V. Potential Application Areas

Vital Records V.A.

Key Recommendations:

- The State should deploy a permissionless public blockchain to create and verify tamper-resistant digital certificates.
- New legislation should be considered to amend the Health and Safety Code sections 102400, 102430, and 103525 to include blockchain application.

Introduction – California Context

Vital records, 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 into school, and so on. The three most common types of vital records are birth certificates, marriage certificates and death certificates. While these three types of certificates are most commonly referred to as vital records, fingerprints, and other genetic data or identifiers could be considered as vital records as well.

In California, vital records are recorded by the local County Recorder's Office where the birth, marriage or death took place. Local county recorder's offices are primarily responsible for the initial intake and recording of information. This information is 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 entire state. Services provided by CDPH-VR include issuing certified copies of California vital records, registering, and amending vital records.[1]

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, multicolored, or impressed into the paper. 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 emails. The program utilizes the Ethereum blockchain to create a hash of a couple's physical marriage certificate. The

[1] SB 373 (2019-2020). http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200SB373

requestor receives a digital copy of the marriage certificate, which can be submitted to agencies to verify for authenticity. The pilot was a great success, with participating couples receiving their marriage certificates within 24 hours via email, instead of having to wait 7 to 10 business days.[2] This usage of blockchain is both more secure than the current paper process, and is also more expedient. The program has since expanded and is being fully implemented by the county.

Illinois Birth Certificates: The Illinois Blockchain Initiative (IBI) was launched on November 16, 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.[3] One of the pilot projects established by the IBI involved the development of digital birth certificates using blockchain technologies. The 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 certificates 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.[4]

Austin MyPass: In February of 2019, the city of Austin 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. [5] The pilot is in early development stages, as the City is still building the platform ~~and has not yet deployed it~~.

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 utilize blockchain technology. The initiative utilizes

---

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

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

[4] OpenCerts Website https://opencerts.io/faq

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

blockchain technology designed to make sure networks, systems, and data are free from compromise all while retaining data privacy. Estonia claims that digitization ensures its history cannot be rewritten by anybody and the authenticity of the electronic data can be mathematically proven. [6]

CONSIDERATIONS AND OPPORTUNITIES FOR BLOCKCHAIN APPLICATION

Equity: Access to identity is an integral part of our social and economic structure, both domestically and globally. Access to proper forms of identification allows individuals to participate in political, economic and social activities, and programs. This identity gap creates barriers for vulnerable populations from gaining needed benefits and social programs.

Using blockchain technologies for vital records such as birth, marriage and death certificates, has the potential to bridge the "identification gap"[7] by providing individuals with agency and power over their identity, as well as accessible and secure digital identification.

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 shown there are 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

[6] Julie Hamill, Harris Bricken. "Blockchain Technology: Local Government," p.7-8.

[7] Ibid, 3.

services. This allows for more efficient and secure interactions with government, which requires the proper forms of identification for verification.[8]

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 government 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 in conjunction with digital files while county registrars get 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 is generally stored is a hash of the data, not the data itself. A hash is a unique identifier for a piece of data (say, an identity record). All of the information in the identity record (name, date of birth, place 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. (e/d)

To preserve privacy, institutions should not store personal information on a blockchain, encrypted or not. They should also be cautious with the hashes of private data

[8] Young, Andrew and Michelle, Winowatan, and Verhulst, Stefaan. "Case Study: Registering Births on the Blockchain in Illinois." GovLab, October 2018. p.4. https://blockchan.ge/blockchange-birth-registration.pdf

[9] Senate Office of Research. "Issue Primer," p.3.

[10] Julie Hamill, Harris Bricken. "Blockchain Technology: Local Government," p.6.

[11] Julie Hamill, Harris Bricken. "Blockchain Technology: Local Government" 13.

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. (e/d)

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.[12]

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 assess 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.[13] The first and only legislation related to the management of vital records is SB 373 (Hertzberg, 2019) introduced in 2019 and still being considered 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

[12] State of Illinois. "Illinois Blockchain," p.14.

