This is a powerful tool that allows a piece of data to be verified at a given time. This level of transparency could improve the public's perception of government and increase trust in public institutions.[10]

Blockchain Implementation: Potential Barriers and Concerns

Disruption: As with any new technology, disruption of current norms and procedures is inevitable. Blockchain technologies should be integrated into existing systems in a way that complements and upgrades current practices in order to mitigate disruptions. In the context of vital recordkeeping, it can be helpful to maintain paper files along with digital files while county registrars become accustomed to new processes.

Privacy and governance: Under the U.S. Constitution, every citizen is protected from unlawful search and seizure. Arguably, this means that even if a government entity is an administrator of information held on a blockchain, that entity may not have unfettered access to personal information of citizens without reasonable controls.[11] This concern is at the heart of many fears surrounding blockchain. Given the general hesitation to publish private information on a distributed ledger, it is recommended that private personal identifiable information be kept to a minimum. Although vital data may be stored on the blockchain, what generally is stored is a hash of the data, not the data itself.

[9] Sarah Noceto and John Thompson, "Issue Primer: Blockchain Technology," California Senate Office of Research, June 2019, p. 3. https://sor.senate.ca.gov/sites/sor.senate.ca.gov/files/Issue%20Primer%20-%20Blockchain.pdf.

[10] Julie Hamill and Harris Bricken, "Blockchain Technology: Local Government Applications and Challenges," ICMA and GFOA White Paper (Nov. 2018), p. 6. https://icma.org/sites/default/files/2018-Nov%20Blockchain%20White%20Paper.pdf.

[11] Hamill and Bricken, "Blockchain Technology," p. 13.

To preserve privacy, institutions should not store personal information on a blockchain, encrypted or not. They should also be cautious with hashes of private data because hashing functions are deterministic, and if the input is known, the hash can be verified. If a small amount of information is hashed, such as names or emails, an attacker could run through a list of likely inputs and compare the generated hashes. Protection against such an attack is typically achieved by adding arbitrary data (known as salt) to the data that will be hashed.

Additionally, if illegal, incorrect or otherwise objectionable data is entered onto a blockchain ledger, it cannot be removed. The permanence and persistence of this information could potentially affect the privacy of individuals. Strong governance models and controls regarding data security and privacy must be examined carefully to regulate information added to the blockchain.

Finally, to the extent the State retains responsibility for vital records, it will need to establish a mechanism for public oversight of the governance of blockchains used to store and access them. Note: oversight does not mean that the State must be involved in the operation of the blockchain(s) or even directly involved in their governance.

Accessibility: Although blockchain removes barriers connected to traditional record management models, it also creates new technological barriers, particularly for low-income or rural communities with limited computer access or broadband connections. Before introducing a blockchain process, it is imperative to evaluate accessibility across populations and provide alternatives for connecting individuals with their digital vital records. Institutions such as public libraries or social service centers could play a role.

Implementation costs: To implement the technology, a reliable existing digitized database must be available to draw from and a population must be willing to participate. In addition, the technical framework for such a system would need to be developed. These requirements could be time-consuming and costly for the implementing agency.

Next Steps

New regulations: The California Legislature has recognized the potential of blockchain technology by the passage of two bills: SB 838 (Hertzberg, 2018), which provides statutory authority for corporations formed in California to use blockchain to create and maintain corporate records, and AB 2658 (Calderon, 2018), which defines blockchain for purposes of law and created the workgroup and framework that has led to this report.[12] The first and only legislation related to the management of vital records is SB 373 (Hertzberg, 2019) introduced in 2019 and still under consideration by the Legislature. SB 373 originally authorized the issuance of birth, marriage, and death certificates by means of blockchain, and has since been focused on marriage certificates. Local governments such as Berkeley and Sacramento have launched pilots that use blockchain technology to improve services, although no programs yet center on the use of vital records.[13]

Several blockchain-based certification and verification pilots have proven successful. While current processes digitize most vital records, the benefits of digitization are felt only by counties and the state's Vital Records Unit at the California Department of Public Health. California should consider removing barriers from counties interested in building a blockchain component into their vital record processes so residents can receive certified copies of their documents faster. In addition to the streamlined time-frame, blockchain technology would make verification more secure.

Currently, the California Health and Safety Code governs California law pertaining to vital records. Sections of this code outline everything from the creation of records to access guidelines. Future legislation would need to address these codes in order to remove barriers for localities that may want to pilot, or transition their certification and validation processes onto a blockchain platform.

V.B. Health Records

Key Recommendations

REC V.B.1 Engage with patient advocacy groups, health consortia, health systems, hospital CIOs, executives at payers, and blockchain-for-healthcare platforms to understand the viewpoints and technical considerations of all stakeholders. Such conversations should also include government agencies and

[12] California Senate Office of Research. "Issue Primer: Blockchain Technology."
[13] California Senate Office of Research. "Issue Primer: Blockchain Technology."

related entities including the California Health & Human Services Agency, school districts and organizations that review immunization records, Centers for Disease Control, Immigration & Customs Enforcement, and the California Department of Food and Agriculture.

REC V.B.2 Develop a framework for providing patient identity and data interoperability. This will better equip those who want to address challenges of data fragmentation and silos, lack of cohesive patient identity and privacy, security vulnerabilities and a one-size-fits-all approach to health care delivery.

Introduction

To achieve the best health outcomes, it is essential to have complete and accurate records that provide a contiguous context for a person's health. Health records of good quality also can foster more tailored and personalized care, bolstering patient engagement and empowerment. Electronic health records (EHRs) were conceived as a means to weave a more complete health context for patients, and today in the U.S., EHRs have been widely adopted; yet their promise has not been realized. Health data remains fragmented and incomplete because the system has not achieved the degree of interoperability needed to bring disparate data sets together to deliver a unified context for patients. From a health data perspective, the patient or healthcare consumer also continues to remain at the fringe of the data continuum, with limited control and less agency in their own health journeys.

Centralized digital systems aggregate important information regarding patient health, financial status, and identity, creating honeypots attractive to cybercriminals. Unfortunately, poor security protocols in the health sector leave health records increasingly vulnerable to crippling data breaches like ransomware with high financial loss. According to *Medical Economics*[14] there have been 172 ransomware attacks on U.S. healthcare organizations since 2016 that have cost a total of more than $157 million. California providers were the most common target of these attacks, at a cost of between $23 million and $35 million. The construct of current health data stores places the burden of providing adequate defense to cyberthreats on providers, payers or other entities which keep copies

[14] Keith Reynolds, "Ransomware Attacks Spike, Cost Healthcare Orgs Millions." *Medical Economics* at MJH Life Sciences, 2020. https://www.medicaleconomics.com/technology/ransomware-attacks-spike-cost-healthcare-orgs-millions.

of health records. Healthcare CIOs have broadly declared security to be one of the most difficult and financially devastating issues in healthcare.[15]

Fragmented data silos and insecure storage systems also complicate reliable and comprehensive care. At the same time, patients are often charged with taking control of their own data if they change providers or insurance plans. The patient bears the burden of trying to establish a continuous and cohesive health record, an arduous process of requesting copies of often decentralized health records and finding a way to keep these records together, easily accessible and secure. In terms of their own health identity, individuals lack true ownership or control over health data.

The adoption of blockchain-based systems, combined with other advanced technologies such as artificial intelligence (AI), machine learning (ML) and Internet of Things (IoT), could help to construct a modern, personalized healthcare system for California. A convergence of these technologies will put the individual at the center of the care continuum, with control over a complete health record that is selectively shared with healthcare providers to improve outcomes and care.

Context for California

At 39.5 million residents, California is the most populous state in the U.S. It also has the largest economy of any U.S. state and if it were a country it would rank 5th in the world by GDP. As a result, its advances in technology and policy can often influence a broader national and even global conversation. As healthcare is a significant item in the state's budget, improving processes and regulations in California promises a worthwhile return on investments to achieve better health outcomes. The COVID-19 pandemic has also both increased demand for healthcare while reducing public revenues to pay for it.

Improving how patient health records are managed and shared will be central to achieving better health for Californians. State law currently requires hospitals to keep a patient's records for up to 7 years. Medi-Cal requires that records be kept for 10 years. These requirements might seem sufficient but are inadequate when patients must manage their health records across multiple providers throughout their lifetimes. Modern health contexts are dynamic models, so patients need

[15] Reynolds, "Ransomware attacks spike," *Medical Economics.*

their records to be portable, private and persistent – accessible anywhere at any time and shareable with health professionals or other entities of choice. Current data storage and sharing models are ineffective and inadequate for this goal.

Interoperability

Currently, ready access to comprehensive patient data through EHR systems has been riddled with problems: patient data is fragmented across too many healthcare stakeholders, and different providers may use different EHR systems. Even within a single health system, providers may use different EHR platforms among various internal divisions, making interoperability difficult.[16]

Without adequate and well-defined frameworks to reduce critical interoperability barriers, ensure streamlined clinical documentation or increased quality measures, health systems for California, and more broadly in the U.S., will continue to struggle to deliver a high quality of healthcare. Blockchain technology has the capabilities to solve many of these systemic issues by providing seamless, real-time coordination and integration of complete and contextual health data across disparate health systems.

Blockchain can also help make the healthcare journey more participatory. With data ownership individuals can share their health data with healthcare providers in a secure, private and selective manner. From a provider's perspective, high personal engagement and participation mean that the healthcare process becomes more collaborative, and likely to produce better outcomes more efficiently.[17] With the right access to patient-owned healthcare data, health systems can offer optimized care to patients, from providing personalized, predictive diagnosis and treatment, to precision medicine and preventive care.

Due to regulatory constraints, it may not be possible to fully decentralize the healthcare system with blockchain. Instead, trusted ecosystem players such as hospitals, insurance companies, clinics, labs and health information exchanges (HIEs) may become part of the processing fabric of the system as they can store and process patient data. Blockchain can improve data sharing and

[16] Adapted from the book *Enterprise Blockchain Has Arrived* by Radhika Iyengar and Jorden Woods (Los Gatos, CA: Woods and Iyengar, 2019).

[17] Woods and Iyengar, *Enterprise Blockchain Has Arrived*, 298-300.

interoperability, leading to better patient data management and coordination. This will provide a better point-of-care experience for patients.

Data storage is particularly important for compliance with regulations regarding record retention. Currently providers and payers are responsible for storing and managing confidential health records. Decentralized data storage with hashes of health records stored on the blockchain will provide verification of data authenticity and integrity. Further, with data sovereignty, patients will take ownership and control of their health records and can safeguard the privacy of their records with selective disclosure mechanisms.

Potential Pilots and Related Case Studies

California Immunization on Blockchain

The healthcare ecosystem is an extraordinarily complex environment. While blockchain technology can play a role in addressing some of these problems, deciding where to begin can be daunting. A relatively simple use-case could help test whether blockchain can be used successfully to improve efficiency. For example, immunization records, which are part of Personal Health Records (PHRs), could be stored on a California Immunization Blockchain.

Currently, Californians are required to present a record of their vaccines for a variety of reasons, touching many participants in the ecosystem who come into contact with an immunization record:

1. The "patient" being immunized
2. The parents or guardians of the patient, if the patient is a minor
3. The healthcare provider administering the vaccine to the patient
4. The county that provides or maintains the immunization record
5. "Relying Parties" that must verify the immunization record, such as:

    a. A school the patient attends or where a teacher/employee works; volunteers at school events
    b. Travel professionals who assist travelers in acquiring visas/permits to visit countries where such immunization records might be needed
    c. Healthcare professionals

The Blockchain Working Group had initial conversations with representatives of the California Immunization Record (CAIR) to discuss this prospect. Managing and sharing immunization records is more complex than it may appear. CAIR representatives indicated potential for improvement. However, more detailed discussions will be needed to arrive at a scope for the pilot, and how it might be approached.

Details of this effort need to be worked out in future discussions, but blockchain technology – with the appropriate security and privacy controls – merit consideration in managing immunization records and should be considered for a pilot on a small scale.

Personal Health Record

The 1996 Health Insurance Portability and Accountability Act (HIPAA) set requirements for privacy in health records.[18] Providers and payers must preserve privacy, but patients are, by law, permitted to have access to their own records. Security is also a requirement for protecting health records as well as safeguarding privacy, but current security protocols are ineffective at preventing cyberthreats like ransomware. The relationship between identity and privacy are intertwined with patient records, but patients still have limited ownership or control over their own complete records. The creation of a Personal Health Record (PHR), which goes far beyond the EHR, offers one solution.

Blockchain technology can make secure PHRs a reality. The PHR is a key building block of the healthcare ecosystem because it will contain a patient's fully self-sovereign and private record of medical history, and will include treatment history from providers, patient-generated health data, and a summary of patient health information. A PHR enables each person to own his or her own comprehensive personal health information and share this data across the ecosystem to receive optimized care.

To date, PHRs have not gained widespread adoption because of significant security and identity concerns. However, blockchain technology, paired with Self-Sovereign Identity (SSI) and Decentralized Identifiers (DID), makes it possible

[18] Health Insurance Portability and Accountability Act of 1996 (HIPAA). https://www.cdc.gov/phlp/publications/topic/hipaa.html.

to achieve a true PHR by simultaneously addressing these concerns in a single system.[19]

Blockchain-related Opportunities and Challenges

COVID-19 presents some unique and near-term opportunities to integrate blockchain with contact tracing as well as COVID-19 testing and antibody testing. For example, contact tracing programs should have privacy protection integrally woven into the mechanisms to limit intrusive surveillance. Testing results for COVID-19 or antibodies should be provided as verifiable credentials (see AB 2004). Results could then be integrated with the individual's PHR.

In a more global context, other ecosystems offer points of reference when developing the healthcare framework for California. Consider the models of Dubai or Estonia, both progressive enterprising ecosystems that are considering or have deployed country-wide Digital Ledger Technology (DLT)-based health systems. A general roadmap for considering blockchain implementations for improved health records could include the following steps:

1. Prioritize health record problems to focus on for which blockchain has a useful application and solution
2. Define the health record use cases to be pursued
3. Define concrete, near-term pilots, bringing together allies in industry and tech – consider legal and regulatory consequences
4. Agree on standards and best practices in the implementations
5. Document outcomes in these health record use cases
6. Determine next steps after results are established
7. Re-align with allies and partners, and identify new partners
8. Explore interoperability with other chains

With the deployment of any emerging technology, some technology challenges must be considered. With blockchain, technology concerns such as scalability, potential cross-chain interoperability, and blockchain-to-legacy system challenges are important considerations. Permissioned or hybrid blockchain systems are currently better positioned to deliver solutions that effectively address these challenges. Deployment across a large state such as California will need

[19] Woods and Iyengar, *Enterprise Blockchain Has Arrived*, 302-303.

to take scalability to a high level. There are other technology challenges for decentralized systems, such as large-scale private key management to be able to deploy across the California population. Finally, on the business side of blockchain, the application of appropriate governance standards will be essential in planning and implementing pilots.

V.C. Supply Chain

This section includes analyses for blockchain applications for Food and Agriculture and Pharmaceuticals.

Key Recommendations

REC V.C.1. Tracking Food Contamination: Work with the California Department of Food and Agriculture to establish a pilot to use blockchain technology, based on the successful experiences of IBM and Walmart, to collect and organize data from growers, transporters, wholesalers and retailers to more quickly trace the source of food-borne contamination and where the products are in the distribution system to speed recall and consumer notification. Explore the possibility of federal grant money to support a California-based pilot.

REC V.C.2. Food Freshness: Explore the use of blockchain combined with IoT sensors and artificial intelligence to help growers better estimate product shelf life and optimize transportation and logistics to ensure that produce can be delivered to destinations within the shelf-life periods.

REC V.C.3. Small Farms: California policymakers could support small farms in their exploration of the use of blockchain technology by identifying opportunities for pilots for California's specialty crops and organic produce where "tip-the-farmer" initiatives could help increase margins and sustainability. California policymakers could also expand oversight of agricultural co-ops and evaluate opportunities to revise their accounting practices and operations using blockchain technology.

REC V.C.4. Cannabis Supply Chain: California policymakers could direct the California cannabis licensing authorities to accept blockchain-based verification and reporting mechanisms for the cannabis supply chain. This might require certifying specific blockchain projects that pass a set of standards for operation and authenticity. California policymakers also could consider authorizing participants in the cannabis supply chain to use payment mechanisms that implement stringent industry "know your customer" processes but also accommodate U.S. regulatory concerns.

REC V.C.5. Pharmaceuticals: Develop a pilot program that brings together a broad group of California partners, including state government, pharma manufacturers, distributors, retail pharmacies, technology companies, healthcare providers and payers, patient advocacy groups, universities and other research facilities. Similar to other consortia like MediLedger, it is recommended that a "California Pharma Consortium" includes distributors and retail pharmacies, to ensure that the "last mile" in the pharma supply chains are secured.

FOOD AND AGRICULTURE

Introduction

California is the agricultural powerhouse of the United States. Over a third of the country's vegetables and two-thirds of the country's fruits and nuts are grown in California, and the state also supplies 19 percent of U.S. dairy.[20] California is known for its agricultural abundance and diversity, including over 400 commodities. Potential applications of blockchain technology for the food and agriculture industry include:

- Supply chain traceability (specifically provenance tracking, logistics, and safety)
- Supporting small farms and the circular supply chain
- Supporting the emerging cannabis industry, particularly with regulatory conformance

Pilots and Related Case Studies[21]

IBM Food Trust focuses on food safety and provides track-and-trace plus point-of-origin tracking for food products in supply chains. The platform's primary use case is the elimination of costly and damaging "food scares" by rapidly

[20] Netstate.com, "California Economy," 2017. https://www.netstate.com/economy/ca_economy.htm.

[21] This section and the following section have been largely adapted from *Enterprise Blockchain Has Arrived*, by Jorden Woods and Radhika Iyengar (2019), Chapter 11.

identifying the source of tainted products. Members of the consortium can trace food back to its origin in seconds, versus 6-7 days with standard processes. Key members include Walmart, The Kroger Co., Carrefour, Albertsons, Nestlé, Dole, and Driscoll's.

Intel's blockchain was deployed in a successful pilot with blueberries from Oregon. Intel used remote sensors in crates of blueberries to track temperature, location and environmental data in real time. Oregon food safety regulators are confident that the reduced time to trace the source of a food-borne disease outbreak from days or weeks to minutes or even seconds will help decrease illnesses while issuing more precise recalls. Growers benefit by ensuring their products are delivered to customers with improved freshness.[22]

Several baby food and milk producers are using blockchain for food traceability. Nestlé and Carrefour are tracking infant formula using the IBM Food Trust blockchain.[23] Plasmon, an Italian subsidiary of Kraft Heinz, is exploring blockchain for baby food in association with the local agriculture ministry. TE-FOOD tracks organic infant formula for Vietnam's largest milk company, Vinamilk.

Considerations and Opportunities for Blockchain Application

Blockchain for Supply Chains. Blockchain-based systems can provide visibility and better data across supply chains.[24] Common applications relating to food and agriculture include:

- Product traceability
- Authenticity and product provenance
- Process transparency

Product Traceability. The ability to quickly find the origin of a product, i.e., food traceability, is important to ensure a reliable and healthy food supply. Food contamination from Salmonella, E. coli, Listeria, or parasites can create food scares,

[22] Kuldeep Singh, "Oregon Farmers Use Blockchain to Track Crops." *C#Corner*, 21 January 2020. https://www.c-sharpcorner.com/news/oregon-farmers-use-blockchain-to-track-crops.

[23] "Danone Uses Blockchain for Baby Formula Traceability," *Ledger Insights*, February 2020. (accessed 21 April 2020). https://www.ledgerinsights.com/danone-blockchain-food-traceability-baby-formula/.

[24] Adapted from Woods and Iyengar, *Enterprise Blockchain Has Arrived*, Chapter 11.

which may lead to significant losses for food producers and distributors when products are pulled from shelves and destroyed in store and at the farm. Severe events have an average cost of over $100 million. As many food-borne illnesses are eventually traced back to a single farm or even a single batch of product, finding the source of contamination quickly can save tens of millions of dollars.

With current supply chain systems, food traceability often takes a week or more since data is fragmented and siloed across the actors in the chain. Most members of a supply chain are only familiar with activities one step forward and one step back, those directly connected to their organization. Because no comprehensive system captures all transactions across the chain, each part of the supply chain must be contacted directly to understand the full path that a product took to reach a retailer.

While media reports on illnesses and deaths mount, retailers and farmers are forced to destroy products quickly to regain consumer confidence. In the U.S. every year, foodborne illnesses affect one in six Americans, lead to hundreds of thousands of hospitalizations, and cause more than 3,000 deaths. They also cost the U.S. economy more than $93 billion annually.[25] Globally, the numbers are much larger; according to the World Health Organization (WHO) 600 million illnesses and over 400,000 deaths annually result from food contamination. Smaller retailers and farmers are especially hard hit since they must absorb the losses, and some may be forced into bankruptcy.

Blockchain-based supply chain systems can provide an accurate and immutable record of all transactions across the chain. These systems assign a unique ID and secure decentralized tagging system that tracks food at the batch or lot number. Often the unique ID is based on a global standard to ensure that all stakeholders are using the same approach for identifying their products. Since all nodes have access to this record, traceability becomes routine.

Food safety is a specific case that has gained significant traction, but the same approach can be applied to any product within a supply chain. Traceability is an important step in determining product authenticity.

[25] Martha Filipic, "High Cost of Foodborne Illness: New Study Provides State-by-State Breakdown." The Ohio State University: College of Food, Agricultural, and Environmental Sciences (CFAES), 3 June 2015. https://cfaes.osu.edu/news/articles/high-cost-foodborne-illness-new-study-provides-state-by-state-breakdown.

Authenticity and Product Provenance. In today's supply chain systems, there is often no simple way to track the provenance and authenticity of a product. More sophisticated centralized systems, such as EPCglobal, have used barcodes, unique electronic product codes (EPC), and radio frequency identification (RFID) technology to track items. These systems rely on centralized certificate authorities and centralized databases, but these systems are fundamentally insecure since they have single points of failure that make them susceptible to cyberattacks and insider fraud.