[13] Senate Office of Research. "Issue Primer—Blockchain Technology." "*Policy Matters"* June 2019. https://sor.senate.ca.gov/sites/sor.senate.ca.gov/files/Issue%20Primer%20-%20Blockchain.pdf

governments such as Berkeley and Sacramento have launched pilot programs that use blockchain technology to improve services, although no programs have yet centered on the use of vital records.[14]

Currently, the California Health and Safety Code governs California Law pertaining to vital records. Sections of this code outline everything from the creation of these records to access to them. Future legislation would need to address these codes.

ENDNOTES

HEALTH RECORDS V.B.

Key Recommendations

- 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 Health & Human Services, school districts and organizations that review immunization records, Centers for Disease Control, Immigration & Customs Enforcement, Food and Agriculture (bacteria detected in the food supply chain resulting in emergency healthcare).
- 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.
- The adoption of blockchain-based systems, combined with other advanced technologies such as AI/ML and 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.

Health Records

[14] Ibid, 4.

Health records are at the heart of documenting healthcare status and delivery. In order to achieve the best outcomes, reliable, complete records are essential. Electronic health records (EHRs) were conceived as the 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 siloed and has not achieved the degree of interoperability needed to bring disparate data sets together to deliver a unified context for patients.

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.

Context for California

At 39.5 million residents, California is one of the most populous states in the U.S. Its advances in technology and policy can often influence a broader national conversation. California, like other states, is also under pressure to improve processes and streamline regulations in healthcare from a budget perspective. The Covid-19 pandemic has both increased demand for healthcare while reducing public revenues to pay for it. ~~At the government level, healthcare encompasses issues ranging from financial/administrative systems, policy and regulatory compliance, health recordkeeping, health data storage and access, and associated issues of identity, security, privacy and interoperability.~~

Improving how patient records are managed will be central to any gains. California 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 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.

Interoperability (Adapted from the book *Enterprise Blockchain Has Arrived* by Radhika Iyengar and Jorden Woods)

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.

Struggles with interoperability spawn other issues regarding health data. Today, the healthcare industry largely uses information technology connected to the Internet. This, combined with poor security protocols at many healthcare facilities, has made centralized EHR systems easy targets for hackers who have stolen millions of patient records or created chaos with cyberthreats such as ransomware attacks. A distributed ecosystem such as blockchain could improve trust as well as interoperability among stakeholders.

Blockchain can 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 means that the healthcare process becomes more collaborative, and likely to produce better health outcomes more efficiently.[5]

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. Bockchain can improve data sharing and 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, the complexity of determining where to begin can be daunting. A relatively simple use-case could help determine whether blockchain can be used successfully to improve the efficiency of

the healthcare system. For example, immunization records could be stored within a California Immunization Blockchain.

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

- The "patient" being immunized
- The parents or guardians of the patient, if the patient is a minor
- The healthcare provider administering the vaccine to the patient
- The county that provides or maintains the immunization record
- "Relying Parties" that must verify the immunization record, such as:
    - A school where the patient attends, or where a teacher/employee works; volunteers at school events
    - Travel professionals who assist travelers in acquiring visas/permits to visit countries where such immunization records might be needed
    - 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

HIPAA is a requirement for privacy in health records. 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; details are available in the 2019 book *Enterprise Blockchain Has Arrived*.

Blockchain-related opportunities and challenges

When developing the healthcare framework for California, other ecosystems offer points of reference. Consider the healthcare models of Dubai or Estonia, both

progressive enterprising ecosystems that are considering or have deployed country-wide deployments of Digital Ledger Technology (DLT)-based health systems. A roadmap for considering blockchain implementations could include the following steps.

1. Prioritize problems to focus on for which blockchain has a useful application and solution
2. Define the 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 use cases
6. Determine what next steps ensue after results are established
7. Re-align with allies and partners, and identify new partners
8. Explore interoperability with other chains
9. Repeat process as warranted

With any system, a feasibility evaluation begins with scenario analysis, from keeping the status quo to on-ramping with blockchain. A thoughtful approach must start with a problem and evaluate what makes sense to solve a given problem. Few endorse the status quo with its embedded risks. Technology risks in blockchain include scalability, governance, potential cross-chain interoperability as well as blockchain-to-legacy system challenges. Permissioned systems are currently better positioned to deliver solutions that effectively address these challenges but deployment across a large state such as California will need 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.