Decentralized and immutable blockchain systems allow a product to be tracked to its origin (traceability) and through every step of the supply chain (authenticity). A number of blockchain projects have already deployed decentralized apps (dApps) that use information in the supply chain to authenticate that a product, such as a luxury good or food item, is in fact authentic. The dApp enables a user to scan a product QR code which provides a full trace and validates authenticity.

Embedded RFID or near field communication (NFC) chips track a product or its components through every step in the chain. At each step, the RFID chip is scanned, a smart contract is executed, and then multiple trusted nodes verify the information is correct before it is written to the blockchain ledger. Supply chain transparency enables quick and inexpensive product authenticity validation, and in the long run, can discourage fraud.

Provenance takes authenticity one step further by also providing information about product history through the supply chain, such as location history, custody history, and environmental conditions during the journey. Such information, including GPS coordinates, custody IDs, temperature data, accelerometer information (for damage assessment) is typically captured by sensors or IoT (Internet of Things) devices. Blockchain technology reduces verification costs, which leads to more widespread industry adoption, and makes checking product authenticity and provenance more commonplace.

Examples of this capability include an offering from Carrefour for over 20 different products including milk, meat, eggs, and fruit sold in their stores, mostly in Europe and China. Consumers can use a smartphone to scan a QR code on the product which provides information such as harvest date, freshness, certifications, and sustainability. Carrefour has indicated these initial blockchain pilots have boosted trust and increased sales markedly, and is expanding blockchain implementation to more than a hundred products.[26]

Process Transparency. Another important aspect of supply chain is process transparency, or exactly what happens at each point in the chain. For example, if a retailer or distributor receives damaged goods it may be impossible to know where in the chain the damage occurred. As a result, the supplier of the damaged goods or a member of the chain that damaged the goods will have no incentive to change their practices. Also, costs increase for all members of the chain since insurance premiums will increase if claims become common.

Because blockchain technology can quickly track information through every step in the process, it is also possible to combine tracking information with data about the environmental or product integrity. Many blockchain projects have proposed including IoT sensor data in smart contracts to make additional information part of the immutable ledger.

As mentioned previously, with IoT sensor data, a growing trend is tracking temperature for products in a temperature-controlled supply chain or "cold chain." Perishable products like food or medicine often need to be refrigerated, and freshness or viability can be affected by temperature swings. A significant fraction of food and medicine is spoiled during shipment due to intentional or accidental conditions that warm the product above recommended or agreed "cold chain" temperatures. IoT devices can provide a real-time log of temperature data that can be used for compliance, enforcing accountability and understanding conditions that led to spoilage or damage.

Food Freshness. Lack of transparency in supply chains and logistics chains, as well as the lack of visibility into supply and demand, lead to tremendous food waste due to spoilage. "Currently, 45% of fruits and vegetables go uneaten, due to a chaotic distribution system that cares little about spoilage. The imprecise nature of today's supply chain (from farmers and shippers to food-packers and grocers) often leads to perishable produce being thrown away."[27]

[26] Benedict Alibasa, "Retail Giant Carrefour Saw Sales Boost from Blockchain Tracking," *Coindesk*, 4 June 2019. https://www.coindesk.com/retail-giant-carrefour-saw-sales-boost-from-blockchain-tracking.

[27] IBM Research, "Blockchain will prevent more food from going to waste," https://www.research.ibm.com/5-in-5/harvest/.

By implementing new tracking technology, such as blockchain, growers would know they are producing the right quantity of food to satisfy demand, and their produce would arrive at peak freshness. Grocers will be relieved that products will stay within their shelf life and that food will not be thrown away. Consumers will not only enjoy fresher food but also enjoy peace-of-mind, knowing that the produce they are consuming is fresh and safe. Advanced technologies converge to mitigate food waste and move closer to zero-waste consumption.

Blockchain Implementation: Potential Barriers and Concerns

Supporting Small Farms and the Circular Supply Chain

Supporting small farms and small-hold farmers is a priority for the State of California. Nearly 75% of California's farms are fewer than 100 acres. Overall, the average farm size in California is 348 acres, much less than the U.S. average of 441 acres. Notably, the Central Valley, especially San Joaquin Valley, produces more than half of California's agricultural output. Most of the farms in San Joaquin Valley are small; in San Joaquin County, for example, the average size among its 4,000 farms is 202 acres.

Several farm programs are exploring using blockchain technology. These include work done by Accenture on a "Tip-the-farmer" pilot[28] and by IBM through FarmerConnect, which allows a bag of coffee or unit of any agricultural product not only to be traced back to its origin, but also enables a small sum of money to be sent directly from consumer to producer, rather than indirectly through the intermediary layers.[29] They also create an efficient way for organized small-hold farmers to establish an ongoing relationship with the supplier, in a manner previously available only to large brands. Blockchain technology could also enhance the relationship between farmers and farming co-ops, in the U.S. as well as internationally.[30]

[28] Anna Baydakova, "Accenture's New Blockchain App Lets Users Tip 'Sustainable' Producers," *Coindesk*, 25 February 2019. https://www.coindesk.com/accentures-new-block-chain-app-lets-users-tip-sustainable-producers.

[29] Christina Trejo, "Farmer Connect Uses IBM Blockchain to Bridge the Gap Between Consumers and Smallholder Coffee Farmers," IBM Press Release, 6 January 2020.

[30] Emilia Picco, "Blockchain In Agriculture Use Case #1: AgUnity," *Disruptor Daily*, 8 September 2019. https://www.disruptordaily.com/blockchain-in-agriculture-use-case-agunity/.

Regulating the Cannabis Supply Chain

The cannabis industry is growing quickly in California, and the pressure to properly test and certify the supply is greater than perhaps anywhere else in agriculture. The regulatory landscape in California also is evolving.[31] In addition to tracking provenance, proper lab testing and labeling in ways that consumers can trust at the point of purchase is essential. This testing and certification is not unlike those emerging in the pharmaceutical supply chain; however unlike pharmaceuticals, the labels must be understandable and trusted by average consumers.

Already a startup community in the blockchain and cannabis space is emerging, and participants are working with increasingly larger partners. One example, TruTrace, "is launching its StrainSecure product in partnership with Deloitte. The system employs blockchain technology to track cannabis from seed to sale, in order to guarantee that customers and retailers know the history of the product" according to a *Cointelegraph* article from September 2019.[32] Furthermore, putting testing results directly on a blockchain, visible to all, can help reassure wholesale or retail buyers that the product they are holding has been independently tested, rather than trusting a simple label on a product. At least one company is focused on this, called CBD LabChain.[33] All this also enables regulators to have a real-time view into the supply chain data and perhaps could automate reporting and auditing, avoiding delays or the risk of incorrect reporting.

PHARMACEUTICALS

Introduction

The global pharmaceuticals industry is big business, valued annually at $1.2 trillion. Pharmaceutical companies spend tens of billions of dollars and go through an arduous process to produce and commercialize prescription drugs. According to the World Health Organization, the counterfeit prescription drug trade is 10% of the global market.

[31] State of California, "Cannabis Regulations," *California Cannabis Portal*. https://cannabis.ca.gov/cannabis-regulations/.

[32] Adrian Zmudzinski, "TruTrace Partners With Deloitte to Track Cannabis Using Blockchain," *CoinTelegraph*, 4 September 2019. https://cointelegraph.com/news/trutrace-partners-with-deloitte-to-track-cannabis-using-blockchain.

[33] Veronica Combs, "New blockchain platform will verify lab results for CBD products," *TechRepublic*, 21 November 2019. https://www.techrepublic.com/article/new-blockchain-platform-will-verify-lab-results-for-cbd-products/.

Compliance will be the biggest driver for many California stakeholders in the pharmaceutical industry. As of January 2109, California requires controlled substances to have unique serialization numbers to have product traceability. Going beyond traceability for controlled substances, many California pharma companies as well as their partners, such as distributors and retail pharmacies, already are part of blockchain networks focused on drug traceability, provenance, and safety. This is a good starting point and a foundation that California can build on to provide a broad range of valuable blockchain-based solutions for the industry and for CA residents.

To assist with achieving compliance with the Drug Supply Chain Security Act (DSCSA), the FDA began a pilot project program in May 2019. The FDA selected 20 participants as part of the pilot program to evaluate and explore different methods of achieving compliance. Blockchain technology provides an immutable, shared source of truth and, when combined with serialization and smart sensors, can provide an effective method of establishing a safer and more secure drug supply chain.

Of the 20 participants in the pilot program, the FDA selected at least seven participants that are using blockchain-based technology platforms working to provide compliance with the DSCSA. These include projects with MediLedger, the IBM/KPMG/Merck/Walmart consortium, UCLA Health, Rymedi, TraceLink, and IDLogiq. These initial pilots showed positive results and suggest that a blockchain-based solution will enable compliance while improving operations and reducing the supply of counterfeit drugs.[34]

The blockchain ledger can provide end-to-end transparency for drug production and distribution, including visibility into every stage of the supply chain. Blockchain technology not only improves the traceability of prescription drugs in the supply chain, it can also ensure that international standards are upheld, such as GDP (Good Distribution Practices), ensuring the integrity and quality of the medication for the end user. Additionally, it will be much more difficult for bad actors to tamper with the process or for pharma companies themselves to market fraudulent products. FWith regulatory tailwind, the deployment of blockchain-based solutions has the potential to protect consumer safety and public health, enhance consumer trust in pharmaceutical drug supplies, as well

[34] Woods and Iyengar, 195.

as bring operational efficiencies to pharmaceutical companies. Some might wonder whether the benefits outweigh the risks or costs. While these are still early days for implementing blockchain solutions, early results from pilots in 2019 provide support for optimism.

Some critics have questioned whether privacy and confidentiality can successfully be maintained. The use of permissioned blockchain systems and zero-knowledge proofs (ZKP) have produced early promising results. MediLedger, as well as other blockchain solutions, use ZKP to preserve privacy and confidentiality while still providing transparency along the supply chain.

Pilots and Related Case Studies

Emerging consortia for combating drug counterfeiting include the following:

MediLedger is focused on pharmaceutical drug compliance with the Drug Supply Chain Security Act (DSCSA). Started in 2017, MediLedger was accepted into the FDA pilot program in 2019. It includes 25 members that span many major pharmaceutical companies, retail pharmacies, and medical distributors. Chronicled is the main technology partner. The MediLedger pilot project final report noted "The working group considers that consortium-based software development has proven to be more cost efficient, have higher quality, and show a quicker time to value than traditional unilateral development efforts." Within the consortium, all members share in the development effort to include costs, requirements and testing. "The output is a single code base that can be deployed by each company with a high degree of interoperable certainty."[35]

IBM/KPMG/Merck/Walmart consortium is focused on compliance with the DSCSA. It was accepted into the FDA pilot program in 2019. The pilot is focused on traceability of vaccines and prescription medicines within Merck's supply chain and is using IBM's Hyperledger Fabric permissioned blockchain framework. The application will enable end customers to scan a quick response (QR) code at pickup to see the provenance and authenticity of the product by providing information such as manufacturing site and duration on store shelves.

[35] MediLedger DSCSA Pilot Project Final Report, February 2020.

Considerations and Opportunities for Blockchain Application

As blockchain is an ecosystem-spanning technology, the impact of compliance with the Drug Supply Chain Security Act is extensive. All California stakeholders that are part of the drug supply chain will be affected. The main concerns with pharmaceutical supply chains, as we have discussed, is traceability, compliance and early detection of issues such as contamination, adulteration, honest reporting of drug manufacturing processes or issues with drug shipments.

In October 2019, California Congresswoman Anna Eshoo and Congressman Adam Schiff held a joint hearing on how to improve protection of the drug supply chain. Congresswoman Eshoo indicated that there are shortages of life-saving medications and a reliance on subpar manufacturing, which has led to recalls of contaminated products. The only time consumers discover they have consumed a contaminated active ingredient pill is when there is a recall and crisis.[36]

Blockchain technology can provide solutions in each of these areas. To solve problems like product shortages, contamination, false labeling, and inventory management in existing pharma supply chains, stakeholders can either join an existing blockchain consortium or create their own. Because they are ecosystem-spanning, consortia include competitors who are now placed in a unique and unprecedented position of being required to share information with their partners. This model is a paradigm shift and requires a new mindset to be deployed successfully.

Additionally, according to KPMG, blockchains can serve as the "ledger of truth" for sharing complex information with regulators, pharmacy benefit managers, contract manufacturers, physicians, patients, academic researchers and R&D collaborators, among others. For California, other stakeholders include the State Board of Pharmacy, California-based pharma manufacturers, distributors/retail

[36] Congresswoman Anna Eshoo, California's 18th Congressional District. Press Release: "Eshoo Holds Hearing to Address Broken Global Pharmaceutical Supply Chain" (30 Oct. 2019). https://eshoo.house.gov/media/press-releases/eshoo-holds-hearing-address-broken-global-pharmaceutical-supply-chain.

pharmacies, hospitals/clinics, and consumer or patient advocacy groups.[37]

Well-managed pharmaceutical supply chains ensure that medicines are available when needed. Transparency across pharma supply chains ensures visibility of prescription drugs along the chains to prevent product shortages. Supply chain visibility also helps pharmacies and distributors better manage their inventories to keep up with demand.

Consortia entail other considerations such as new technology platforms and governance. These elements are likely to require new thinking for most stakeholders along the drug supply chain. Training will be needed both for blockchain in general and on specific platforms. On the technology front, the concept of decentralization will be new and unfamiliar territory. Current models are all centralized, and as processes move into the decentralized models required in blockchain-based systems, companies will be required to learn how to migrate to decentralized frameworks, build consensus across them and employ governance standards.

Governance presents a non-technical challenge, one that many experts believe may be more difficult to master than the technological issues. Good governance is a strong success factor in blockchain networks. Since blockchain networks are decentralized, consortium members must agree on a framework for how they will work together and resolve issues. Creating governance standards raises considerations such as what information is to be shared, how privacy is maintained, member eligibility criteria, and member accountability, among many others.

Existing consortia and their frameworks present excellent starting points for those wanting to learn about consortia and best practices. Additionally, the IEEE P2145 Blockchain Governance Standards Working Group is assembling a best-practices approach including developing lexical standards for governance to provide guidance to companies and consortia.

[37] Arun Ghosh, "Guest Column: Blockchain's Evolving Role in the Pharma Supply Chain," *Outsourced Pharma*, 24 April 2019. https://www.outsourcedpharma.com/doc/blockchain-s-evolving-role-in-the-life-sciences-supply-chain-0002.

V.D. Property

Potential uses cases considered as part of this section include: Real estate titles, vehicle and parts supplies and tracking, insurance, and firearm sales and ownership.

Key Recommendations

REC V.D.1. Real Estate: Titling. Continue to monitor ongoing efforts for potential applications in land titling.

REC V.D.2. Real Estate: Licenses. Explore issuing real estate licenses on a blockchain system while continuing to run the existing process in parallel until a new system is proven. This application may offer a more efficient license tracking system that could eliminate interstate fraud and streamline interstate collaboration. Discussions are needed with the Department of Real Estate to understand interest and readiness for this type of pilot.

REC V.D.3. Real Estate: Fraud Detection, Efficiencies. To the extent that emerging technologies have the potential to make title search, record validation, or detection of error or fraud cheaper, faster, or more accurate, encourage counties to consider blockchain technologies and to be forthcoming in providing technologists the data they need; encourage lenders, title insurers, and other private-sector actors to adopt efficient new technologies; encourage new players to enter the space; encourage governments and regulators to provide a level playing field and remove barriers; and encourage all parties to pass savings on to the end user.

REC V.D.4. Real Estate: Vendors and Procurement. Allow vendors to describe the system they can build and the costs, let them choose the underlying technologies to employ, and let the state's procurement officials select the most competitive bid. If blockchain offers an advantage, they will be well positioned to win in the marketplace. Procurement officials should have access to skilled and unbiased technical review and assistance in order to evaluate proposals effectively.

REC V.D.5. Vehicles and Parts. Further investigation is needed to identify whether there are specific regulatory barriers to applying blockchain technology to use cases in vehicles and parts. None are known at this time.

REC V.D.6. Vehicles and Parts: License Registration. Discussions with the Department of Motor Vehicles should continue to determine whether registration of motor vehicle operators is an appropriate use case for blockchain technology.

REC V.D.7. Property Insurance. Since streamlining insurer operations could have significant benefits for constituents in terms of pricing, access, and convenience, the state should encourage private industry to adopt blockchain technology as appropriate. California should also keep an open dialogue with industry to advance legislation and policies that might encourage and enable benefits to the consumer while minimizing potential risks such as potential loss of privacy.

REC V.D.8. Firearms. Although blockchain technology may find applications in firearms-related data in California, no opportunities have presented themselves at this time.

REAL ESTATE

Introduction

The titling of real property is a tremendous driver of economic empowerment.[38] Title enables a property owner to protect the claim to ownership, improve the property, sell it, leverage it as a financial asset, and minimize exposure to fraud or expropriation.

According to IBISWorld, the real estate sales and brokerage market size in California in 2020 is $31.2 billion.[39] Twenty-eight thousand five hundred home transactions closed escrow in California in February 2020, a 9% increase from February 2019. Volumes are expected to decrease due to shelter-in-place orders and disrupted economic activity due to COVID-19. In 2019, there were 437,500 home sales in

[38] We acknowledge the contributions of Kai Stinchcombe in this section who departed the Working Group before the completion of this report. Also thanks to Eric Bryant, National Accounts Director at First American Data Tree, for his research assistance on the sections on Real Estate and Insurance. Additional information was provided by J.P. Wagner of SFB Technologies; Ally Medina of the Blockchain Advocacy Coalition; Daniel Leibsohn of Community Development Finance; Mike Manning of Symbiont; and Manish Dutta, Chris Wade, and Tammie Arnold of Alpha Ledger.

[39] IBISWorld. https://www.ibisworld.com/industry-statistics/market-size/real-estate-sales-brokerage-in-california-united-states/.

California, a roughly one-percent decrease from 2018.[40] Even though it is widely speculated that home sales will take a hit due to the pandemic, perhaps not recovering until 2022-23, the volume and value of the real estate market in California is extensive and affects a large number of people.

Property Ownership Is Complicated. Determining who owns property is non-trivial. Real property is complicated and may include, in addition to land, water rights, mineral rights, air rights, easements that allow other people to access the property, liens for taxes, mortgages, loans, or other improvements. The boundaries of a property might shift due to an earthquake, or with rising sea levels or erosion. Furthermore, historical conveyances could be vague; for example, a hundred years ago a will might have left "all my property within San Francisco rather than a specific set of lots, making exhaustive searches difficult.

Title Authentication and History. Authenticating and understanding the set of transactions related to a property can be complicated, especially if there are forged or fraudulent transactions recorded in the Registrar's office. Fraudulent transactions may also make establishing ownership difficult. Incorrect interpretations of title history incur costs to a buyer, seller, insurer, or the taxpaying public.

Challenges of Common-Law Titles. The entire process of title research and insurance seems like a burdensome and expensive solution to a problem that ought not to exist. However, the alternative option of Torrens titles,[41] in which the government-kept record is de facto correct, had been previously adopted in California only to be repealed.[42] Torrens systems were found to be poorly implemented, did not prevent inaccurate data from being recorded, and did not solve the problem of financial responsibility for inaccuracy or fraud. Blockchain could potentially be used to address weaknesses in the current common-law title process, with the goals of reducing fraud, increasing efficiency, and reducing costs to the end user.

[40] Editorial Staff, "California home sales volume lays low," *ft Journal*, 6 April 2020. https://journal.firsttuesday.us/home-sales-volume-and-price-peaks/692/.

[41] "Torrens title," Wikipedia. https://en.wikipedia.org/wiki/Torrens_title.

[42] T. R. M. "Property: Registration of Land Titles: Inconclusiveness of a Torrens Title," *California Law Review* 12, no. 1 (1923): 49-53. doi:10.2307/3473595."The Torrens System of Title Registration: A New Proposal for Effective Implementation," 29 *UCLA L. Rev. 661 (1981-1982)*.
"Possessory Title Registration: An Improvement of the Torrens System," *William Mitchell Law Review* Vol. 11: Iss. 3, Article 6. Available at: http://open.mitchellhamline.edu/wmlr/vol11/iss3/6.

Pilots and Related Case Studies

Many governments in the United States and abroad have investigated the use of blockchain for real estate, as have companies in the private sector. A few examples follow below.

Chicago (Cook County). Velox worked on a pilot with Chicago's Cook County to record titles on the blockchain (however www.velox.re is no longer a working website). A government leader of the initiative noted that "the prerequisite to adopting blockchain at his office is to iron out the flaws in the state's current laws that allow data to remain unrecorded at the time of transactions, which would undermine the point of blockchain: to contain all available data about the transaction in one place."[43]

TruSet and Imbrex. TruSet and Imbrex Capital partnered to create the first blockchain-based state-by-state collection of residential real estate contracts in June 2019.[44] Leads of the project noted, "In the residential real estate industry, states use unique standards for purchase and sale agreements (PSAs). Some states, such as California and Colorado, do not require attorney involvement and contracts are standardized by local governments."

RealT. RealT focuses on tokenizing residential properties by issuing digital securities on the Ethereum blockchain to represent fractionalized ownership. They are actively operating in the Detroit market and only accept Accredited Investors. Rental payments are paid automatically to Ethereum wallets that hold RealTokens, and rent is paid in the Dai stablecoin. Tokens can be sold directly on the RealT website or through Uniswap.[45]

Figure. Figure uses a blockchain system to allow homeowners to borrow against their home equity, provides an alternative to reverse mortgages, and refinance mortgages and student loans. The company has originated more than $700

[43] Joanne Clever, "Could blockchain technology transform homebuying in Cook County--and beyond?" *Chicago Tribune,* 9 July 2018. https://www.chicagotribune.com/real-estate/ct-re-0715-blockchain-homebuying-20180628-story.html.

[44] "TruSet and Imbrex Partner to Create the First Blockchain-Based State-By-State Collection of Residential Real Estate Contracts," June 2019.

[45] RealT: https://realt.co/.

million in loans and was valued at $1.2 billion in its latest Series C funding round. The blockchain platform developed by Figure, Provenance.io is used to originate, finance, and sell home equity lines of credit (HELOCs) to banks, asset managers, and credit funds.[46]

Propy. Propy is a blockchain-powered platform that connects real estate brokers, buyers, and sellers and allows them to close deals online. They also provide tools for real estate agents. The venture capital arm of the U.S. National Association of Realtors (NAR) has invested an undisclosed amount.[47]

General Public. Many articles are available online about how individuals are using Bitcoin and cryptocurrency to purchase real estate.[48]

Considerations and Opportunities for Blockchain Application

Real estate license issuance and recording. The California Department of Real Estate handles issuance and tracking of the California real estate license. States have different systems, so fraud can occur when individuals hold multiple licenses in different states. The Department of Real Estate could benefit from using a standard unique identifier blockchain system that is uniformly adopted by many states. Potential benefits include eliminating interstate fraud and streamlining interstate collaboration.

One initiative creating such a unique identifier blockchain system is a collaboration between the Real Estate Standards Organization (RESO)[49] and Consensys.[50] A proof of concept is in development and under discussion with Wyoming; project leaders are very keen to work with California. The state could consider whether to explore partnership to run a pilot.

Efficient title search. Title insurers create their own repositories of publicly recorded

[46] Ben Lane, "Blockchain lending startup Figure is now a billion-dollar company," *Housing Wire*, 6 December 2019.

[47] Benedict Alibasa, "US Realtors Association Invests in Blockchain Startup Propy," *Coindesk*, 10 June 2019. https://www.coindesk.com/us-realtors-association-invests-in-blockchain-startup.

[48] Kayla Matthews, "5 cities that let you buy real estate with bitcoin," *Cointelegraph*, 26 October 2017. https://cointelegraph.com/news/5-cities-that-let-you-buy-real-estate-with-bitcoin.

[49] Real Estate Standards Organization (RESO): https://www.reso.org/.

[50] ConenSys: https://consensys.net/.

documents nationwide. If the state provides more records digitally in a unified, easily accessible and authenticated manner, the title search process could be made faster and less resource-intensive. Title insurers could then choose to pass the savings on to the consumer. If prices remain high despite new efficiencies, transparent and easily accessible data could allow new entrants to enter the space, enabling competition to drive prices down.

Digital transformation. The usefulness of moving title registration systems into a modern, transparent data storage system (real time, standardized, structured, indexed, public) is the primary consideration. Storing title registration either in a more traditional database or on a blockchain-based system will make title research easier and more conclusive. Easier title research could reduce fraud, which might lower insurance rates in a competitive market. Standardization across the state in an open format would reduce the costs of search technology and could help define a national standard.

County-level search tools and private firms already aggregate this type of data. Making improvements to the technology to standardize the system, or making that system a public good rather than a private service has the potential for savings on title insurance.

Blockchain Implementation: Potential Barriers and Concerns

Current IT infrastructure. Further work is needed to understand how California's 58 counties record deeds. Each county likely has its own process, some of which are more technologically up-to-date than others. The California Department of Real Estate has an online search function for public license information, and the department will need to be consulted to understand the architecture of its database and personnel requirements.[51]

Technical decisions could increase fraud. Should California decide to move to open standards/APIs/feeds while public data continues to be maintained by county recorders, either permissioned or public blockchain systems may be considered as the underlying datastore.

[51] State of California, "Public License Information Search," California Department of Real Estate. http://criis.com/index.html, http://www2.dre.ca.gov/PublicASP/pplinfo.asp.

The success of any system will depend on the software built into it or on top of it – how data is validated when entered, who is offering to host replication servers, how errors are corrected, and what indexing and search tools are provided to the public. Solutions could be built on either open source datastores (like mysql or postgres), on proprietary datastores (like Oracle), or on blockchains.

Permissioned blockchain solutions may have advantages and disadvantages in how validation and replication are accomplished. Adopting more open rules for recording property transfers using unpermissioned or semi-permissioned blockchains would allow members of the public to directly record property transactions on a distributed ledger. While this is intuitively attractive, absent tremendous progress in digital identity, title fraud would likely be increased by such a system rather than decreased.

Security and privacy. As titles and real estate licenses are public records, security and privacy considerations are not as critical as in other potential use cases. However, inappropriate use of public records remains an issue.

VEHICLES AND PARTS – REGISTRATION AND TRACKING

Introduction

The California Department of Motor Vehicles holds customer demographics, identity, residency, and social security number (SSN) verification status for 80% of Californians.[52] This data is used by employers, government entities, and insurance companies.

The estimated total of vehicle registrations at year-end 2019 was 36,423,657.[53] This represents a 2 percent increase, or approximately 716,000 more vehicles over 2018. In 2019, the estimated number of out-of-state cars being registered in California was 249,186.

Inauthentic auto parts have become a dangerous increasingly large market. The

[52] Correspondence with Ajay Gupta, Chief Digital Transformation Officer, California DMV, May 2020.

[53] "Estimated Vehicles Registered by County, January 1 through December 31, 2019." https://www.dmv.ca.gov/portal/uploads/2020/06/2019-Estimated-Vehicles-Registered-by-County-1.pdf.

U.S. Immigration and Customs Enforcement's Homeland Security Investigations office leads the nation in investigations of fraudulent car parts and has stated that every single part of a car can be counterfeited.[54] When it comes to fake auto parts, the largest concern is safety since a part may underperform or fail completely, with disastrous consequences for human life.

Pilots and Related Case Studies

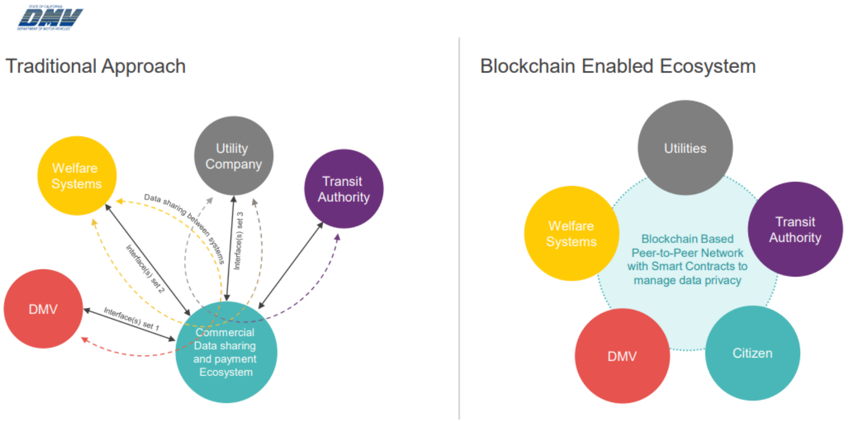
Department of Motor Vehicles Potential Use Case

The Department of Motor Vehicles (DMV), prior to the COVID-19 crisis, had been exploring innovative blockchain solutions to help increase efficiency, boost transparency and reduce economic costs. DMV was forced to put its research aside to focus their energy and resources on the COVID-19 crisis. The Blockchain Working Group encourages DMV to return to these discussions once timing is appropriate.

Additional information on these potential use cases are described below:

Use Case 1: Shared Citizen Verification

Create an empowered citizen with blockchain-based verification ecosystem

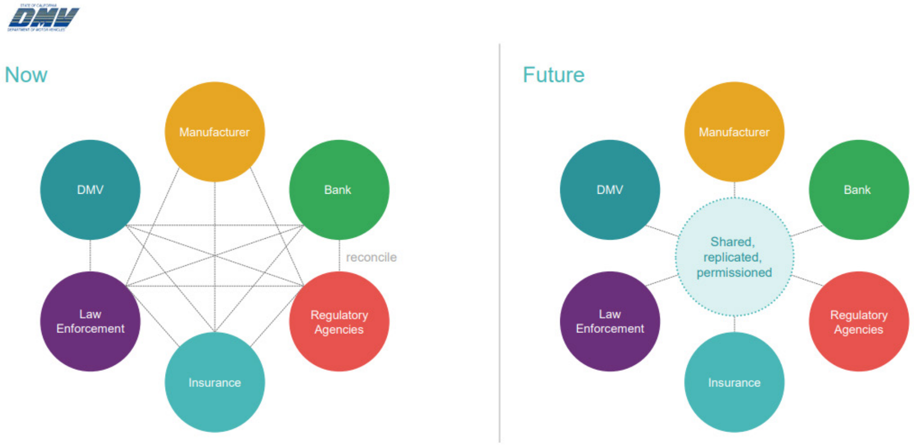

STATE OF CALIFORNIA
DMV
DEPARTMENT OF MOTOR VEHICLES
Traditional Approach
Welfare Systems
Utility Company
Transit Authority
DMV
Commercial Data sharing and payment Ecosystem
Data sharing between systems
Interface(s) set 1
Interface(s) set 2
Interface(s) set 3
Blockchain Enabled Ecosystem
Utilities
Welfare Systems
Transit Authority
Blockchain Based Peer-to-Peer Network with Smart Contracts to manage data privacy
DMV
Citizen

[54] Christina Vazquez, "Feds warn of counterfeit auto parts." *Local10 News*, 2 May 2016. https://www.local10.com/consumer/2016/05/02/feds-warn-of-counterfeit-auto-parts/.

This pilot could explore the creation of a digital wallet for the citizen, who would hold the authority of sharing their information with other entities once such information is verified by DMV (or another attested public entity). This would avoid repeated verification steps for customer and State/public service entities, resulting in reduced workload, economic benefits and auditability. Information sharing could constitute simply sharing verification status or verification documents.

Use Case 2: Tracking Vehicle Lifecycle

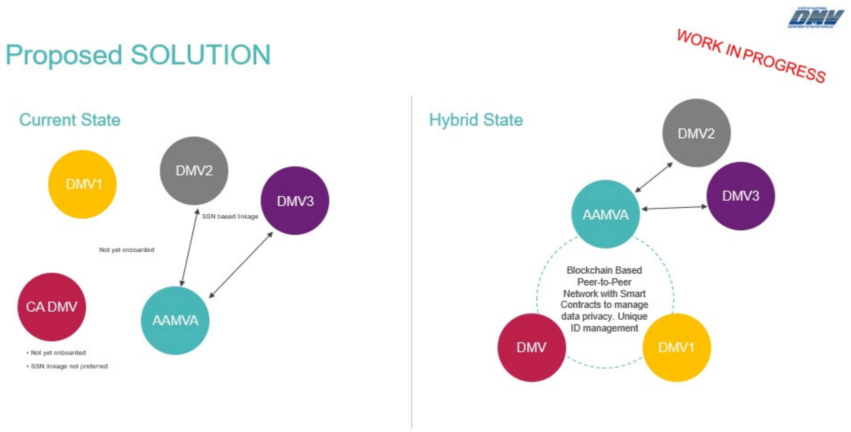
Create a simpler tracking system with in-built fraud reduction



This pilot could build a common blockchain platform where all the stakeholders participate towards title transfer transactions for a specific vehicle identification number, or VIN, which could simply the effort of maintaining point-to-point interfaces and also make the data readily available for analysis (salvaged, accident damage, illegal transfers), as well as information sharing by regulatory and law enforcement entities.

Use Case 3: State to State

Create fine-grained security for sharing driver records across states



Proposed SOLUTION

WORK IN PROGRESS

Current State
DMV1
DMV2
DMV3
SSN based linkage
Not yet onboarded
CA DMV
AAMVA
• Not yet onboarded
• SSN linkage not preferred
Hybrid State
DMV2
AAMVA
DMV3
Blockchain Based Peer-to-Peer Network with Smart Contracts to manage data privacy. Unique ID management
DMV
DMV1

This pilot could create a common blockchain platform where already participating states can continue to use existing hub and spoke mechanisms that they have already invested in, while new States and the American Association of Motor Vehicle Administrators' system (including the States supporting their undocumented migrant population) get onboarded on a blockchain system and share a unique ID (non Social Security Number) across the ecosystem with a mapping back from AAMVA to Social Security Number–based tracking system

Several companies are innovating with blockchain in the automotive industry:[55]

Autoblock: Uses blockchain ecosystem to buy and sell cars.

Axt: Offers a robust vehicle history report to consumers, dealers, and lenders.

BigChainDB: Provides ownership transfer pass that includes title, service providers, prior damage, maintenance, and inspection history to fight fraud.

GEM: Provides insurance charges based not only on distance but also driving behavior.

[55] "10 Blockchain Startups Disrupting The Automotive Industry," *Startus Insights*, January 2019. https://www.startus-insights.com/innovators-guide/10-blockchain-startups-disrupting-the-automotive-industry/.

One Car Payment: Consolidates all vehicle payments into one single monthly fee to help consumers save money.

VLB: Provides increased transparency of spare parts and reduced costs for vehicle maintenance and repairs.

Ownum's CHAMPtitles: Ownum's CHAMPtitles product is a blockchain portal for processing vehicle titles. They aim to simplify the process that typically includes a consumer, a car dealer, a manufacturer, a bank, an insurance company, a state DMV, and a title-issuing authority such as a county recorder. Digital collaboration solutions pre-blockchain would not have worked due to leakage of data through systems' metadata, making each organization wary of leaking proprietary information.[56]

Considerations and Opportunities for Blockchain Application

Efficiency and minimizing fraud. The DMV would benefit from improvements in data handling, which would in turn benefit its constituents. In the current auto title transfer process, there is considerable lien sale fraud and revenue loss for the State, which could potentially be minimized or eliminated with technological improvements. A set of service providers also integrates with DMV systems to provide paid support to dealers and individuals. Streamlined data collection and retrieval could additionally benefit law enforcement and regulatory bodies.

Tracking vehicle lifecycle. In California, the DMV could develop a blockchain platform to track the vehicle lifecycle. Each car owner, starting with the manufacturer, would be required to transfer title of a new or used vehicle to the seller. Not only would new and used vehicles be subject to the transfer process, impounded vehicles up for auction and vehicles going to dismantlers and junkyards would also undergo the transfer process. The existing process is labor-intensive for the DMV staff and individual owners. A common blockchain platform that tracks auto titles for specific VINs would make it easier to track data such as vehicles salvaged, involved in accidents, and illegally transferred.

Vehicle recording. A blockchain system could record each vehicle as it rolls off the

[56] Andrew Westrope, "Startup Ownum's First Product Is Blockchain Vehicle Titles," *Government Technology*, 22 March 2019. https://www.govtech.com/biz/Startup-Ownums-First-Product-is-Blockchain-Vehicle-Titles.html.

production line by writing details such as make, model, and price upon transfer to the dealer. When the vehicle is sold, the dealer would share the customer data with the DMV so the DMV could check the vehicle's history, verify the owner's details, and confirm registration. Smart contracts could automatically assign license plates and creation of new records such as title and registration. Continuous updates to the vehicle's record could facilitate insurance claims and manufacturer recalls. Law enforcement and regulatory agencies could also access the data to trace illegal auctions and sales.

Trust. Given that many parties do not necessarily want to share all their data, blockchain technology may be appropriate for selective data sharing among multiple people and organizations.

Overall benefits include:

- Updated and consistent vehicle information
- Reduced cost and time for vehicle transfers
- Simpler workflow for the DMV and consumers, leading to faster service and lower costs
- An agreed-upon, complete vehicle transaction history
- Same validated record for all parties
- Vital information source for fraud detection, warranty, service, and more
- Creates the potential for Internet of Things (IoT) vehicle linkage, for instance to automatically pay for tolls or parking or even annual registration fees

Blockchain Implementation Potential Barriers and Concerns

IT infrastructure. Additional follow up with the DMV is needed to determine the state of current infrastructure and staff available.

Security and privacy. Vehicle, vessel, driver's license and identification card records are open to public inspection in California. Confidential information such as social security numbers and addresses may only be disclosed to a court, law enforcement agency, or other authorized individual. Therefore, if a blockchain or alternative system is implemented, the DMV must still take care to protect confidential information and to verify access to this data.

Digital identity. Trustworthy digital identity is essential to the success of blockchain applications since the owner of the vehicle is tied to title, registration, insurance, etc. Accidents could also be recorded including involved parties.

Key challenges to be considered for blockchain application include:

- Consent must be obtained from all participating parties and partners
- Data-sharing policies must be agreed upon, including resolution processes for unauthorized read or write access, or potential for memorializing mistakes
- Cost of time and resources to implement, while considering ability for future upgrades

PROPERTY INSURANCE

Introduction

The California Department of Insurance (CDI) regulates the insurance industry and protects consumers. California is the largest insurance market in the United States, with annual direct premiums of $310 billion. It is also the fourth largest insurance market in the world. Almost 1,400 employees work at the CDI to oversee more than 1,400 insurance companies and license more than 420,000 agents, brokers, adjusters, and business entities. The CDI recovers more than $84 million a year for consumers. The CDI enforces insurance laws of California and has oversight over how insurers and licensees conduct business in California.[57]

Property and casualty insurance includes title insurance, auto, commercial, and home insurance. According to the CDI, the written premiums in 2018 for property and casualty in California was $75 billion.[58] Of note, homeowners insurance was $8.3 billion of the total while private passenger auto was $29.9 billion. The current claims processing system is highly manual, and it is estimated that blockchain and smart contracts could make the process significantly faster and cheaper. While insurance is generally run by private companies, the CDI and the State of

[57] California Department of Insurance: http://www.insurance.ca.gov/.

[58] 2018 California Property & Casualty Market Share, California Department of Insurance. http://www.insurance.ca.gov/01-consumers/120-company/04-mrktshare/2018/index.cfm.

California control regulation and insurance law, which affect private companies' ability to adopt new technologies.

Pilots and Related Case Studies

None of these insurance examples involve the state directly but rather come from private industry.

First American Financial. First American is one of the leading title insurers in the United States, with revenues of $6.2 billion in 2019.[59] In 2018, First American announced the launch of a blockchain system for the real estate title production process.[60] This platform has the goal of enabling the exchange of previous title insurance policies between underwriters that participate in the system. Old Republic Title Insurance, the third-largest title insurer in the U.S., has agreed to participate. First American designed the system and did not disclose details of the technology used. Each policy in the system is coded with a unique property identifier to enable accurate searches. First American says it is already common practice for title insurance underwriters to share policy information to reduce risk and increase efficiency.[61]

State of Vermont Study. As noted in a blockchain study by the state of Vermont, "blockchain technology offers no assistance in terms of reliability or accuracy of the records contained on the blockchain; if bad data is used as an input, as long as the correct protocols are utilized, it will be accepted by the network and added to the blockchain."[62] Therefore, some organizations like the American Land Title Association (ALTA) conclude that blockchain may enable efficiencies

[59] First American Financial: https://www.firstam.com/news/2020/fourth-quarter-and-full-year-2019-results-20200213.html

[60] "Real estate title insurance blockchain launched by First American," *Ledger Insights*, 2019. https://www.ledgerinsights.com/real-estate-title-insurance-blockchain-launched-by-first-american/.

[61] Ben Lane, "Old Republic will use First American-designed blockchain solution," *Housing Wire*, 28 November 2019.

[62] "Blockchain Technology: Opportunities and Risks," State of Vermont, 15 January 2016. https://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf.

in the title insurance process, but would not replace the need for human oversight in the form of title insurance professionals.[63]

Lemonade. Lemonade uses artificial intelligence and blockchain to offer renters and homeowners insurance. Lemonade takes a fixed fee from each monthly payment and allocates the rest toward future claims. Smart contracts verify losses for claims so payments are made faster than in traditional insurance. One could employ similar ideas for auto insurance and claims.

openIDL. Open Insurance Data Link, or openIDL, is an open blockchain network that streamlines regulatory reporting and provides new insights for insurers, while enhancing accuracy and timeliness for regulators.[64] It streamlines the statistical reporting process, and is governed by the American Association of Insurance Services (AAIS) using the IBM Blockchain. AAIS is the only national, not-for-profit insurance advisory organization and authorized statistical agent.

The Institutes RiskStream Collaborative. The RiskStream Collaborative is an industry-led consortium collaborating to use blockchain for risk management in insurance.[65] Members consist of over 40 leading risk management and insurance companies, many of which are household names. Currently, seven use cases are being designed or built, and three applications are expected to be delivered in 2020.

Non-Property & Casualty Insurance Examples. While not in the property category, companies such as Etherisc started with a product providing automated insurance payouts if a flight is delayed or cancelled.[66] It has since started planning blockchain-based insurance for hurricane protection, crypto wallet insurance, collateral protection for crypto-based loans, crop insurance, and social insurance. Companies like ReGa have started offering blockchain-based pet insurance.[67]

[63] Zachary Kammerdeiner and Ashley Sadler,"Blockchain Can't Protect Property Rights, but Title Insurance Can," American Land Title Association, 19 April 2018. https://www.alta.org/news/news.cfm?20180419-Blockchain-Cant-Protect-Property-Rights-but-Title-Insurance-Can.

[64] OpenIDL: https://aaisonline.com/openidl.

[65] The Institutes RiskStream Collaborative: https://web.theinstitutes.org/riskstream-collaborative.

[66] Etherisc: https://etherisc.com/.

[67] Nina Lyon, "First Mutual Pet Health Insurance Service on Ethereum Platform," *Coin Idol*, 14 March 2017. https://coinidol.com/pet-health-insurance-service-on-ethereum/.

Considerations and Opportunities for Blockchain Application

Efficiency and improved customer experience. The purpose of title insurance is to pay for losses occurring from a defect in the title and any resulting litigation. When purchasing real estate, lenders usually require title insurance, and cash buyers often also buy it. Potential title issues could include property alterations, tax liens, encroachments, and divorce claims. If title insurers share access to previous searches and insurance, it should streamline the whole process, providing better efficiency, pricing, and customer experience. To date, progress in advancing this system has been sluggish.

Since insurance is operated by private companies, the companies themselves could gain from improvements in operations, potentially benefiting the consumer with greater access, better service, and lower prices. While many in legacy insurance industries would like to keep the status quo in order to protect jobs and margins, others argue that change is inevitable and the industry should adapt with the times.

Security and privacy. From the State's perspective, security and privacy are not significant issues, apart from potentially upgrading systems of record that insurance companies rely on. Because these are typically public records, security and privacy concerns would be lower than other use cases.

Use of smart contracts. The use of smart contracts in an insurance context could shorten the execution time of events such as claim payouts. Remittances could be automatic instead of manual, escrow may no longer be necessary, there could be costs savings, and a virtual signature could negate the need for a physical presence. Peer-to-peer networks could be established via smart contracts to self-insure, without the need for an intermediary or administrator.

Role of government to encourage private industry. While property insurance is operated by private industry, government can play a role by encouraging innovation through regulations. Since streamlining insurer operations could have significant benefits for constituents in terms of pricing, access, and convenience, the state could encourage private industry to adopt blockchain technology as appropriate. California should keep an open dialogue with industry to advance legislation and policies that provide benefits to the consumer while minimizing potential risks, such as loss of privacy.

FIREARMS

Introduction

Within the United States, databases for firearm tracking and background checks are managed at the federal and state level. The FBI uses the National Instant Criminal Background Check System (NICS) to ensure firearms purchasers are eligible to own a firearm under federal and state law.[68] The Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) operates the National Tracing Center (NTC), which tracks firearms involved in criminal investigations.[69]

In 2019, the California Department of Justice established a state-level firearm tracking system called the Automated Firearms System.[70] This electronic repository documents all firearm purchases and transfers within the state and includes information on firearm ownership, transfers, and purchases as well as registration of assault weapons, Carry Concealed Weapons Permit records, and law enforcement records. Individuals must update their personal information and firearm information through the California Firearm Application Reporting System (CFARS), and information is verified before an individual can purchase a firearm or ammunition.

Pilot and Related Use Cases

Some literature exists on the potential applications of blockchain in firearm tracing. A 2018 article by Professor Thomas Heston from Washington State University explains how blockchain could theoretically be used to trace firearms:

> “Individuals currently owning a gun or purchasing a gun would get an electronic gun safe, similar to a bitcoin (BTC) wallet. This wallet would ideally be tied to biometric data such as a retina scan or fingerprint. Whenever a gun was created, purchased or sold, the transaction from one electronic gun safe to another would be recorded on the

[68] FBI, National Instant Criminal Background Check System (NICS): https://www.fbi.gov/services/cjis/nics.

[69] ATF, May 2019, "Fact Sheet - National Tracing Center." https://www.atf.gov/resource-center/fact-sheet/fact-sheet-national-tracing-center.

[70] California Department of Justice, *Automated Firearms System Personal Information Update*. https://oag.ca.gov/firearms/afspi.

> blockchain in an immutable, time-stamped manner." Electronic gun safes would include pertinent information about the individual, such as criminal background and mental health background. Firearms transfers, purchases, or sales would be verified through a blockchain's immutable and time-stamped ledger.[71]

Related legislation. Some states, including Arizona, Missouri, and Tennessee, have proposed legislation and created statutes prohibiting mandatory firearm tracking using blockchain out of concerns for privacy.[72] Still, today most blockchain-based firearm tracking applications are theoretical.[73]

V.E. Utilities and Natural Resources

Key Recommendations

REC V.E.1. Energy sector. Additional discussion and research are required to determine whether the concept of a "regulatory sandbox" is feasible in California.

REC V.E.2. Water sector. The State should evaluate the opportunity for blockchain-based technology to support a more efficient framework that further leverages the momentum from recent California water data efforts. Addressing the needs of different stakeholders to control and monitor how they responsibly share water data could enhance the efficiency of regulatory efforts, support more transparent decision-making, and ultimately, increase trust among stakeholders.

ENERGY SECTOR

Introduction

Blockchain is a flexible technology that theoretically has dozens if not hundreds of potential applications in the utilities and natural resources sectors. While it has the capacity to facilitate changes and enhancements in these sectors, many blockchain applications are still hypothetical or have been tested only within

[71] Heston, "A Blockchain Solution to Gun Control," *Int'l Journal of Scientific Research* 7.

[72] California Senate Office of Research, *Issue Primer - Blockchain Technology*, June 2019.

[73] J. Francis, "Could Blockchain Impact Gun Control?" *Bitcoinist*, 23 February 2018. https://bitcoinist.com/blockchain-impact-gun-control/.

limited pilot projects. Of these, most of the work has centered on the energy sector, and this is reflected in the media discourse, academic research and project analyses. For this reason, this report primarily considers examples in the energy sector with a limited focus on applications in other parts of the utilities and natural resources sectors.[74]

Pilots, Research, and Related Use Cases

Silicon Valley Power (City of Santa Clara) Electric Vehicle Pilot Project. Power Ledger partnered with Silicon Valley Power, a not-for-profit municipal electric utility owned and operated by the City of Santa Clara, "to monetize electric vehicle infrastructure, creating the potential for tokenized energy."[75] The platform was used to help Silicon Valley Power prepare and submit regulatory reports for the California Air Resource Board's Low Carbon Fuel Standard. This proof-of-concept project was considered a success and ended in 2019.[76]

Sacramento Municipal Utility District Electric Vehicle Pilot Project. The Sacramento Municipal Utility District (SMUD) in 2019 announced an initiative that "will utilize blockchain-enabled tokens as part of an effort to encourage EV owners to charge their vehicles at workplaces when local renewables peak during the day."[77] The charger automatically begins charging when a surplus of energy is available, and consumers are charged a discounted rate. Consumers will be offered "rebates or credits on charging that they can accumulate as blockchain-enabled tokens."[78]

[74] Thanks to Dana Nothnagel, Executive Fellow of the California Research Bureau, for her research assistance in this section.

[75] Power Ledger, "Tokenization of renewable energy credits." https://www.powerledger.io/project/santa-clara-united-states/.

[76] Interview with Duncan McGregor, Power Ledger, 13 January 2020.

[77] Paul Ciampoli, "SMUD official details electric vehicle blockchain project," American Public Power Association, 27 September 2019. https://www.publicpower.org/periodical/article/smud-official-details-electric-vehicle-blockchain-project.

[78] Ciampoli, "SMUD official details electric vehicle blockchain project."

Considerations and Opportunities for Blockchain Application

Smart contracts. As demand for decarbonized energy grows, the energy sector is experiencing a shift toward more digitized and decentralized operations.[79] In their article titled "Blockchain Applications in Smart Grid – Review and Frameworks," Musleh, Yao, and Muyeen explain that "the main challenge [for the energy sector] is the appearance of the new type of grid user called the prosumer, who produces and consumes electrical energy in a local area."[80] Blockchain could provide the technology needed to support prosumers, for example through smart contracts embedded in peer-to-peer (P2P) energy trading systems, and facilitate greater use of renewables.[81] However, most experts agree that we are in the early stages of understanding this use case. "We are still decades away from transactive energy," said Marzia Zafar, who was Director of Innovation and Insights at the World Energy Council when research was conducted for this report.[82]

Modernized grids and improved energy transfer. Modern grid concepts like smart grids, microgrids, and peer-to-peer energy transfer are popularly cited solutions to facilitate energy decarbonization, as well as potential blockchain use cases in the utilities sector. Fundamentally, energy grids need greater flexibility in order to accommodate energy from multiple sources, rather than from a single centralized utility. All of these modernized grid concepts may be used separately or simultaneously within a system and can increase energy resiliency and better integrate renewable resources.

Blockchain is a promising platform for these applications in a variety of ways. Blockchain could allow for detailed data collection on power consumption and creation from multiple sources. Data could be shared in real time with any

[79] Interview with Marzia Zafar, World Energy Council, 21 January 2020; Andoni, Merlinda et al. "Blockchain technology in the energy sector: A systematic review of challenges and opportunities," *Renewable and Sustainable Energy Reviews*, 100: 144, February 2019. https://www.sciencedirect.com/science/article/pii/S1364032118307184; Marzia Zafar, "Blockchain/The emerging of active consumer: Developing A Smarter Network," *World Energy* 58, October 2019.

[80] Ahmed Musleh et al., "Blockchain Applications in Smart Grid – Review and Frameworks," *IEEE Access* 7, 17 July 2019. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8730307.

[81] Musleh et al., "Blockchain Applications in Smart Grid – Review and Frameworks."

[82] Interview with Marzia Zafar, World Energy Council, 21 January 2020.

number of users and system managers, and the platform could automatically execute transactions. This is key to a grid that incorporates energy from multiple sources at once. Blockchain can also tokenize energy credits, making it possible to trade energy within a grid of many different users.[83]

Mike Orcutt, writing for the *MIT Technology Review*, explains the transition from a centralized grid to a decentralized, blockchain-based grid:

> The electricity sector is, for the most part, still based on massive, centralized power plants that generate power sent long distances over transmission and distribution lines. In recent years, though, a growing number of smaller 'distributed' power generators and storage systems, like rooftop solar panels and electric-vehicle batteries, have been connecting to the grid.
>
> The owners of these systems struggle to maximize their value because the system is so inefficient... For instance, it generally takes 60 to 80 days for an electricity producer to get paid. With a blockchain-based system...producers can get paid immediately, so they need less capital to start and run a generating business.[84]

Blockchain-enabled grids could eventually have a significant impact on the energy industry. In fact, "investment banking firm Goldman Sachs predicts that using blockchain to facilitate secure transactions of power between individuals on a distributed network could result in transactions worth between $2.5 – $7 billion annually."[85]

Julie Hamill of the International County/City Management Association (ICMA) writes that although blockchain is not necessary for a microgrid to function, "blockchain in a microgrid system will provide more transparency and efficiency."[86]

[83] Andoni, "Blockchain technology in the energy sector."

[84] Mike Orcutt, "How Blockchain Could Give Us a Smarter Energy Grid," *MIT Technology Review*, 16 October 2017. https://www.technologyreview.com/s/609077/how-blockchain-could-give-us-a-smarter-energy-grid/.

[85] Julie Hamill, "Blockchain Technology: Local Government Opportunities and Challenges," ICMA and GFOA white paper, November 2018. https://icma.org/sites/default/files/2018-Nov%20Blockchain%20White%20Paper.pdf.

[86] Hamill, "Blockchain Technology: Local Government Opportunities and Challenges."

Improved data collection, transparency. Even without restructuring distribution systems, utilities could use blockchain to improve data collection, which might streamline wholesale energy trade as well as internal administrative functions like billing and data validation.[87] As with the modernized grid examples, utilities could collect real-time information from nodes at any level of the distribution process, whether to track fuel supply for power plants, monitor electrical lines, or gather data on individual home energy use. Improved data collection through blockchain could lower costs and increase efficiency for both utilities and ratepayers.[88] A benefit to exploring blockchain-enabled back-office solutions is that these administrative applications may encounter fewer regulatory restrictions compared to the front-end applications that may affect how energy is used or sold.[89]

Because of its qualities as an immutable ledger and platform for sharing data, blockchain could allow utility operators to better detect breaches or faults in distribution systems. It could also improve trust among regulators, utilities and consumers. "Blockchain can introduce a level of transparency not currently seen in the energy sector," said Marzia Zafar of the World Energy Council.[90] Zafar explained that the transparency and traceability benefits offered by a blockchain platform could help move regulation from a reactive process to a proactive process. Tony Giroti of the Energy Blockchain Consortium confirmed the value of blockchain in utility regulation. "From the regulator's perspective, there is a guarantee that the data has not been tampered with. It provides the immutability of data and the provenance of that data."[91] Data could also be shared with auditors, helping to reduce auditing costs and other administrative costs.

Carbon monitoring and trading. Blockchain technology may also be a valuable tool for carbon monitoring and trade. According to the United Nations Climate Change Secretariat, blockchain could improve carbon emission trading by guaranteeing transparency and validating and settling transactions

[87] Andoni, "Blockchain technology in the energy sector."

[88] Andoni, "Blockchain technology in the energy sector."

[89] Interview with Marzia Zafar, World Energy Council, 21 January 2020.

[90] Interview with Marzia Zafar, World Energy Council, 21 January 2020.

[91] Interview with Tony Giroti, Energy Blockchain Consortium, 17 January 2020.

automatically.[92] It could also enable enhanced climate finance flows by developing transparent crowdfunding and peer-to-peer financial transactions in support of climate action. Finally, blockchain could allow for better tracking and reporting of greenhouse gas emissions; the transparency and efficiency of the system could improve emissions progress in monitoring and mitigate tracking issues like double counting.[93] At this point, blockchain use for carbon monitoring and trading is still preliminary. IBM has partnered with Energy Blockchain Lab to create a new platform for monitoring carbon footprints and buying carbon credits in China.[94] The success of this program could demonstrate the effectiveness of blockchain in this sector.

Blockchain Implementation: Potential Barriers and Concerns

Regulatory environments are not constructed for peer-to-peer transactions. The utilities and natural resources sectors often exist within highly structured regulatory environments, but the implementation of emergent blockchain technology does not always align within this existing structure. Dr. Neil Wasserman, professor of computer science at George Washington University, says that from his perspective, "a key obstacle to making [blockchain] work is the interface between the legal environment under which we understand transactions and software environment under which we understand transactions." [95] Blockchain allows for transactions and data collection in ways that regulations are not currently structured to manage.

For example, a microgrid pilot project in Brooklyn encountered the following obstacles: "by law, individuals are not allowed to sell or buy electricity directly from each other. Brooklyn Microgrid participants are buying and selling tokens for energy credits, rather than actually exchanging U.S. dollars for electricity."[96]

[92] United Nations Climate Change, "How Blockchain Technology Could Boost Climate Action," United Nations Framework Convention on Climate Change, 1 June 2017. https://newsroom.unfccc.int/news/how-blockchain-technology-could-boost-climate-action.

[93] United Nations Climate Change. "How Blockchain Technology Could Boost Climate Action."

[94] IBM, "Energy Blockchain Labs Inc," January 2018. https://www.ibm.com/case-studies/energy-blockchain-labs-inc.

[95] Interview with Neil Wasserman, George Washington University, 13 January 2020.

[96] Hamill, "Blockchain Technology: Local Government Opportunities and Challenges."

The ICMA's Julie Hamill observes that "for blockchain to enable distributed energy users to transact directly in energy sales, the existing laws must be changed."[97] The coordinators of the pilot project have engaged in discussions with New York regulators to "sell energy through a utility bill, as required in New York State," without being subject to the same state utility regulations.[98] In this situation, the prohibition is not against blockchain but against peer-to-peer energy sales. That is, buying and selling energy directly under a regulatory scheme that prevents it would not be allowed whether the technology enabling the transfer was blockchain, some other form of distributed ledger technology, or a low-tech solution altogether. While regulations prevent large-scale structural changes to the energy distribution system, they do not prevent the use of blockchain itself.

Some industry experts argue that uncertainty within the law regarding blockchain prevents companies from experimenting with the technology regarding the tokenization of energy credits.[99] Parts of Europe and Australia have created regulatory "sandboxes" that give companies more freedom to test new technology like blockchain. Similar to discussions in this report related to financial instruments, regulatory sandboxes may offer a similar opportunity for energy in California, though more research and analysis is required.

Much like other new technologies, stakeholders share a concern that regulating blockchain this early in its development could stifle technological progress. Zafar writes, "regulators must clearly state their philosophy and long-term vision: The current regulation is defined for vertically integrated utilities. Regulators need to redefine policies so they are suitable for and do not unintentionally constrain new business models enabling transactive energy systems."[100]

Lack of fully vetted projects. Amy Ahner, Director of Administrative Services, Village of Glenview, Illinois, and member of the International City/County Management Association Smart Communities Advisory Board, explained that one of the biggest barriers to implementing large scale blockchain projects is the lack of "fully vetted projects that are actually going through the whole process of case study, prediction, operational impacts, integration requirements, and studying

[97] Hamill, "Blockchain Technology: Local Government Opportunities and Challenges."

[98] Hamill, "Blockchain Technology: Local Government Opportunities and Challenges."

[99] Interview with Duncan McGregor, Power Ledger, 14 January 2020.

[100] Marzia Zafar, "Blockchain/The emerging of active consumer: Developing A Smarter Network."

the regulatory process."[101] Giroti notes that "all the current use cases right now are very preliminary."[102] For California, this means that large-scale changes to regulatory structures must be based on anticipated changes because most projects are still in the proof-of-concept stage.

NATURAL RESOURCES

Introduction

Theoretically, blockchain could enable a multitude of technological advancements in the natural resources sector. Most information on this use case surrounds supply chain management (see section above). Smart contracts could facilitate costly transactions between suppliers and vendors in the utilities sector as well, and easily accessible ledgers could reduce auditing costs.[103]

Water Management. California was the first state in the United States to formally recognize the human right to water.[104] Still, California faces significant water management challenges to mitigate the impact of droughts, floods, and other water supply disruptions. Improved data collection and access will help the State address and overcome these challenges. The State already affirmed its commitment to open water data through the 2016 Open and Transparent Water Data Act (AB 1755), which makes water and ecological data more readily available and will help inform the State's approach to water management.[105]

Pilot Projects and Related Use Cases

Freshwater Trust, Solano County, CA. Alex Johnson, from the Freshwater Trust, is using a blockchain platform created by IBM to help farmers trade water in Solano County. Johnson deployed "simple, solar powered sensors, originally

[101] Interview with Amy Ahner, ICMA, 14 January 2020.

[102] Interview with Tony Giroti, Energy Blockchain Consortium, 17 January 2020.

[103] Felipe Mota da Silva and Ankita Jaitly, "Blockchain in Natural Resources: Hedging Against Volatile Prices," TATA Consultancy Services, March 2018. https://www.tcs.com/content/dam/tcs/pdf/Industries/energy_resources_and_utilities/Blockchain-in-Natural-Resources-Hedging-Against-Volatile-Prices.pdf.

[104] Office of Environmental Health Hazard Assessment, "The Human Right to Water in California," 14 October 2019. https://oehha.ca.gov/water/report/human-right-water-california.

[105] California Department of Water Resources (2020), AB 1755: Open and Transparent Water Data Platform for California. https://water.ca.gov/ab1755.

developed to monitor creaky groundwater pumps in East Africa. The sensors will be used to detect how much water is flowing in real-time."[106] Using that data, farmers will then be able to trade water on a blockchain platform. This project relies on smart contracts to facilitate the agreement between parties. This pilot project demonstrates the potential value of blockchain in aquifer management, but many regulatory and geographic challenges must be overcome before this technology can be implemented more widely.[107]

Considerations and Opportunities for Blockchain Application

Blockchain could facilitate more effective coordination of water data and allow stakeholders immediate access to it. The decentralized, auditable, and transaction-oriented nature of a blockchain approach could make data about water quality and quantity more accessible across a variety of sectors. Streamlining the exchange of information through a cooperative system with a verifiable ordering of transactions and appropriate user permissions would enable new efficiencies and innovations, from helping to inform constituents about the safety and availability of water in their area to guiding water conservation efforts.[108] Alex Johnson from the Freshwater Trust notes that there is a level of distrust in California's water sector. For this reason, Johnson argues that blockchain "allows a group of people who don't necessarily trust each other to make deals, without the need for third-party oversight."[109]

[106] Matt Black, "How the Blockchain Could Protect California's Aquifer," *Wired*, 26 April 2019. https://www.wired.com/story/how-blockchain-could-protect-californias-aquifer/; J. O'Connell, "Thirsty California May Be Wary of Blockchain Water Rights," *Cointelegraph*, 12 March 2019. https://cointelegraph.com/news/thirsty-california-may-be-wary-of-blockchain-water-rights.

[107] Barber, "How the Blockchain Could Protect California's Aquifer."

[108] Callie Stinson, "How blockchain, AI, and other emerging technologies could end water insecurity," *GreenBiz*, 2 April 2018. https://www.greenbiz.com/article/how-blockchain-ai-and-other-emerging-technologies-could-end-water-insecurity.

[109] Barber, "How the Blockchain Could Protect California's Aquifer."

V.F. Finance, Payments and Commercial Business

Key Recommendations

REC V.F.1. Welfare and entitlement programs. Any pilots should be done at a small scale that will not negatively affect vulnerable populations who rely on these services. To our knowledge, blockchain has not yet been used for entitlements, welfare, or social benefits by any government in the United States.

REC V.F.2. Taxes and revenue. Evaluate and study the potential for blockchain application to better administer, collect, and detect fraud related to sales and use taxes.

REC V.F.3. Bonds and public finance. Research blockchain-based digital municipal bond issuance programs and the creation of a consortium to manage negotiation of bond issuance fees for the State of California. These universal fees would be implemented via blockchain.

REC V.F.4. Public banking. The State of California should monitor developments in public banking and potential opportunities to integrate blockchain technology.

REC V.F.5. Digital Asset Banks. Define a framework for Special Purpose Depository Institutions (SPDI), and subsequently grant existing banks a charter to bank Digital Assets would enable greater monetization and overall growth of these new technologies.

REC V.F.6. Cannabis and banking. California should explore the use of 1) public banks; 2) digital asset deposit and custodial institutions; and 3) a regulatory sandbox for blockchain and cannabis innovators.

REC V.F.7. Government role in remittances. The State has a limited role in the remittance market, no recommendations at this time.

WELFARE AND ENTITLEMENT PROGRAMS

The Blockchain Working Group researched California's various social benefit and entitlement programs to explore where blockchain may be a good fit. Potential benefits include decreasing processing time of applications and decreasing fraudulent claims.

Blockchain Working Group members contacted experts in the state and were advised against any blockchain pilots in this area because of the potential to disrupt services that Californians depend on.

Although blockchain has not been used for welfare payments in the United States, other countries have conducted some implementations and pilots. The UK's Department of Welfare and Pensions attempted a small-scale pilot of blockchain technology in 2016 to distribute welfare payments, but found that it was not viable because of limited adoption and expensive costs.

The UN has also used the technology to distribute payments to refugees in refugee camps. UN officials have found the technology to be particularly appealing in the refugee context because it protects the privacy and security of migrants more than traditional database systems, and can withstand disasters that can destroy more centralized recordkeeping systems.

TAXES AND REVENUE

Introduction

Blockchain technology may be a tool in the administration, collection, and risk assessment and fraud detection, of all types of taxes. As discussed below, it may be more useful in the administration of sales and use taxes than income taxes.

Income tax. For income taxes, the California Franchise Tax Board has introduced a feature called Cal-File, a simplified form and process for W-2 income tax filers to complete, submit and make payments or obtain refunds. This simplified process, and the underlying database technology, is already in place, with widespread adoption limited by lobbying from the return preparation industry (not by technology barriers). As such, blockchain technology is not needed to solve an existing problem for income tax administration and collection in California.

Gross-basis taxes. For sales and use taxes, which are gross-basis taxes based on transactions, blockchain technology could be useful to better administer and collect taxes and detect fraud. This application is worth further study and evaluation. Rather than prescribe how California should evaluate blockchain technology for use in sales and use tax administration, this section describes how two countries, the Netherlands and Thailand, are evaluating blockchain technology for use in value-added tax (VAT) administration and enforcement, in particular, in combating VAT fraud.

Value-added tax. Like sales tax, value-added tax is a tax on consumption and borne by consumers. Unlike sales tax, value-added tax is borne only by the ultimate consumer, with intermediaries "crediting" value-added taxes paid to its suppliers against value-added taxes charged and collected from its customers.

Use Case

Netherlands. The Netherlands has strongly encouraged the use of blockchain solutions to address the problem of VAT fraud. Two prototype solutions have emerged from the private sector, with a common requirement that all stakeholders to the system need to be on the same "network" or blockchain.

Microsoft/PwC's VAT Fraud Prevention Prototype: Microsoft and PwC Netherlands partnered to develop a VAT Fraud Prevention Prototype based on Microsoft's technical platforms.[110] Per the product materials, the VAT Fraud Prevention prototype is designed to enable implementation of blockchain technology in VAT Fraud Management in 3 phases:

> Phase 1. Information exchange:
> The first phase focuses on establishing the blockchain as a trusted platform for information exchange and logging, where all transactions are registered and exchanged between different stakeholders. Information exchange is critical to success in multinational environments (such as the EU) where establishing an architecture to exchange and share information between countries is complicated.
>
> Phase 2. Real-time VAT:
> The second phase focuses on how smart contracts can resolve the liquidity problem of the real VAT scenarios. Smart contracts will be

[110] Microsoft, Vertex, and PwC, "Two practical cases of blockchain for tax compliance," October 2019. https://www.pwc.nl/nl/tax/assets/documents/pwc-two-practical-cases-of-blockchain-for-tax-compliance.pdf. Vertex, "Two Applications of Blockchain for Tax Compliance," Vertex, Inc. 4 October 2019. https://www.vertexinc.com/resources/resource-library/two-appli-cations-blockchain-tax-compliance.

used to implement automated VAT payments between companies, automatically adjust VAT accounts of companies, automate the VAT returns from the tax administration agencies and minimize the administrative burden of managing VAT processes for businesses.

Phase 3. Cryptocurrency phase:
The last phase is the most advanced scenario and foresees that tax administration agencies will adopt and regulate a cryptocurrency. In this phase, business-to-business VAT transactions will use a cryptocurrency to automate the process and create incentives for the consortium governing VAT collection.

Attributes of the VAT Fraud Prevention Prototype include:

- The option to operate in a multi-national business environment where businesses from different countries exchange invoices.
- The Prototype splits companies into two groups: Whitelisted (WL) and non-Whitelisted (non-WL) companies. Whitelisted companies are those that have elevated tax control policies and demonstrated high tax compliance. They have a deferral period for the VAT payment as a reward for their historical high VAT compliance and an incentive to be an early adopter of the Prototype.
- All VAT payments are labeled and traced in the VAT ledger/trial balance. The trial balance is settled automatically at the end of a given period through smart contracts, when VAT is paid to the tax administration.
- Banks are members of the consortium and all transactions are implemented through the banking system. The implementation of the blockchain-based VAT includes a range of stakeholders, including tax administrations, corporate taxpayers, and financial institutions.

BONDS AND PUBLIC FINANCE

Introduction

California is the fifth-largest economy in the world and the largest issuer of municipal debt in the country ($60.6 billion in 2019).[111] California is also a leader in progressive ideas and tasked with addressing systemic challenges.

Municipal financing can play a role in addressing capital-intensive endeavors to reach these goals. The municipal debt market consists of two main instrument types, loans and bonds, and each offers opportunities related to blockchain technology.

Muni Bonds. The municipal bond market represents approximately $4 trillion in outstanding debt, with approximately $400 billion of new issuance per year. California is the largest issuer in the country, more than $60 billion annually. Most municipal bonds are available in $5,000 denominations and a tradable lot is generally considered anything greater than $250,000 in face value.[112]

The market is based on legacy processes, established when communications technology was in its infancy. Primary issuance is controlled by underwriters or broker-dealers, who purchase entire offerings directly from issuers and then distribute the bonds through their propriety sales channels. This is a closed process with limited transparency.

The current municipal bond market has evolved slowly over time. The most significant change in the past five decades has been the dematerialization of bond certificates and coupons. The removal of physical certificates has driven the consolidation of municipal debt securities into the Depository Trust Corporation (DTC) and wholly owned Cede & Co, which, acting as de facto transfer agent, owns substantially all the issued shares in the United States.

While municipalities are specifically identified as exempt issuers in the Securities and Exchange Act of 1933, almost all issues today are initiated through an

[111] State of California, "Governor Newsom Proposes 2020-21 State Budget," 10 January 2020. https://www.gov.ca.gov/2020/01/10/governor-newsom-proposes-2020-21-state-budget/.

[112] See https://california.municipalbonds.com/ for information about California Municipal Bonds.

underwriting process. Due to the participation of Broker-Dealers regulated by the Financial Industry Regulatory Authority (FINRA), the rules promulgated by the Municipal Securities Rulemaking Board (MSRB) come into play. The Municipal Issuer is not subject to MSRB or FINRA regulation, but the underwriter managing the issue is. That said, California has promulgated rules and procedures that both the State and municipalities in the State must follow.[113]

Considerations for improvement include the following:

The current market is outdated. The current market structure is hampered by antiquated processes and outdated technology.

Investor access is limited. Unlike the equity market, which trades on exchanges and is open to all market participants, the debt markets trade privately in over-the-counter (OTC) transactions. Consequently, large financial institutions can leverage these markets to the detriment of other investors. This hampers transparency and prevents genuine public oversight.

Borrowers are underserved. For municipal borrowers, the existing mechanisms for accessing capital contain multiple sources of friction, which can lead to higher costs and significant funding delays. Municipal debt is used to finance both long-term capital projects and short-term cash flows. Long-term capital projects are designed to maintain and improve public assets such as public infrastructure. Short-term financing is used for cash flow to manage the timing between income (tax, fees, fines), and expenses at the state and local levels.

Fees and Costs. Two categories of fees are recorded when municipal bonds are issued: costs of issuance and underwriting costs. Costs of issuance are an aggregation of a variety of costs, e.g., bond counsel, financial advisors, rating agencies, and bond experience, to name a few. Currently, each municipality negotiates these costs individually, but municipalities could join together and

[113] California State Treasurer, "California Debt Financing Guide." https://www.treasurer.ca.gov/cdiac/debtpubs/financing-guide.pdf.

negotiate as a group for better rates. Blockchain can facilitate transparency regarding rates and manage the costs of issuing bonds.[114]

Another important dimension of the municipal market is the cost to issue and trade. A 2015 report by the Haas Institute estimated that issuance costs (separate from the interest or coupon paid on debt) averaged 1.02% on a weighted basis and 2.05% on an unweighted basis (approx. $3 and $4 billion per year), with issues under $10 million experiencing substantially higher costs. Underwriting fees represented 46%, and bond counsel represented 15%.[115]

By considering blockchain technology, California may lead a technology update that enables greater transparency, expands investor access, deepens engagement with local financial institutions, improves efficiencies, and lowers cost.

Studies, Pilots and Related Use Cases

Jefferson County, Washington. The Brinnon Fire District recently funded two fire trucks on a blockchain platform. The investor was a local community bank, and the municipality and investor engaged directly on the platform, while incorporating guidance from bond counsel. The transaction required no underwriter, incurred no RFP (request for proposal) costs, and followed all state regulations.

Berkeley Micro Bonds. The City of Berkeley has issued an RFP to issue blockchain-based Micro Bonds for the purchase of a fire truck. Berkeley's goal is to leverage its tax-exempt status as a municipal issuer and the outsized local economic impact of its regular budget with the efficiencies of the blockchain token markets to offer a new kind of cost-effective, affordable, and scalable debt instrument.

Wyoming. Wyoming has recently passed legislation empowering municipalities to issue bonds as digital securities.[116]

[114] Mark Joffe, "Doubly Bound: The Costs of Issuing Municipal Bonds," Haas Institute for a Free and Democratic Society and Refund America Project, 2015. https://haasinstitute.berkeley.edu/sites/default/files/haasinstituterefundamerica_doublybound_cost_of_issuingbonds_publish.pdf.

[115] Joffe, "Doubly Bound."

[116] Wyoming Legislative Record; Adopted 3/12/2020; Effective 7/1/2020. https://wyoleg.gov/Legislation/2020/HB0020.

Considerations and Opportunities for Blockchain Application

The municipal market, including both bonds and loans, can benefit from a technology infrastructure that enables improved transparency, flexibility in funding options, more open access, and contract standardization. Blockchain technology is well suited to address these issues in a way consistent with the regulatory framework and objectives, and beneficial for both issuers and investors. Blockchain provides investors with certification upon purchase of assets in real-time, while appropriately recording and reporting the transaction with minimal fees. Blockchain token architecture offers a platform for payment systems as well as new types of financial instruments currently emerging from the Distributed Finance (or DeFi) community.

IT infrastructure. New administrative procedures will be required, but the basic structure of web/app access and digital identity authentication supported by cloud-based databases is already well understood.

The structure for tokens already exists. Adoption of e-wallets to facilitate transactions and holding is a non-technical matter of disseminating market information. In terms of network speed and access, current transmission rates from WiFi or cell phone service is sufficient at the end-user level, while commercial internet connections and cloud offerings are readily available at reasonable cost for administration.

The program itself would be an enterprise software implementation with some procedural updates. The benefits of affordable bond pricing increase the local velocity of money, and the ability to retain more offering fees would generate growth in local economies.

Security and privacy. Encryption is the gold standard for privacy, and security on the administration of the program would fall to the governmental entity itself, an SEC-regulated Transfer Agency, and/or a FINRA/MSRB Broker Dealer. Security and privacy are well understood and defined in terms of responsibility and procedures. Tokenization will add improved security models to existing frameworks.

Trust. When bonds are certificated into tokens, they are held in wallets controlled by the holder who can choose to continue to hold those certificates to maturity, transfer the certificates to another wallet (e.g., Coinbase wallet), or trade certificates with another wallet holder. In every case, the blockchain will record every movement of value as tokens are "spent" and created. While the ownership will be obscured by the nature of blockchain addresses, all transactions will be viewable by anyone with an internet connection and appropriate blockchain browser, and regulators will have real-time inspection powers.

Cost reduction and transparency. The advent of blockchain and related distributed ledger technologies presents an opportunity to change how fees are calculated. Tokenization of muni bonds can replicate legacy processes at lower costs and higher transparency. Such transparency provides opportunities for cost reduction because it allows issuers to benchmark their expenses against their peers. Blockchain can lower overall costs for government issuers by reducing costs of underwriting, distribution, contract complexity, reconciliation and transparency.

Flexibility. Blockchain technology allows California to issue bonds that can be certificated as tokens on public or private blockchain. If the State chooses to use a Transfer Agent to track ownership of each note and generally manage the project, it could give bond holders the option to choose whether to hold the security 1) directly registered with California; 2) on a blockchain of their choice; or 3) at the Depository Trust Company (DTC) (required for institutions but may be desired by retail investors).[117] The transfer agent could also act as a paying agent for the State and facilitate investor instructions to change their holdings between the three states of certification.

Given concerns regarding money laundering, the bonds should be issued as zero-coupon instruments where the difference between the issue price and the face value redemption represents the tax-free interest for investors.

Efficiency. Blockchain technology may enable the State of California, as well as its cities and counties, to issue bonds that are better, faster, and lower cost to both municipalities and investors. Blockchain allows assets to be exchanged or fractionalized while adhering to market regulations. Tokens allow for quicker

[117] Joffe, "Doubly Bound."

proof of ownership and demonstration of liquidity that will reduce market frictions and reduce operational costs. Blockchain will streamline settlement and clearing functions while offering community banks more opportunities and trades to fit individualized investment strategies. The process will underpin moves toward contract standardization with blockchain-enabled smart contracts. Eventually, blockchain will allow retail investors an opportunity to access the primary bond market.

Access and transparency. Blockchain can be used to replace outdated underwriting models with direct access at primary issuance, via a blockchain-enabled marketplace. As infrastructure develops, lower transaction size will enable retail investors to access the primary issuance market in a cost-effective way, with ongoing secondary market liquidity. Blockchain technology provides issuers, regulators, and investors with direct access to relevant data via blockchain nodes. Residents gain an opportunity to invest locally through blockchain mechanisms.

Blockchain Implementation: Potential Barriers and Concerns

Digital identity. Digital identity is critical for all participants in public banking using the most trusted models for authentication at every level.

Statutory and regulatory considerations. As municipal issuers are specifically exempted in the Securities and Exchange Act of 1933, the only barriers are those imposed by the State of California. For trading municipal securities in the secondary market, trades will follow the same regulations as regular securities transactions (registration with FINRA, follow MSRB rules, Know Your Client procedures at account opening). Transfers involving only a transfer agent will follow the SEC rules governing Transfer Agent activities.[118]

Risks. The retraining and adoption phase will take time and money to execute properly. Loss or theft of tokenized bonds presents less of a risk, since transactions of lost or stolen instruments are easily traced, destroyed, and re-issued.

[118] United States Securities and Exchange Commission, "Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities," 8 July 2019. https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities.

Word of caution: Two general considerations should be evaluated before adopting a blockchain-based system. One relates to the technology itself, and the other to the unintended consequences of potential use cases.

- **Technology considerations.** Blockchain solution providers and platforms are still quite varied and do not easily communicate with one another. Blockchain adopters should be clear on use cases and benefits associated with the various platforms. The use of fungible or non-fungible tokens to secure transactions should be understood.

- **Potential effects.** Effects such as liquidity, an important dynamic in a well-functioning muni market, should be considered. Currently, liquidity is related to instrument type. Loans are currently less liquid than registered bonds with CUSIPs (an official registration number issued by the Committee on Uniform Securities Identification Procedures), and transaction size matters (smaller transactions tend to have less liquidity and higher cost). Ideally, a blockchain market infrastructure will improve liquidity, as transparency and access increase while costs decline. However, any implementation strategy needs to consider carefully the liquidity implications. For a micro bond offering sold directly from the issuer to retail investors, the ability to sell the bonds in the secondary market or back to the issuer at market prices will be critical. Any type of compartmentalized offering linked to blockchain infrastructure needs to ensure that assets will not be stranded and that appropriate liquidity will be available.

PUBLIC BANKING AND DIGITAL ASSET BANKS

Introduction

The Public Banking Act AB 857 allows city and county governments to create or sponsor public banks and authorizes the State of California to license up to ten public banks in total, at up to two per year.[119] These banks are intended to provide public agencies access to loans at interest rates much lower than those otherwise obtained via private banks. Supporters of the act believe that public

[119] AB 857 (2019 - 2020). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB857.

banks are inclined to provide loans for public projects such as infrastructure and affordable housing. Partnerships with non-profit organizations engaged in helping the unbanked could amplify community benefits.[120]

Blockchain can provide value through efficiency in many areas, including authentication, payment automation, and settlements. When implemented during the bank's establishment, these benefits could be seamlessly attainable. Specific instances include more streamlined background checking for identity verification and automatically tracked loan payments. The technology also permits an entity to securely bank and transact with low income persons in disparate parts of the state using a cell phone. Blockchain-enabled lending offers a more secure way of offering personal loans to a larger pool of consumers through a cheaper, more efficient, and more secure loan process.

The prospective public bank's sponsor must propose a viable business plan, pending approval by both the state department of business oversight and the public. The law also requires each public bank to carry direct deposit insurance from the Federal Deposit Insurance Corporation (FDIC). As public entities, these banks would be required to provide public access to meetings and records.

Pilot and Use Cases

North Dakota. The Bank of North Dakota ("BND") is currently the last surviving state-run, and state-owned American bank. It is recommended that future public banks, including those in California, consider exploring the use of blockchain technology.

Considerations and Opportunities for Blockchain Application

Efficiency. Blockchain can provide value through efficiency in many areas, including authentication, payment automation, and settlements. When implemented during the bank's establishment, these benefits are seamlessly attainable. Specific instances include more streamlined background checking for identity verification and automatically tracked loan payments. The technology

[120] One example is the non-profit banking institution Community Development Finance, an organization that provides check cashing and loan services to the vulnerable populations in Oakland.

also permits an entity to securely bank and transact with low-income persons in disparate parts of the state using a cell phone.

Partnerships. Partnerships with non-profit organizations such as Community Development Finance, an organization that provides check cashing and loan services to the vulnerable populations around Oakland, could serve to amplify community benefits.

Regulatory considerations. There do not appear to be any statutory or regulatory barriers; a California public bank could implement blockchain technology in compliance with all existing statutes and regulations.

Blockchain Implementation: Potential Barriers and Concerns

Trust and intermediation. The leadership of the bank and city and county governments involved may have differing levels of comfort and enthusiasm for using blockchain technology in their operations. Publishing information about blockchain technology's functions and benefits can assist the general public to become familiar with the technology.

DIGITAL ASSET BANKS: SPECIAL PURPOSE DEPOSITORY INSTITUTION

California's emerging regulation of Digital Asset Banks will need to be negotiated in accordance with Federal law and the Securities and Exchange Commission. Further research and guidance from experts in banking, investments, currency regulation and related areas are needed before making recommendations.[121]

Introduction

Based on a survey conducted last year of 2,068 Americans, it is conservatively estimated 36.5 million people in the United States own some form of digital asset – with perhaps the highest percentage based in California.[122] Average holdings were $5,447 versus a median of $360 for non-digital assets. That would represent an extrapolated total holding of $198 billion, many of which individuals hold

[121] See analysis of proposed AB 2150 at http://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201920200AB2150.

[122] Richard Laycock, "A rising number of Americans own crypto," *Finder*, 20 November 2019. https://www.finder.com/how-many-people-own-cryptocurrency.

custody themselves rather than in an institution due to lack of availability. More broadly, a study by Gartner stated that blockchain technology will create more than $176 billion dollars of business value by 2025 and $3.1 trillion by 2030.[123] The survey on which these numbers are based was conducted at the bottom of the digital asset market in the past five years, and average holdings have risen approximately 40% since then.

California is home to blockchain companies, many of which make regular, significant transactions with virtual currencies. These transactions include asset purchases, payroll, investments, loans, rent and more. However, despite this degree of economic output, these companies are not allowed to bank their digital assets.

California-based digital asset businesses might benefit from a Special Purpose Depository Institution (SPDI) charter. A Digital Asset Bank could grant blockchain companies access to stable banking, on-demand digital asset conversion into dollars, financial products, and custody of digital securities and other virtual assets. In the absence of California banking services, some blockchain companies are looking elsewhere.

In addition, investors are reticent about investing in California-based blockchain technology companies and innovators for fear of liability and inability to bank in California with digital assets. California has an opportunity to become a leader in this field, as our existing capital requirements and other relevant legislation lend themselves to the creation of a Digital Asset Bank charter.

Considerations and Opportunities for Blockchain Application

Permission considerations. A key question is whether to use proprietary or open source blockchain-based software, whether the provider is willing to use a vault service, and whether blockchain technology is the best solution overall. Within the world of open source blockchain-based software, users and developers can determine the level of open versus permissioned access that is best for a given case.

[123] "Gartner predicts 90% of current enterprise blockchain platform implementations will require replacement by 2021," 3 June 2019. https://www.gartner.com/en/newsroom/press-releases/2019-07-03-gartner-predicts-90--of-current-enterprise-blockchain.

Selective information disclosure. A strong argument for blockchain is the ability to disclose information selectively. For example, the front and back of a driver's license may be requested for identification when the occasion only requires certain information such as age or home address, as well as whether the driver's license is valid. A blockchain application could be used in conjunction with Department of Motor Vehicle (DMV) officials to verify the license and then utilize the app to selectively disclose the required information to certain parties, while the DMV has full access to all the information on-chain. A similar exercise could be used for financial information, and indeed it is particularly important that any evolution in digital currencies not be tied to excessive disclosure of personal information.

Blockchain Implementation: Potential Barriers and Concerns

Regulatory considerations. Leading digital asset custody companies and exchanges would be most relevant to consult before establishing a Californian SPDI and supporting legislation. The legislation that underpins the adopting legislation for an SPDI involves defining what digital assets are, providing potential safe harbors and protections for non-security digital assets and so forth. Coinbase and Maker DAO are two California-based companies that could be approached; Kraken still has a significant presence in San Francisco but is also known to be applying for a Wyoming SPDI.[124]

Trust considerations. State-sponsored SPDI's will bring the faith and credit of the State of California into consideration for those interested in investing in California-based blockchain businesses but who may not be familiar with the technology itself.

CANNABIS AND BANKING

Introduction

California began the global reform of cannabis policies with the passage of Proposition 215, the Compassionate Use Act in 1996. Collectives and cooperatives began to formalize the production and distribution of medical cannabis, and

[124] Job opening advertisement: https://www.linkedin.com/jobs/view/operations-director-special-purpose-depository-institution-coo-at-kraken-1854869856/.

the Board of Equalization determined in 2007 that the sale of medical cannabis was subject to sales tax. The passage of the Medical Marijuana Regulation and Safety Act in 2015 laid out a licensing and regulatory framework followed by the Adult Use of Marijuana Act (Proposition 64) in 2016. On January 1, 2018, the state of California became the fifth U.S. state to license the regulated production and sale of cannabis to adults.

California is the largest single cannabis marketplace in the world, and its cultivated crop produces more economic value than any other agricultural commodity. Adult use sales in 2019 totaled $808 million and expected to top $3.5 billion throughout calendar 2020. As of late April 2020, there are over 650 licensed retail cannabis storefronts and 300 licensed retail cannabis delivery services with at least 100,000 direct employees and an estimated 6.4M (non-tourist) cannabis consumers in California with thousands of non-retail licenses and ancillary businesses, all of which would benefit from greater access to financial solutions and other blockchain-related applications.[125]

Federal treatment of cannabis as a controlled substance has stopped banks from developing relationships with and services for the cannabis industry. Federal law, however, could change and California could do well to be prepared should that happen.

In that event, blockchain fintech may be useful for settling cannabis transactions, improving public and consumer safety, generating economic value, and promoting alternative, decentralized local financing for small and social equity businesses, and promote statewide economic development and post-COVID recovery. Digital currencies, digital asset banking, and next-generation fintech solutions may be useful to address cannabis industry pain points, increase tax revenues, and improve public safety.

Blockchain fintech and licensed commercial cannabis businesses in California face similar opportunities and challenges:

[125] "California cannabis market," *Cannabis Business Plan*. https://cannabusinessplans.com/california-cannabis-market/. Dan Mitchell, "How does California's cannabis market compare?" *East Bay Express*, 12 February 2020. https://www.eastbayexpress.com/oakland/how-does-californias-cannabis-market-compare/Content?oid=28682926.

1. Payments and lending limitations for cannabis consumer and business financial transactions need improvement

2. An abundance of data on cannabis transactions and production is collected and stored but seldom analyzed or used to improve or verify processes

3. Because Federal solutions for new and popular business models are not forthcoming, state governments, startups, and stakeholders have improvised solutions

4. Many of the proposed blockchain fintech ideas and policy suggestions could benefit the cannabis industry

5. Certain features of the cannabis industry may make blockchain fintech more difficult to implement but other factors may assist in industry adoption

6. Microlending for small and social-equity businesses should be a policy goal

7. Blockchain innovations could improve safety and public safety

8. Cannabis blockchain solutions can add value and improve competitiveness

California is uniquely suited to benefit from the synergies of blockchain fintech businesses and state-licensed commercial cannabis enterprises. The sheer size of its labor, consumer goods and commodities markets places the state economy in the top ranks of global markets. Blockchain fintech enterprises are starting up in California as is the burgeoning state-licensed commercial cannabis industry.

The ongoing difficulty of state-licensed cannabis enterprises to obtain access to the financial sector is both a private sector problem and a public safety issue. Regulation affecting both areas must be addressed at the State and Federal level. Due to the ongoing Schedule 1 status of marijuana under the federal Controlled Substances Act, and despite the state-legal nature of regulated commercial cannabis activities, bankers and other private sector providers are averse to providing financial services to cannabis businesses. However, since February 2014, the U.S. Treasury's FINCEN guidelines for banking Marijuana Related Businesses have provided a degree of guidance for the financial sector to comply with the Bank Secrecy Act. These guidelines call for implementing comprehensive, ongoing due diligence of banked cannabis entities, their ownership, policies, and activities.

The FINCEN validation infrastructure with its ongoing scrutiny of cannabis transactions, supply chain movements, and production details creates a costly compliance overhead. This cost has been a limiting factor for most banks desiring to provide services to state legal, tax paying and job creating cannabis enterprises. As a result, the better capitalized operators are able to bear the cost of acquiring access to bank accounts, giving them a competitive advantage over smaller operators, who fall further behind.[126]

Under the pre-2018 collective framework, virtual currencies such as Bitcoin and Ethereum were often used to compensate producers and service providers throughout the medical cannabis supply chain. However, applicability is limited in the current state licensed system.

Pilots and Related Case Studies

Given that the industry is not yet federally legal, academic literature and pilot projects are limited.

Digital asset cannabis purchase and tax payment, City of Emeryville. Ohana Dispensary in Emeryville, CA, hosted the first compliant digital asset purchase of cannabis products using a dollar-backed stable coin (11 September 2019). The purchaser identification, receipt, and tax payments, were instantly stored, and transmitted to the relevant agencies at the moment of transaction.[127]

[126] "New FinCEN Guidance Affirms Its Longstanding Regulatory Framework for Virtual Currencies and a New FinCEN Advisory Warns of Threats Posed by Virtual Currency Misuse," Financial Crimes Enforcement Network, 9 May 2019. https://www.fincen.gov/news/news-releases/new-fincen-guidance-affirms-its-longstanding-regulatory-framework-virtual.

[127] Jamie Redman, "California City Official Uses Bitcoin Cash to Purchase Cannabis," Bitcoin.com, 11 September 2019. https://news.bitcoin.com/california-city-official-uses-bitcoin-cash-to-purchase-cannabis/.

Legislation: Assembly Bill 953. One prominent proposal was introduced by Assemblymember Ting: Assembly Bill 953 (now reintroduced as AB 3090) which proposed a "stablecoin" (cryptocurrency pegged to the dollar) as a framework for levying and collecting local cannabis tax payments.[128]

Without widespread adoption by end consumers and third-party vendors though, these activities are still largely marginal to the overall cannabis marketplace. The private sector's past efforts to stoke cannabis consumers' interest in blockchain fintech, like gift card solutions, and cannabis-themed ICO crowd-fund offerings largely failed and may have stalled opportunities to unite these two young industries.

Robust digital wallet solutions and quick settlement transactions are maturing, as are stablecoin products. It is reasonable to anticipate increased consumer adoption and blockchain market penetration into the cannabis industry (and vice versa).

In the past cannabis record-keeping was viewed as self-incriminating evidence of felony crimes. Now cannabis businesses with good record-keeping practices are granted greater access to financial services, to licensure in other markets and even access to investment capital. This improvement of data capture is ideal for blockchain apps.

Considerations and Opportunities for Blockchain Application

Safety considerations. The primary, default mode of operations for the cannabis industry is often physical cash, which carries public health and safety risks. Establishing digital asset custodial options and other blockchain fintech infrastructure solutions for commercial and public stakeholders would permit rapid deployment of capital through secure digital means, while allowing both state and federal regulators and auditors appropriate levels of transparency.

Efficiency. Transaction settlements between retail customers and retail cannabis storefronts, and business-to-business transactions become faster, automated, and cheaper on blockchain platforms. They may also ease the burden on

[128] http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB3090.

government agencies by reducing the need for intermediaries. Regulation of the cannabis (and possibly soon hemp) supply chains in California and many other states requires third-party verification of quality control on finished products, conducted by distributors and independent testing laboratories. This element of the cannabis supply chain, with its validation of a permissible product embedded in an immutable, transmitted document meant for sharing publicly, is remarkably akin to processes and roles within a blockchain ecosystem.

Reliability. Blockchain and other digital ledger solutions can bring improvements in efficiency and reliability of information gathered at all steps of document collection, verification, storage, and long-term usage.

Transparency. The existing intermediary roles of wholesale distributors and brokers of cannabis products will be enhanced and more transparent if a robust blockchain fintech infrastructure were available to the cannabis industry. Manufacturers of pharmaceutical grade products needing specific known product characteristics and others employing current Good Manufacturing Processes would benefit from greater reliability and trust in the supply chain. And investors in small cannabis businesses would gain confidence in their investments.

Integration with other blockchain applications. The cannabis industry's emergent digital ledger innovations are primarily concerned with the tracking and tracing cannabis products. The fundamental problem, however, is yet to be addressed: a lack of access to banking and financial services. Rather than advocating for cannabis-specific banking options, we believe that existing proposals such as public banks (or, more specifically related to blockchain, Special Purpose Depository Institutions) may benefit licensed cannabis businesses as well as non-cannabis businesses.

Integration with Digital Asset Banking. (See section above for details.) Current laws require banks to obtain FDIC insurance on cash deposits, which is threatened if they choose to bank cannabis companies. However, a specialized financial institution (such as a Special Purpose Depository Institution or SPDI) backed by a stable cryptocurrency, pegged to the dollar, would not require FDIC insurance on digital assets held in custody for account holders, cannabis or otherwise.

A second advantage of establishing a public bank or other institution with a digital asset component would be to facilitate loans and interest payments in a peer-to-peer model. This decentralized finance infrastructure of microlending has proven to strengthen communities where the loans are serviced.

Blockchain Implementation: Potential Barriers and Concerns

Because of the conflict between State and Federal regulations regarding the cannabis industry, barriers and recommendations discussed below focus on the local and State level, understanding that some items will need to be reconciled with Federal guidelines.

IT considerations. Major conditions that make the cannabis industry unfavorable for adoption of blockchain fintech solutions relate to rural internet access and access to commercial lending services.

Engagement and adoption. Stakeholders within the cannabis industry should review the benefits of blockchain's potential with regard to improving public safety and local economic development in this report. The Working Group recommends that subject matter experts also be consulted, such as the California Tax and Fee Administration, the California Association of Treasurers and Tax Collectors, as well as private sector stakeholders.

CALCOIN

Introduction

In a short time, the COVID-19 pandemic has thrown much of the world into severe recession, overloaded the healthcare industry, and devastatingly affected low-income families. Nearly 22 million Americans filed for unemployment in the four weeks between mid-March and early April 2020, abruptly discontinuing what had been a record 113-month streak of employment growth. The unemployment rate has declined slightly in May, after reaching a high of 14.7% the month before.[129]

[129] "Monthly unemployment rate in the United States from May 2019 to May 2020," *Statista*, https://www.statista.com/statistics/273909/seasonally-adjusted-monthly-unemployment-rate-in-the-us/.

In response to the pandemic's economic impact, the U.S. Congress passed a $2-trillion "Coronavirus Aid, Relief, and Economic Security Act'' (CARES Act) on March 26, 2020.[130] Unfortunately, many Americans and small businesses experienced delays in gaining access to expected funds or receiving responses to their loan applications.[131]

The delay in direct aid has exposed the antiquated and inflexible software systems connecting America's financial infrastructure. Unemployment systems in 12 states, including the system used in California, rely on COBOL, a programming language from the 1960s.[132]

Even where conventional software systems handle these requests, the underlying financial infrastructure to disseminate the aid — Automated Clearing House, or ACH, transfers — is still costly and slow. The U.S. Government is likely to spend between $47.82 million and $358.65 million of these limited yet crucial funds on ACH transaction fees alone. Once the aid is received, additional money is deducted from actual aid on the transaction fees for credit and debit card processing.[133]

The COVID-19 pandemic unveiled the imminent need for a free, digital, and publicly accessible payment network to disburse aid with more efficiency and transparency and avoid the cost and privacy issues of commercial payment platforms. The CARES Act originally had included a "digital dollar," a digital payment system designed to speed relief payments to families in distress but this provision was removed before the bill's enactment.[134] Several current proposals

[130] HR 748, https://www.congress.gov/116/bills/hr748/BILLS-116hr748enr.pdf.

[131] Ben Popkin and Stephanie Ruhle, "'Extremely disappointing' and 'entirely predictable' — slowdowns and lockouts plague second round of PPP," *NBC News*, 27 April 2020. https://www.nbcnews.com/business/business-news/extremely-disappointing-entirely-predictable-slow-downs-lockouts-plague-second-round-ppp-n1193421.

[132] Makena Kelly, "Unemployment checks are being held up by a programming language nobody knows," *The Verge*, 14 April 2020. https://www.theverge.com/2020/4/14/21219561/coronavirus-pandemic-unemployment-systems-cobol-legacy-software-infrastructure.

[133] Shailee Adinolfi, "The US could deliver stimulus checks faster -- with tech's help," *Wired*, 12 May 2020. https://www.wired.com/story/opinion-the-us-could-deliver-stimulus-checks-faster-with-techs-help/.

[134] Lawrence Wintermeyer, "Covid-19 economic stimulus: Get money to people faster with digital dollars," *Forbes*, 30 March 2020. https://www.forbes.com/sites/lawrencewintermeyer/2020/03/30/covid-19-economic-stimulus-get-money-to-people-faster-with-digital-dollars/.

in Congress recognize the urgent need for far-reaching technological changes in order to deliver economic stimulus more effectively.

The potential benefit of instant cash aid disbursement stretches far beyond disaster relief programs and into other state programs such as unemployment, nutrition, and housing assistance. With capabilities to coordinate with the federal government, digital dollar programs would enable states to better and more directly serve their most financially vulnerable residents.

Pilots and Related Use Cases

While few government entities have implemented blockchain solutions for aid or welfare benefits, several non-governmental organizations (NGOs) are beginning to beta-test aid distribution on the blockchain, including the Red Cross and Oxfam International. These programs have demonstrated marked improvements in both beneficiary registration and aid disbursement processes when tried in Syria, Kenya, Vanuatu, Lebanon, and Greece, among others.

State of New York, 'Inclusive Value Ledger.' The New York State Legislature is considering legislation creating an "inclusive value ledger."[135] The bill proposes a state-owned electronic payments platform similar to PayPal or Venmo and would offer low cost, rapid distribution of public benefits. Low income unbanked and underbanked persons could collectively save millions of dollars in fees by not having to rely on check-cashing storefronts to access aid payments. Likewise, the state would also achieve significant savings by streamlining the process of obtaining state-administered benefits from unemployment to tax credits.

International NGOs and Government Programs. The United Nations World Food Program recently used a blockchain platform to deliver aid when it transferred cryptocurrency-based food vouchers to 10,000 refugees in Pakistan.[136] The trial was so successful that the UN plans to expand the program to 500,000 Syrian refugees in Jordan. The United Kingdom Department of Work and Pensions ran a pilot program to deliver welfare payments via a blockchain network. Recipients received benefits

[135] Charlie Innis, "Assemblyman Floats Government Launching Digital Currency For Taxpayer Use," *Kings County Politics*, 12 December 2019. https://www.kingscountypolitics.com/assembly-man-floats-government-launching-digital-currency-for-taxpayer-use/.

[136] World Food Programme,"Building Blocks, Blockchain for Zero Hunger," 22 May 2020. https://innovation.wfp.org/project/building-blocks.

distributions via apps on their phones. The digital payments could be used for expenses just like regular welfare payments.[137] The program demonstrated promise but the government remains cautious about expanding the implementation due to limited uptake and concerns about capacity and energy consumption.[138] Additional international projects include Sempo and Project i2i in the Philippines.

Considerations and Opportunities for Blockchain Application

Legal considerations. As a new approach to money, CalCoin may well require adjustments to regulations and will raise some novel legal questions. For example: in contrast to physical cash, CalCoin may restrict residents outside the state from using it.

Governance. While decentralized systems offer many advantages, a broad-based decentralized platform with no responsible entity can be problematic. Lack of structured governance could hamper decision-making at the technical and design levels. Lack of clear ownership would raise legal and regulatory questions, namely for the assignment of liability. This concern calls for a controlled and regulated infrastructure which assigns clear governance structures for system design, development, maintenance, funding, upgrades, and the like.

Security and privacy. Security and privacy are of utmost importance when dealing with benefits recipients' identities, medical benefits, and banking, and other sensitive information. Fortunately, it would be technically feasible to fine-tune CalCoin's privacy features with various mixes of anonymity versus traceability of transactions.

The CalCoin benefits distribution program targets the unbanked. For this population, identity verification must be possible without the user needing an electronic device or card. Thus, questions of encryption and cybersecurity will be paramount.

[137] Luke Parker, "UK Government pilot uses blockchain for welfare distribution," *Brave New Coin*, 14 July 2016. https://bravenewcoin.com/insights/uk-government-pilot-uses-blockchain-tech-for-welfare-distribution.

[138] Nikolova, Maria "UK sees the use of blockchain as nonviable for welfare and benefits system," *FinanceFeeds*, June 8, 2018. https://financefeeds.com/uk-sees-use-blockchain-nonviable-welfare-benefits-system/.

GOVERNMENT ROLE IN REMITTANCES

Blockchain technology has been used with considerable innovation for international remittances. Blockchain is a promising technology to facilitate cheaper and more efficient cross-border transactions because it eliminates intermediaries, most of whom take a cut out of every cross-border payment. Companies like Ripple are creating blockchain-based alternatives to current remittance technologies and have piloted their technologies with money transfer companies including Western Union and Moneygram.

V.G. Civic Participation

The California Secretary of State provides services in four major areas: Political Reform Division (campaign finance); Elections Division (including voter registration); Business Programs Division; and State Archives Division.

The Working Group considered three of the four major areas for blockchain application: voting, business programs, and archives. Although the Working Group ruled out applications of blockchain technology for voting at this point, two remaining areas might benefit from blockchain technology: State Archives Division (in the near term) and Business Programs Division (future application).[139]

Key Recommendations

REC V.G.1. State Archives: The Secretary of State's State Archives Division would be an effective first blockchain pilot project. The Division should solicit feedback from stakeholders and consider issuing a Request for Information to help outline the scope of the project and required budget. If indicated, the California legislature should work with the Secretary of State leadership to determine how best to move the State Archives online with blockchain technology.

REC V.G.2. Business Programs: The Secretary of State's Business Programs section may be a potential use case in the future, as the Secretary of State's employees deploy a new technology when developing future modules for the new portal.

[139] We acknowledge the contributions of Kai Stinchcombe in this section who departed the Working Group before the completion of this report.

REC V.G.3. Internet Voting: Security experts generally agree that internet-based implementations of voting systems, blockchain or otherwise, have not overcome security challenges. In applications to date, blockchain-based systems rely on factors other than blockchain, such as centralized voter databases, facial ID or postal delivery, cryptographic mixing, dual-device vote validation, etc., to solve these problems. Those experimenting with new voting technologies in California are encouraged to evaluate the quality of these solutions as a whole, rather than relying on a specific technology.

THE CALIFORNIA STATE ARCHIVES

The California State Archives has served as the repository for many significant records relating to state laws, policy, and legislation since 1850. The Archives collects, catalogs, preserves, and provides access to the historic records of state and local governments, and private collections. Each year thousands of researchers contact and visit the California State Archives seeking documentation to support their historical investigation. Staff help researchers identify collections that are most relevant to their area of interest and retrieve those paper records from a secure storage area. In addition, the Records Management and Appraisal (RMA) unit, within the State Archives Division, is responsible for administering the State Records Management Act (Government Code Sections 12270-12279) and providing statewide guidance on records management and trusted systems.

One of the State Archives' primary goals is to digitize and provide broader online access of their historical records to the public. State Archives currently digitizes records onsite and has small vendor-based digitization projects that are completed as funding becomes available. Over the past year, State Archives has been working closely with the Department of Finance and the Department of Technology to identify feasible solutions to develop a user-friendly public access hub on their website. This hub would include a mechanism to absorb records directly from other state agencies, cloud storage (for both immediate access to files and specialized storage for records with restrictions), preservation storage, the ability to format these documents to be ADA-accessible, and to translate these documents to better serve California's multilingual population. As part of this effort, staff have researched and considered various solutions including trusted systems, blockchain technology, and other related technology.

In addition to the immediate goals of this project, State Archives seek to demonstrate and provide detailed guidance to other State agencies and entities interested in undertaking similar projects in the future.

Pilots and Related Case Studies

The National Archives and Records Administration released a white paper in February 2019 exploring the benefits of blockchain technology as it relates to archives.[140] The white paper includes useful analysis of the implications of using blockchain with records management.

Considerations and Opportunities for Blockchain Application

Level of risk/privacy: Although it is an important historical division, the State Archives use case would not directly affect a large number of businesses or individual Californians, making it a low-risk endeavor. The level of security and privacy risks are much lower for State Archives than other Secretary of State divisions, such as Elections or Business Programs. Because the State Archives contain public records, privacy concerns are minimal.

Authentication: State Archives documents are public records, and security measures must be employed to ensure that they are original, authentic documents. Because blockchain technology can authenticate records, this benefit suggests an effective use case.

Current IT infrastructure maturity: The Secretary of State has been willing to implement pilot projects in various areas with its IT infrastructure. With additional resources, extensive modifications would not be necessary to conduct a blockchain pilot with the State Archives.

Added value of using blockchain: State Archives documents are used by local governments, litigators, and others. The current paper-based system would gain efficiencies by moving online. Blockchain could provide transparency and ease of access to these records.

[140] National Archives and Records Administration, "Blockchain White Paper," February 2019. https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf.

Blockchain Implementation: Potential Barriers and Concerns

Decentralization: If blockchain technology were used to digitize the archives, the State Archives Division would be the central authority and the single writer onto the blockchain. However, "blockchains are useful primarily in the case when there are multiple, mutually distrusting writers (appenders), and they are all peers, with no central authority."[141] Hence, blockchain technology may not be required to digitize the archives.

The National Archives explored this issue in its white paper, recognizing that the shift from a centralized-based model of trust to a network model is becoming more prevalent among technology sectors. Without reaching a conclusion on this issue, the National Archives noted, "[t]his shift may impact how records are organized and arranged and maintained over time, which in turn will impact how records managers collect records, apply intellectual and access controls, and execute disposition rules."[142]

Blockchain technology could be a good choice if multiple writers, such as local governments or multiple states, cooperated to store their archives on the blockchain. A shared effort may also reduce costs of digitization.

Security issues: There are potential security threats with digitization:

> Archives personnel could digitize documents and maintain their integrity by digitally signing all of the documents and widely publishing the signature algorithm and their public key(s). Even so, with changes of administration or malicious insiders it is always possible for private keys to leak and hence there is a possibility new signed documents could be forged. Protecting against that kind of threat requires serious attention to key management issues (e.g., Shamir secret sharing, and key revocation) and training Archive employees.[143]

[141] Email from David Jefferson, 27 March 2020, on file with Professor Michele Neitz (emphasis original).

[142] NARA, "Blockchain White Paper," 2019, p. 11.

[143] Email from David Jefferson, 27 March 2020, on file with Professor Michele Neitz.

A way around this security threat would be multiple, widely distributed copies of the signed digital documents (which would not require blockchain technology).

Funding: Although the State Archives Division serves a critical function for the state, it has a very slim budget and follows the budget process for any funding requests. Additional resources would be required to complete this pilot.

Next Steps

Solicit feedback from stakeholders: Multiple state officials should be consulted before moving forward:

- Secretary of State officials
- Local Government Archive Departments
- National Archives and Records Administration

Consider developing a Request for Information (RFI) for a digitization/ authentication system, blockchain or not. Information submitted should include financial estimates to help develop a proposed budget. As an "IT project," such an implementation would require approval from the Department of Technology as well as funding from the Legislature. The agency is excited to explore blockchain applications and has been successful with previous technology pilots. This use case provides for a relatively low-risk pilot project with potential benefits.

SECRETARY OF STATE: BUSINESS PROGRAMS

The Business Programs Division has been experimenting with modules related to new technologies, featured in its online portal.[144] The website describes itself as:

> A new online portal to help businesses file, search, and order business records. Whether you are filing a financing statement pursuant to the Uniform Commercial Code (UCC), searching for a corporation (Corp), limited liability company (LLC), limited partnership (LP) filing or looking for an immigration consultant, this hub consolidates all your online filing and search needs.

[144] California Secretary of State, https://www.sos.ca.gov/business-programs/bizfile/.

This section may offer a potential use case in the future, since the Secretary of State's employees could deploy a new technology as they develop future modules for the new portal.

INTERNET VOTING

Introduction

Security experts generally agree that internet-based implementations of voting systems, blockchain or otherwise, have not overcome the inherent challenges in implementing an online voting system, particularly security challenges. In reviewing pilot projects, blockchain systems have not been shown to be inherently better at achieving the goals – authentication and authorization, auditability, anonymity, failure reduction, and increased participation – of an internet-enabled election system. In applications to date, blockchain-based systems rely on factors other than blockchain, such as centralized voter databases, facial ID or postal delivery, cryptographic mixing, dual-device vote validation, etc., to solve these problems. The issues raised by pilot projects relate to security goals required of any voting system and a set of well-established best practices for addressing them.[145] These principles should apply equally across technologies, including blockchain.

Pilots and Related Case Studies

The Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA): The earliest pilots of internet voting in the U.S. operate under the UOCAVA[146] including the first

[145] Verified Voting Foundation: Principles for New Voting Systems (https://www.verifiedvoting.org/voting-system-principles/); see also ProCon.org's summary of positions on voting machines by the National Academy of Sciences (https://votingmachines.procon.org/source-biographies/national-academy-of-sciences-nas/).

[146] 52 USC Ch. 203: "Registration and voting by absent uniformed services voters and overseas voters in elections for federal office," effective as of 28 October 2009. https://www.fvap.gov/uploads/FVAP/Policies/uocavalaw.pdf.

pilots of blockchain-based voting, in Denver, Utah County, and West Virginia.[147] These tests incited controversy and concern among cyber professionals who believe significant questions remain unanswered.[148]

Voting System Considerations

Authentication and authorization:

In setting up a voting system, authentication (determining that you are who you say you are) and authorization (determining that you are eligible to do what you are trying to do) must be addressed. In current voting practices, the government creates an authorization list through the registration system, establishing who is eligible to vote. At the time of voting, the government authenticates individuals through in-person signatures at polling places. There are examples of more stringent authorization and authentication such as reviewing and purging the voter rolls as means to reduce the risk of unauthorized voting, and requiring a photo ID at the polls to reduce the risk of unauthenticated voting.

Blockchain does not appear to help with potential risks of voter fraud. Neither password nor code distribution by mail or face comparison against previously collected face data (e.g., passport or driver's license) creates an inherent advantage of blockchain over non-blockchain systems.

Voter verifiability and auditability:

Voter verifiability is the concept that the voters should not have to trust an external system certifying their cast ballot matches their intended vote.[149] As

[147] Larry Moore and Nimit Sawhney, "Under the Hood: The West Virginia Mobile Voting Pilot," Voatz, 2019. https://sos.wv.gov/FormSearch/Elections/Informational/West-Virginia-Mobile-Voting-White-Paper-NASS-Submission.pdf; Connie Loizos, "Voatz, the blockchain-based voting app, gets another vote of confidence as Denver agrees to try it," *TechCrunch*, 7 March 2019. https://techcrunch.com/2019/03/07/voatz-the-blockchain-based-voting-app-gets-another-vote-of-confidence-as-denver-agrees-to-try-it/; Benjamin Freed, "Utah County, Utah, begins review of mobile-app votes," *StateScoop*, 4 September 2019. https://statescoop.com/utah-county-utah-begins-review-of-mobile-app-votes/; West Virginia Secretary of State Mac Warner, "WV Secretary of State – 24 Counties to Offer Mobile Voting Option for Military Personnel Overseas," 20 September 2018. https://sos.wv.gov/news/Pages/09-20-2018-A.aspx.

[148] David Jefferson et al., "What We Don't Know About the Voatz "Blockchain" Internet Voting System," White Paper, 1 May 2019. https://cse.sc.edu/~buell/blockchain-papers/documents/WhatWeDontKnowAbouttheVoatz_Blockchain_.pdf.

[149] Raj Karan Gambhir and Jack Karsten, "Why paper is considered state-of-the-art voting technology," Brookings Institution, 14 August 2019. https://www.brookings.edu/blog/techtank/2019/08/14/why-paper-is-considered-state-of-the-art-voting-technology/.

an example of current practice, the machine-recorded all-electronic totals are instantly available, but there is also a human process – voter sees receipt, receipt is in a sealed ballot box, auditors can check the receipts afterward; that verifies the electronic totals are correct.

The best implementations for a voter casting a ballot remotely (whether open- or closed-source, blockchain or not) involve some level of trust in the user's device or devices. Often two devices are required (a mobile app and a website, or two physical devices), one of which produces a barcode or key and the other that validates that the registered vote accurately represents the voter's choices. The greatest single point of failure is the app, website or device itself. A compromised website could display a code that suggests a validated vote for one candidate but transmits something different, for example.[150] Or malicious code inserted into the app (or a fraudulent copycat app with a confusing name uploaded to the app store, or using a malicious download link distributed on social media) could be used to forge ballots at scale.

In an open-source or open-standards implementation, the apps might be independently produced, which reduces the odds of failure. At this point there is not a significant gap between the way blockchain and non-blockchain systems enable voters to validate their vote or track it auditably through the system.[151]

Strong anonymity:

America has historically associated the secret ballot (or "Australian ballot") with not just the ability to vote secretly, but an inability to not vote secretly ("strong anonymity"). The purpose of strong anonymity is to prevent those in positions of power to ask about voting choices or coerce voters.

Strong anonymity is a near-impossible challenge for any voting system that is not in-person. An employer, union, advocacy group, campaign, or abusive spouse could as easily push someone to fill out a paper ballot as an electronic one. Internet voting (including blockchain voting) does not appear to increase anonymity concerns. Clever cryptography enables votes to be sent in partial

[150] Jefferson et al., "What We Don't Know About the Voatz 'Blockchain' Internet Voting System."

[151] "Agora: Bringing our Voting Systems into the 21st Century," White Paper (n.d.). https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5b6c38550e2e725e9cad3f18/1533818968655/Agora_Whitepaper.pdf.

chunks to separate servers that cannot individually decrypt them. Once cast, reference implementations of online voting employ a “mixing” process to separate the voters’ identities from their votes. Ultimately, the anonymization servers must be trusted to behave as intended, i.e., not to be running malicious software that intercepts and decrypts incoming data.

Depending on the implementation, the use of time stamps in blockchain may be used to record the order of votes cast. In a small enough voting pool, this could be used to establish identifying information. If we can remove this concern without introducing new ones, however, mail voting, non-blockchain internet voting, and blockchain voting seem to be at parity in their ability to protect anonymity.

Distributed decision-making as a strategy to prevent large-scale fraud:
A goal of many voting systems is to increase the number of parties that must collaborate to have a large-scale effect on the outcome in order to minimize the potential impact of any given official or vendor’s fraud or incompetence.

- Blockchain systems (relative to other internet systems) eliminate some single points of failure but may introduce others.

- For example, it is an advantage that you can (in some blockchain implementations) choose a server to send your vote to (each run perhaps by an independent nonprofit) rather than face only a single choice. On the other hand, some leading blockchain applications are not open source, and an open-source implementation might be associated with a higher level of transparency or confidence in the results. Additionally, the number of nodes and who is running them matters tremendously for this sort of application – if a majority of nodes are all being run by the software provider, for example, it reintroduces a point of failure that was supposed to be eliminated.

- Large-scale compromises of websites, computers, or apps, or theft of passwords or private keys are possible in either scenario, as are attacks on the voter registration database or human aspects of the audit systems. (See, for example, the Moscow election, conducted on blockchain, in which independent parties claim races were stolen.[152] The challenge was not a failure of blockchain, but a poor – or sabotaged – implementation, in which auditing tools were delayed or canceled.)

Participation and the security/accessibility tradeoff:
Purging the rolls and requiring identification, restricting absentee ballots, and using inconvenient technology all reduce the number of ballots successfully cast. In contrast, features like same-day registration and widespread mail voting increase turnout, at the cost of greater vulnerability to fraud. In any expansion or reduction in accessibility, there are also tradeoffs to relative participation. A broad goal of using technology in the voting process would be to increase turnout by people who expect to be able to transact online or from mobile devices, or for whom in-person voting is particularly inconvenient – e.g., wage workers, students, and digitally-native younger people. But it will naturally also increase, on a relative basis, the participation of technology-users relative to non-technology-users.

Blockchain Implementation: Potential Barriers and Concerns

Authentication: Distributing private keys securely to millions of citizens (by mail or on devices) is daunting. (A malicious link could easily be circulated on social media designed to "validate" voting information but that actually steals passwords or ID codes that might allow an actor to vote at least thousands of times.)

An internet voting system might be more secure than in-person voting (which typically does not validate either a password or a face) or mail voting (which validates only a postal address). However, with internet voting the problem is more serious because a single person could steal thousands of private keys or introduce malware to the system affecting thousands of votes.[153] In contrast, a system to vote in person a thousand times would be much more challenging and would much more obviously expose the culprits to identification and arrest. Validating faces against photo IDs at scale also presents unique challenges: if the system fails, what recourse does the voter have to get their face verified, for

[152] Denis Dmitriev, "Shut up and trust them: Why Moscow's new Internet voting system relies on faith, not transparency or peer review," *Meduza*, 7 September 2019. https://meduza.io/en/feature/2019/09/07/shut-up-and-trust-them.

[153] Sunoo Park et al., "Going from Bad to Worse: From Internet Voting to Blockchain Voting," MIT, 20 February 2020 (DRAFT). http://people.csail.mit.edu/rivest/pubs/PSNR20.pdf.

example? How do we ensure that the face recognition system is free of racial, gender, or age bias, as has been commonly reported across such systems?

Security: Few computer scientists with expertise in elections believe that implementations of election protocols (such as voter authentication, ballot auditability, and anonymity) are mature enough or secure enough to be deployed at scale.[154] Security breaches are ubiquitous in online systems regardless of sector. Election systems are among those whose infallibility is the most essential yet hardest to secure.

V.H. Education and Workforce

Key Recommendations

REC V.H.1. California should emphasize interoperability, security, and scalability when piloting the use of blockchain for education and workforce records.

REC V.H.2. The California Future of Work Commission should adopt recommendations on skills-based hiring and credentials, ensuring workers have the means to control and electronically share credentials in a secure and verifiable manner.

REC V.H.3. The State should enable and facilitate a results-focused forum for technology demonstrations that advance public sector applications, leveraging opportunities to re-use, re-purpose, and build upon existing efforts.

REC V.H.4. The State should develop a framework of key questions, considerations, and paths forward for groups interacting with the California public school system and public service. Such a framework could help stakeholders identify blockchain-based pilot projects and serve as a public resource.

REC V.H.5. The State could encourage creative "cross-pollination" from other sectors and application areas by incentivizing and providing a safe space for transparent discussion of lessons learned and best practices. Illustrating the

[154] David Jefferson, "If I Can Shop and Bank Online, Why Can't I Vote Online," Verified Voting, 2011. https://www.verifiedvoting.org/resources/internet-voting/vote-online/.

different phases of technology adoption, and encouraging discussion of risks, benefits, and "readiness levels" needed along the way will provide clarity for technology developers, policy writers, and solution adopters moving forward.

Introduction

California comprises an estimated active workforce of over 19 million operating within a variety of local and international institutions.[155] As the American Workforce Policy Advisory Board's "White Paper on Interoperable Learning Records" states, "American workers, who are engaged in lifelong learning, deserve to have a way to translate their full education, training, and work experience to a record of transferable skills that will open the doors to higher wage occupations and careers."[156]

Education and workforce records are integral to a dynamic labor ecosystem. Presently, California has regulatory regimes that require licensing of numerous professions and trades. The Department of Consumer Affairs operates more than 150 types of licenses.[157] People who hold these licenses often must prove that their licensure is current and they have completed requirements such as continuing education. There are rules on transferring licensure when someone moves to California with credentials from out of state, or when a California resident moves elsewhere.

Pilots and Related Use Cases

Academic records. Blockchain technology has been used by MIT for certificate dissemination since 2015 and for diplomas since 2017.[158] Additional efforts from a California community college, Foothill-DeAnza College, as well as Arizona State University and other institutions have explored using blockchain and information

[155] U.S. Bureau of Labor Statistics, U.S. Department of Labor, "Economy at a Glance – California," June 2020. https://www.bls.gov/eag/eag.ca.htm.

[156] American Workforce Policy Advisory Board, "White Paper on Interoperable Learning Records," September 2019. https://www.in.gov/che/files/Interoperable%20Learning%20Records_FINAL.pdf.

[157] State of California, Department of Consumer Affairs, https://www.dca.ca.gov/consumers/public_info/index.shtml.

[158] Elizabeth Durant and Alison Trachy, "Digital Diploma debuts at MIT," MIT, October 2017. http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain- technology-1017.

about digital education records to help improve degree completion and student services.[159] In 2019, Dallas County Community College District announced a partnership with a blockchain technology company to provide students with lifelong access to their entire academic and continuing education records, with 100 educational institutions accepting the student-submitted records.[160] Indeed, one straightforward use case would be to enable easier transcript verification for community college students who transfer to four-year colleges. Even earlier in life, students who move among school districts (as foster youth often do) could verify their academic achievements more seamlessly.

Considerations and Opportunities for Blockchain Application

Credentials verification. Ninety-five percent of California employers conduct background checks on applicants, verifying previous employment, past performance, and educational credentials.[161] Once employed, people often need to share their working credentials with others to obtain services such as loans or join professional organizations.

Verifying these credentials is often a time-consuming, paper-based process. While the process of generating employment verification letters and salary verification letters has increasingly become digitized, often a paper letter is still required to alleviate concerns about fraud and misrepresentation. Without adequate security and verification, electronic credentials are seen as too easily forged and thus unreliable. The result is a time-consuming system that adds friction in the hiring process, slows down bank loans and other transactions, and is so complex that businesses turn to intermediaries such as background check companies to compile the information.

Blockchain-based credentialing systems can help remove existing friction by

[159] Lindsay Mckenzie, "Boosting Degree Completion with Blockchain," *Inside Higher Education*, 9 July 2019. https://www.insidehighered.com/news/2019/07/09/arizona-state-tackling-college-completion-blockchain

[160] Dallas Community College District, "Dallas County Community College District Students Receive 'GreenLight' Toward Ownership, Lifelong Access to Academic Records," August 2019. https://www.dcccd.edu/news/2019/pages/viewnewsitem.aspx?NewsItem=38.

[161] Thomas Ahearn, "NAPBS Survey Reveals 95 Percent of Employers Conducting Employment Background Screening in 2018," July 2018.
https://www.esrcheck.com/wordpress/2018/07/02/napbs-survey-reveals-95-percent-employers-conducting-employment-background-screening-2018/.

enabling secure sharing of online credentials, verified for proof and under the individual's control. With blockchain, a party with which a credential is shared can verify both that it was issued by the purported issuer, by verifying the issuer's signature via a public key stored in a blockchain decentralized identifier (DID). Likewise, the party can also determine that the individual sharing the credential is the authorized recipient, again by verifying his or her signature via a public key stored in a DID. Finally, the blockchain can keep a record of revoked credentials, allowing the party relying on the credential to determine whether it is still valid.

Capturing a breadth of skills. Current credentialing systems do not necessarily reflect the skills of workers in a comprehensive manner. A liberal arts degree from a four-year institution, for example, is often considered a proxy for an individual's ability to reason and complete work, yet the same individual may gain skills on the job that are unrelated to or unrepresented by their degree. Notably, individuals who do not complete formal educational degrees have highly-valuable skills and experiences gained through employment or independent study, but may be unable to easily demonstrate these qualifications.

With the ever-increasing pace of change in the labor market, workers seeking to retrain or gain new skills now have multiple options beyond enrolling in formal degree programs. A broader-based credentials ecosystem powered by blockchain could enable more skills-based hiring and aid workers in navigating a changing labor market.

This dovetails with the ongoing efforts from California's Future of Work Commission, which among other things is addressing both "The impact of technology on work, workers, employers, jobs and society" and "the best way to...ready the workforce for jobs of the future through lifelong learning."[162] As echoed by the American Council on Education, "Blockchain, in particular, holds promise to create more efficient, durable connections between education and work."[163]

[162] State of California, Executive Order N-17-19, Governor Gavin Newsom, 14 August 2019. https://www.gov.ca.gov/wp-content/uploads/2019/08/Future-of-Work-EO-N-17-19.pdf.

[163] Kerri Lemoie and Louis Soares, "Connected Impact: Unlocking Education and Workforce Opportunity through Blockchain," Washington, D.C., American Council on Education, 2020, p. v. https://www.acenet.edu/Documents/ACE-Education-Blockchain-Initiative-Connected-Impact-June2020.pdf.

Iterative design process. To empower all Californians and bolster the workforce ecosystem, care must be taken to "stress test" the robustness of any new systems. A user-centered, iterative design process with stakeholder input could help the State to explore, test, and deliver technology and governance guidelines that support realistic use cases. The process should include representatives from a wide range of public and private educational institutions, informal learning communities, technology developers, policy makers, and the general public.

Although education and workforce development applications may have specific requirements and needs, the overarching successes and "lessons learned" from exploring blockchain-based technologies, particularly those used for other public sector applications, should be reviewed to better inform new projects and improve existing initiatives. As a convener and bridge between disparate areas of the state and region, the State of California is well poised to spark multi-stakeholder discussion and provide a forum to seed avenues for future collaboration.

Empowerment. A blockchain-based credentials system could empower a more diverse and nuanced set of credentials that reflect the pace and trajectory of modern work, and facilitate accountability in the gig economy. Employers could quickly verify skills of their employees and training programs could more easily document and prove the skills of their participants. Notably, the agility and scalability of digital credentialing can provide a path to engage smaller institutions and organizations, from new startups to community-led nonprofits, that historically have not had the resources to invest in credentialing or measure their workforce development efforts. Blockchain may "hold particular value for those currently underserved by the existing education-to-employment paradigm."[164]

Privacy. In particular, frameworks for "privacy-by-design" and "privacy-by-default" that can be adapted to a variety of scenarios, while adhering to transparent standards, will lead to more viable long-term solutions. With the goal of contributing to an "education landscape that increases learner agency and promotes more equitable learning and career pathways," the Digital Credentials Consortium of more than 12 higher education institutions is focusing on verifiable infrastructure for digital credentials of academic achievement, incubating

[164] Lemoie and Soares, *Connected Impact*, p. vi.

standards openly for "learner-controlled, privacy-preserving credentials, in a manner that ensures interoperability."[165]

Community of practice for blockchain. One can anticipate the need for supporting open and accessible education and training about blockchain and related technologies. Such training will build greater fluency with emerging concepts and identify opportunities for increased productivity and innovation by those creating, using or affected by blockchain-based applications. Educational efforts and content related to blockchain could include modular web-based tutorials, community training workshops, or a series of public-facing infographics or videos to provide a welcoming environment for learners of all backgrounds.

Whether the State collaborates with other organizations or hosts formal training or certification mechanisms on its own to generate a pipeline of skilled blockchain contributors, care should be taken to support a diverse and collaborative "community of practice" for blockchain. By prioritizing low-barrier-to-entry paths for individuals to collectively "upskill" and develop new blockchain competencies, the State and its partners can establish a healthy ecosystem that inspires growth and shared learning. Highlighting the value of blockchain through technology demonstrations and emphasizing key transferable skills, products, or services needed for the public sector will serve as a mechanism for not only accelerating practical blockchain innovations and innovators, but also for promoting the sharing of resources and ideas.

[165] Digital Credentials Consortium, "Building the digital credential infrastructure for the future," February 2020. https://digitalcredentials.mit.edu/wp-content/uploads/2020/02/white-paper-building-digital-credential-infrastructure-future.pdf.

VI. The Role of State Government

VI. The Role of State Government

Key Recommendations

REC VI.1. Consider establishing a **Blockchain Innovation Zone** to incentivize and provide safe harbor to blockchain companies working to solve California's most pressing problems.

REC VI.2. Foster collaboration through supporting a **multi-stakeholder advisory group** to promote best practices that would include government regulatory agencies, consumer advocacy groups and other industry stakeholders.

REC VI.3. Consider creating a **unit within the California Department of Technology** to monitor developments in the blockchain industry. Possible responsibilities for this unit include:

- Monitoring and reporting any consumer protection issues
- Training the IT workforce within government agencies
- Working with the state legislature and local governments to create flexible and adaptive regulations
- Attending or hosting conferences to encourage responsible blockchain business development in California
- Arranging community education programs to teach more Californians about consumer protective measures related to blockchain and ensure that our laws are adaptive to changes in the industry

REC VI.4. **Blockchain definition.** Legislature should adopt an accurate, concise definition of blockchain, such as that proposed in this report. With this agreement, policymakers can turn to two questions: 1) How can blockchain be used to increase efficiency? and 2) What changes to state laws and regulations will be needed to implement the new technology?

REC VI.5. **Neutral terminology.** Adopt technology-neutral terminology to expand use cases for blockchain.

Fostering a Welcoming Business Environment

Introduction

Blockchain technology offers decentralization, immutability, interoperability, security, transparency, and financial innovation to the economy and other fields. Over the next decade, blockchain technology may be integrated within many industries to enhance trust, safety, health, and efficiency in sectors such as healthcare, real estate, finance, data, energy, trade, and government. Blockchain technology is projected to have a value of $176 billion by 2025,[1] and 10 percent of global GDP is projected to be stored on blockchain ledgers by 2027. [2]

California is home to nearly 600 blockchain companies, around 6 percent of the global blockchain market,[3] less than the 20 percent California typically commands for most technology fields, given Silicon Valley's prominence in the State. Blockchain companies face regulatory uncertainty and lack safe harbors granted to other emerging industries. At the same time, such companies must comply with regulations established by Federal agencies including the SEC, the CFTC, and the IRS.[4]

The vast majority of blockchain businesses in California are small businesses and startups. Nearly two-thirds of the companies have 10 or fewer employees. California can add value to this market by supporting blockchain entrepreneurs with 1) blockchain-centered incentives; 2) greater regulatory certainty; and 3) opportunities to establish digital asset banking.

[1] ConsenSys, "Gartner: Blockchain Will Deliver $3.1 Trillion Dollars in Value by 2030." https://media.consensys.net/gartner-blockchain-will-deliver-3-1-trillion-dollars-in-value-by-2030-d32b-79c4c560.

[2] McKinsey Digital, "Blockchain beyond the hype: What is the Strategic Business Value?" https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.

[3] "California Blockchain Companies," *Crunchbase.* https://www.crunchbase.com/search/organization.companies/field/hubs/org_num/california-blockchain-companies.

[4] "Crypto Asset Market Coverage," Report by Satis Group.
https://research.bloomberg.com/pub/res/d2gg3p_HTg39HRCuzQjIyy8NVZQ.

Blockchain Innovation Zone

California should consider creating a Blockchain Innovation Zone in which qualifying companies receive incentives and resources. The incentives program should be tied to achieving state economic development benchmarks over the next decade, and only those companies working toward those goals (although not necessarily their only line of business) should be granted such incentives.

The State could consider offering qualifying blockchain companies legal exemptions currently lacking at the Federal level but have been adopted in other states including Arizona, Colorado, and Wyoming. The state could also offer grants, loans, and tax credits for blockchain startups working to serve key industries.

To qualify, blockchain companies should target sectors affecting California industries. This incentive package would reduce expenses for early-stage, cash-strapped companies looking to help California meet its policy and economic goals.

A. **Public-Private Partnerships.**
Expand the State's use of public-private partnerships, and sponsor pilot projects.

B. **Money Transmitter License.**
Consider amending current regulations regarding requirements for obtaining a money transmission license to accommodate cryptocurrency companies.

C. **Decentralized Autonomous Organizations.**
A cornerstone of blockchain companies is the Decentralized Autonomous Organization. DAOs are a collection of smart-contract automated agreements and business processes which guide the governance of many blockchain businesses. Participation in the DAO may require operating the blockchain's code ("proof of work") or obtaining and assigning the native-network asset ("proof of stake"). DAOs might be considered an advancement of co-ops with bylaws written in computer code. DAOs can serve the same purpose as co-ops while removing many of the administrative frictions. For

DAOs working toward the public good, California could provide protections like those created for non-governmental organizations (NGOs) or offer legal standing as a California Benefit Corporation.[5] This potential framework merits further study and analysis.

D. **Facilitate blockchain-enabled municipal finance.**
(See also discussion in Chapter V.) Municipal finance is about to face its biggest challenge in over a century with depressed revenues and likely continued need for social distancing, making paper-based approaches very difficult. The current proposal from the Federal Reserve to expand its plans to buy municipal bonds under emergency powers currently limits this option for counties with fewer than two million people or cities with fewer than one million residents. Such municipalities are raising their concerns, but States may be faced with needing to establish new arrangements to enable smaller entities to effectively raise financing. This is just one of the challenges that smaller municipalities will face in the coming months and years.[6] By expressly supporting the adoption of blockchain-based digital municipal bond issuance programs, the State can help address issues that will arise with municipal finance as well as support enterprise-class adoption of blockchain technology. A starting point would be to adopt legislation similar to Wyoming's, expressly allowing bonds issued by municipalities to be digital securities.[7]

Regulatory Clarity

One cornerstone of business success is clarity of the regulatory regime. Cryptocurrency is defined in five ways at the federal level: securities (SEC); commodities (CFTC); currency (Treasury); property (IRS); and money transmission (FinCEN). The latter is a particular thorn; in addition to obtaining necessary federal

[5] California Corp Code Div. 1.5 "Social Purpose Corporations Act." https://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml?tocCode=CORP&division=&title=1.&part=&chapter=&article=.

[6] Jeanna Smiaek, "Fed Gearing Up to Help Smaller Local Governments," *New York Times*, 20 April 2020. https://www.nytimes.com/2020/04/20/business/economy/fed-local-governments-coronavirus.html.

[7] State of Wyoming Legislation 2020. https://wyoleg.gov/Legislation/2020/HB0020.

Money Service Business licenses, companies wishing to engage U.S. customers must comply with individual licensing requirements in all 50 states and then must also apply for BitLicenses in states such as New York and Washington.

California can improve the blockchain business climate by adopting a common legal definition of blockchain and clarifying key regulations.[8] California could follow the lead of other states such as Arizona, Colorado and Wyoming and countries such as Singapore, Germany and Switzerland: define digital assets based on their function and regulate them separately. California could create three categories: i) payment, ii) consumptive/utility tokens, and iii) asset tokens, and exempt consumptive or utility tokens from state securities laws. The State should further research and explore these possibilities.

Working with Consumer Advocates and Other Stakeholders

Introduction

The need for regulators and advocates to work together on blockchain policy is clear. As a complex emerging technology, blockchain requires collaboration between subject matter experts and regulatory agencies to ensure that proposed regulations are proportional to the issue being addressed. While there is inherent risk in allowing stakeholders with business-fueled incentives to influence policy, a degree of inclusion is necessary to develop balanced regulation that addresses the true demands. Regulators will need to develop expertise they currently lack regarding cryptocurrency to effectively regulate it, and do so through a process that allows them to make independent and objective decisions.

Consider the New York State BitLicense. The designer of the virtual currency licensing framework indicated on numerous occasions that BitLicense was largely a response to the Mt. Gox cryptocurrency exchange hack. Although well-intentioned, the regulatory framework was prohibitively expensive for many smaller cryptocurrency businesses, and ultimately drove cryptocurrency business

[8] See efforts in this direction in legislation proposed by Assemblymember Calderon in February 2020: Assembly Bill 2150, Corporate securities: exceptions: digital assets. http://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB2150.

out of the state.[9] The complexity of cryptocurrency necessitates increased collaboration between industry experts who understand and have experience with real-world use cases and the regulators creating and enforcing licenses and other frameworks while ensuring that consumers' and investors' interests are adequately protected. The end goal is creating regulatory policy that protects consumers, provides businesses with legal certainty, and does not compromise the core concepts of a decentralized blockchain system.

Technical limitations also apply to policy and regulation to address blockchain. Because of the dynamic and rapidly changing nature of blockchain technologies, regulators alone are ill-prepared to execute regulatory functions on their own. Rather, continual collaboration between industry stakeholders and advocates is needed to effectively create, enforce and update regulations on blockchain.

From a paper in the Stanford Journal of Blockchain Law and Policy: "Especially because code embedded in a blockchain system could determine the level of oversight on the activities within a blockchain-based financial ecosystem, regulators should consider ways to cooperate with engineering communities developing code despite often disparate incentives and mindsets."[10]

Impediments to Collaboration among Regulators, Consumer Advocates and Stakeholders

One of the biggest roadblocks to regulators working together with advocates and stakeholders is the lack of open communication. While regulators are consistently becoming more technologically literate, agencies may not have sufficient resources to become subject-matter experts on blockchain technology, capable of making decisions in a vacuum. Shin'ichiro Matuso, research professor and director of the Blockchain Technology and Ecosystem Design Research Center at Georgetown University, has highlighted the need to solve this communication problem.

[9] Michael del Castillo, "The 'Great Bitcoin Exodus' has totally changed New York's bitcoin ecosystem," *New York Business Journal*, 12 August 2015. https://www.bizjournals.com/newyork/news/2015/08/12/the-great-bitcoin-exodus-has-totally-changed-new.html.

[10] "Call for Multi-Stakeholder Communication to Establish a Governance Mechanism for the Emerging Blockchain-Based Financial Ecosystem," Part 1 of 2 (2020), *Stanford Journal of Blockchain Law & Policy*. https://stanford-jblp.pubpub.org/pub/multistakeholder-comm-governance.

Referring to the lack of open communication and traditionally tense relationship between regulators and stakeholders: “The main issue is, we still don’t have proper communication channels among stakeholders in this ecosystem. Regulators don’t have a functional language to talk with open-source engineers. Open-source engineers sometimes do not want to speak with regulators.”[11]

To this end, government regulatory agencies, together with consumer advocacy groups and industry stakeholders, should consider a multi-stakeholder governance model for regulating blockchain technologies. Blockchain advocacy groups may include: Electronic Frontier Foundation, Blockchain Advocacy Coalition, Chamber of Digital Commerce, Colorado Council for the Advancement of Blockchain Technology Use, and Global Blockchain Business Council.

As a result of the decentralized and open-source nature of blockchain, a multi-stakeholder governance framework is necessary for oversight of blockchain systems. This runs counter to the general model of regulatory agencies, which are by definition central authorities. A multi-stakeholder framework, similar to the governance standard adopted for the Internet, has the potential to benefit all parties involved.

Recommended Amendments to California Statutes

Introduction

In establishing the Blockchain Working Group, California’s Legislature has taken the first step in studying blockchain technology and assessing its potential value in the public and private sectors, while weighing potential risks. Given the complexity of the technology and lack of familiarity among most lawmakers and residents, clarity is needed to evaluate any meaningful regulation or adoption. Rather than outlining comprehensive steps for current statutes to accommodate possible blockchain applications, this section intends to describe what other states have done, what principles should guide California’s regulatory framework, and what incremental changes could be implemented to meet California’s needs.

[11] “Bridging the gap between bitcoin and global regulators,” *Coindesk*, 17 July 2019. https://www.coindesk.com/bridging-the-gap-between-bitcoin-and-global-regulators.

Related Efforts in Other States

States such as Wyoming have taken a business-friendly approach, enacting a total of thirteen blockchain-enabling laws allowing the industry to flourish there. Meanwhile, states like New York have instituted a tighter regulatory framework, creating a license that imposes specific requirements for any business offering cryptocurrency services to New York–based customers. Like New York, California has tens of millions of consumers and access to investor capital. However, New York's approach is often regarded by blockchain advocates as too restrictive. Wyoming has been highlighted by industry advocates as successful in attracting business, but it is a far less populous state, with a far smaller and less complex economy, with the ability to be more nimble.

Guiding Principles

An important distinction that sets California apart from other states is Silicon Valley and its leadership in technology innovation. Given this characteristic, the following principles should guide California's regulatory framework.

1. **Promoting innovation:** As leaders in tech innovation, California companies seek to attract talent and startups from around the world. Overly prescriptive definitions or requirements may stifle innovation.

2. **Protecting consumers:** Some of the world's best known and most valuable companies are technology companies based in California. This makes them attractive targets for cybersecurity attacks. Indeed, six Silicon Valley companies are listed among the 15 largest security breaches of the 21st century, representing half of those in the United States.

   California is also home to some of the strongest consumer data protection regulations in the United States. The California Consumer Privacy Act (CCPA) of 2018 went into effect in January 2020, and an amendment to the Act, the California Privacy Rights Act (CPRA) will likely appear on the November 2020 ballot.[12]

[12] "CCPA 2.0 announces key signature threshold for ballot initiative," *National Law Review*, 5 May 2020. https://www.natlawreview.com/article/ccpa-20-announces-key-signature-threshold-ballot-initiative.

Given this reality, it is absolutely critical to adopt proper guardrails to protect all Californians from data breaches and bad actors. One way to ensure these protections would be to consider creating a unit within the California Department of Technology to monitor developments in the blockchain industry. This unit could:

- Monitor and report any consumer protection issues, including working with the federal government to protect against fraudulent activities.
- Train the IT workforce within government agencies to understand the technology.
- Work with the state legislature and local governments to create flexible and adaptive regulations, possibly including state disclosure requirements modeled after the federal securities laws.
- Attend or host conferences to encourage responsible blockchain business development in California.
- Arrange community education programs to teach more Californians about consumer protective measures related to blockchain and ensure that our laws are adaptive to changes in the industry.

3. **Equity and accessibility:** As the fifth-largest economy in the world, and one of the most culturally and ethnically diverse, California has an opportunity to promote access to blockchain technology for underserved and underrepresented communities. The State must ask how it can make the blockchain industry itself more diverse, based on gender, race, age, national origin, and socioeconomic factors, and how it can educate Californians about the potential of blockchain technology. A key component will be to expand workforce training. Partnerships with public universities and bolstering programs within the workforce development division of the California Department of Technology would be a good place to start.

VII. Acknowledgements

VII. Acknowledgements

The Blockchain Working Group would not have been able to complete its work without excellent organizational and strategic support from staff and leadership of the California Government Operations Agency:

- Yolanda Richardson, Secretary
- Julie Lee, Undersecretary
- Gabriela Montano, Blockchain Working Group Manager
- Stuart Drown, Deputy Secretary for Innovation and Accountability
- Oriel Gomez, Executive Fellow
- Viana G. Barbu, Attorney, Department of General Services
- Amy Palmer, Deputy Secretary for Communications
- Jacob Roper, Assistant Secretary for Communications

We are also grateful to Orit Kalman, Senior Mediator/Facilitator in the Consensus and Collaboration Program of CSU Sacramento, for expertly guiding the Working Group meetings, conducting the preliminary assessment, and finalizing the report.

Additional programmatic support was provided by Maitreyi Sistla, assistant at the CITRIS Policy Lab and recent graduate of the UC Berkeley Goldman School of Public Policy.

Thanks to Ripple and the University Blockchain Research Initiative for support to design the report and Ryan Olson for its design.

VIII. Appendix

VIII. Appendix

Cybersecurity: 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. Looking to the longer term, technology suppliers should be encouraged to incorporate crypto-agility into their offerings, so that it will be possible to modernize the underlying cryptography as/when required. For example, NIST and its contemporaries are aware of the potential threat to public-key cryptography from future quantum computers. Accordingly, NIST has been conducting a program to standardize "post-quantum safe" cryptographic algorithms. Crypto-agile systems would reduce the cost and time required to transition to these new standards and would also enable the rapid mitigation of threats to conventional cryptography as/when they emerge.

B. Ensure the provenance of a transaction before it enters the blockchain: Transactions should be digitally signed before they are submitted to the blockchain. Ideally, the provenance of transaction data originating in the physical world would be traceable, through a chain of signatures, all the way back to the point where the information was obtained from a human user or physical sensor. Realistically, this will not always be practical since, in many cases, the data entering blockchains will be sourced from existing legacy applications that lack such provenance records. This re-positioning of legacy applications as blockchain frontends will be essential to the rapid and smooth adoption of the technology.

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. In general, even encrypted sensitive information should not be placed on widely accessible blockchains. Since encryption protection has a limited lifetime (typically a few decades) efforts

should also be made to avoid placing long-lived sensitive information (such as healthcare records) on less accessible blockchains that lack strong access controls equivalent to those used with highly restricted databases.
Note that this does not preclude recording a digital thumbprint of sensitive information on a blockchain provided the thumbprint cannot be used to reveal the sensitive information itself. Such a record could be used to verify the authenticity of sensitive off-chain information that is stored in a separately secured and less accessible system.

D. Provide transparency regarding the integrity of transaction data originating outside the blockchain: While a digitally signed transaction provides assurances about the provenance of the transaction, it cannot guarantee the integrity of the data itself. Commercially reasonable and technology-neutral efforts should be taken to validate and preserve the accuracy of the data when importing, updating or reversing records on the blockchain.

E. Cryptographic Algorithm Implementations and Key Management
The implementation of cryptography algorithms is complex and most crypto vulnerabilities arise from errors in the implementation rather than in the underlying algorithms themselves. Application developers unaccustomed to working with cryptography also underestimate the intricacies of key-management (the discipline of managing the life-cycle of cryptographic keys).

Blockchain applications using cryptographic keys for encryption and signing should consider using field-proven software packages and/or certified cryptographic hardware solutions to implement the underlying algorithms and/or to secure cryptographic keys, in adherence to NIST guidelines and in keeping with best practices of the industry.

An additional consideration related to hardware-based key management arises when personal keys are managed by members of the public. For various reasons, some individuals may not be able to prevent the physical object that stores their signing key (e.g., a USB-like key fob) from being lost or stolen, and they may not have ready access to the facilities, processes and/or credentials that would restore their timely access to systems that provide them critical services.

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.

Survey responses

Throughout the process, a public survey was available on the GovOps Blockchain webpage for members of the public who wanted to provide information and feedback. GovOps received thirty-two entries. A summary of responses to survey questions are provided below.

Q1. What opportunities or constraints should policymakers keep in mind when crafting legislation regarding blockchain? Perspectives could address technical, economic, social, environmental or other concerns.

Respondents to the survey highlighted the importance of considering blockchain as a tool and evaluating blockchain in the context of other technologies when seeking to address a specific challenge. Opinions differed regarding the need for and the role of legislation in advancing blockchain. (9 responses)

Respondents highlighted opportunities related to blockchain adoptions for specific use cases and more generally in improving state government efficiency, effectiveness, transparency, and accountability. Several comments highlighted societal benefits related to state and local government functions as well as to the blockchain industry. (12 responses)

Respondents suggested that the Blockchain Working Group consider security, immutability, data ownership, and privacy in their analysis of appropriate use cases for implementation and highlighted the importance of balanced analysis. (10 responses)

Q2. Considering potential application areas, which sectors or cross-cutting applications may be well suited to adopt blockchain solutions? Which areas will need further technological or infrastructure development or regulatory changes before a blockchain framework could be implemented? Which, if any, sectors should NOT be considered for incorporating blockchain technology?

Respondents offered the following list of potential use cases for blockchain applications: Supply chain (5), Digital ID (4), Finance and banking (4), Healthcare (3), Social services benefits (2), Property (2), Voting registration (2), Data coordination (2), and Natural resources/Utilities (1).

Many of the responses cautioned against identifying application areas for blockchain as a 'technology in search of a problem' and expressed skepticism regarding the use of blockchain. (10 responses)

Q3. How can the state improve civic literacy regarding blockchain technology? What examples of successful user interfaces should the Working Group consider as models?

Respondents provided specific examples and tools for improving blockchain civic literacy including videos, user friendly interface, publicly accessible seminars and conferences that are put on by expert organizations, white paper, and incorporating blockchain into STEM education. Explanation of blockchain technology should be directly related to its use case application, provided in plain language, and in the context of general technology education. Respondents provided examples and links of accessible blockchain information. (22 responses)

Some respondents suggested that given that blockchain may not be an appropriate technology for state application, and that education and outreach are not needed. (4 comments)

Assembly Bill No. 2658
CHAPTER 875

An act to add and repeal Sections 11546.8 and 11546.9 of the Government Code, relating to blockchain technology.

[Approved by Governor September 28, 2018. Filed with Secretary of State September 28, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

AB 2658, Calderon. Secretary of the Government Operations Agency: working group: blockchain technology.

Existing law, the Uniform Electronic Transactions Act, specifies that a record or signature may not be denied legal effect or enforceability solely because it is in electronic form and that a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation. Among other things, the act provides that if a law requires a record to be in writing, or if a law requires a signature, an electronic record or signature satisfies the law.

Existing law specifies that there is, in the Government Operations Agency, the Department of General Services, which shall develop and enforce policy and procedures and institute or cause the institution of those investigations and proceedings as it deems proper to assure effective operation of all functions performed by the department and to conserve the rights and interests of the state.

This bill, until January 1, 2022, would require the Secretary of the Government Operations Agency to appoint a blockchain working group on or before July 1, 2019. The bill would define blockchain. The bill, on or before July 1, 2020, would require the working group to report to the Legislature on the potential uses, risks, and benefits of the use of blockchain technology by state government and California-based businesses, as specified.

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. Section 11546.8 is added to the Government Code, to read:

11546.8. (a) For the purpose of this chapter, "blockchain" means a mathematically secured, chronological, and decentralized ledger or database.

(b) This section shall remain in effect only until January 1, 2022, and as of that date is repealed, unless a later enacted statute, that is enacted before January 1, 2022, deletes or extends that date.

SEC. 2. Section 11546.9 is added to the Government Code, to read:

11546.9. (a) The Secretary of the Government Operations Agency shall appoint a blockchain working group and designate the chairperson of that group on or before July 1, 2019, to evaluate all of the following:

(1) The uses of blockchain in state government and California-based businesses.

(2) The risks, including privacy risks, associated with the use of blockchain by state government and California-based businesses.

(3) The benefits associated with the use of blockchain by state government and California-based businesses.

(4) The legal implications associated with the use of blockchain by state government and California-based businesses.

(5) The best practices for enabling blockchain technology to benefit the State of California, California-based businesses, and California residents.

(b) The working group shall consist of participants from all of the following:

(1) Three appointees from the technology industry.

(2) Three appointees from non technology-related industries.

(3) Three appointees with a background in law chosen in consultation with the

Judicial Council.

(4) Two appointees representing privacy organizations.

(5) Two appointees representing consumer organizations.

(6) The State Chief Information Officer, or his or her designee.

(7) The Director of Finance, or his or her designee.

(8) The chief information officers of three other state agencies, departments, or commissions.

(9) One member of the Senate, appointed by the Senate Committee on Rules, and one member of the Assembly, appointed by the Speaker of the Assembly.

(c) The blockchain working group shall take input from a broad range of stakeholders with a diverse range of interests affected by state policies governing emerging technologies, privacy, business, the courts, the legal community, and state government.

(d) On or before July 1, 2020, the blockchain working group shall report to the Legislature on the potential uses, risks, and benefits of the use of blockchain technology by state government and California-based businesses.

(1) The working group's report shall include recommendations for modifications to the definition of blockchain in Section 11546.8 and recommendations for amendments to other code sections that may be impacted by the deployment of blockchain.

(2) A report submitted pursuant to this subdivision shall be submitted in compliance with Section 9795 of the Government Code.

(e) The members of the working group shall serve without compensation, but shall be reimbursed for all necessary expenses actually incurred in the performance of their duties.

(f) This section shall remain in effect only until January 1, 2022, and as of that date is repealed, unless a later enacted statute, that is enacted before January 1, 2022, deletes or extends that date.

CalGovOps

CALIFORNIA GOVERNMENT OPERATIONS AGENCY