Notes

1. *Enterprise Blockchain Has Arrived*, by Radhika Iyengar and Jorden Woods, copyright 2019, Chapter 17 (pp. 297-311).
2. https://www.healthit.gov/sites/default/files/page/2018-11/Draft%20Strategy%20on%20Reducing%20Regulatory%20and%20Administrative%20Burden%20Relating.pdf

Endnotes

1. Pipes, Sally. "California's Costly, Inaccessible Healthcare System". *Forbes*. Forbes Media. 23 July 2018. https://www.forbes.com/sites/sallypipes/2018/07/23/californias-costly-inaccessible-healthcare-system/#62689aea32f6 (accessed April 21, 2020)

2. Bryan, Darcy N., Jared M. Rhoads and Robert F. Graboyes. "Healthcare Openness and Access Project: Mapping the Frontier for the Next Generation of American Healthcare – June 2018 Update". *Mercatus Center: George Mason University*. June 2018. PDF: https://www.mercatus.org/system/files/bryan-healthcare-hoap-apr2019-mercatus-

project-overview-v1.pdf (accessed April 21, 2020)

3. Alyssa Keefe to Alex M. Azar II, Donald W. Rucker, MD and Seema Verma, January 28, 2019. Draft Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs. PDF: https://www.calhospital.org/sites/main/files/file-attachments/cha_comments_onc_draft_strategy_to_reduce_ehr_burden_012519_final.pdf (accessed April 21, 2020)

4. Bryan, Darcy N., Jared M. Rhoads and Robert F. Graboyes. "Healthcare Openness and Access Project: Mapping the Frontier for the Next Generation of American Healthcare – June 2018 Update". *Mercatus Center: George Mason University*. Jun. 2018. PDF: https://www.mercatus.org/system/files/bryan-healthcare-hoap-apr2019-mercatus-project-overview-v1.pdf (accessed April 21, 2020)

5. Woods, Jorden and Radhika Iyengar, *Enterprise Blockchain Has Arrived: Real Deployments. Real Value*. (Los Gatos, CA: Woods and Iyengar, 2019), 299-300
6. Ibid, 301
7. Ibid, 302-304

V.C. Supply Chain

This section includes analyses for blockchain application for food and agriculture and pharmaceuticals.

Key Recommendations

Tracking Food Contamination

- Work with the California Department of Food and Agriculture and the U.S. Food and Drug Administration to establish a pilot to use blockchain technology, based on the successful experiences of IBM and Walmart, to collect and organize data from growers, transportorters, 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 use of federal grant money to support the California-based pilot.

Food Freshness

- Explore the use of blockchain combined with IoT sensors and artificial intelligence (AI), 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. 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.

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 their oversight of agricultural co-ops and evaluate opportunities to revise their accounting practices and operations using blockchain technology.

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 avoid tripping U.S. regulatory concerns.

FOOD AND AGRICULTURE

INTRODUCTION – CALIFORNIA PERSPECTIVE

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% of U.S. dairy.[2] 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

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 identifying the source of tainted products. Food Trust was developed by IBM on Hyperledger Fabric and launched in late 2018. 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, Tyson Foods, Unilever, Dole, Driscoll's, and more. Both Walmart and Carrefour, a large European supermarket, are requiring all vendors for particular food products to use the platform in 2019.

Walmart China Blockchain Traceability Platform (WCBTP) is focused on food safety, like IBM Food Trust above, and will provide similar services for food products in Walmart China's supply chains. It is being developed with VeChain, PwC, Mongolia Kerchin, and the China Chain-Store & Franchise Association. By the end of 2019 over 120 food product lines will be fully tested across 10 product categories. The service will launch during 2020 and by the end of the year will cover 50% of meat sales, 40% of vegetable sales, and 12.5% of seafood sales. Consumers will be able to access traceability information and food inspection reports by scanning a QR code with a smartphone. The platform is being developed with VeChainThor.

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. "Food safety regulators in Oregon are confident that will lessen the time it takes to trace back the source of a food-borne disease outbreak from days or weeks to minutes or even seconds, helping to decrease illnesses while issuing more precise recalls. Growers benefit by ensuring their fruits, vegetables, meat and seafood are as fresh as possible by the time it reaches customers." [5]

Several other baby food and milk producers are already using blockchain for food traceability. Nestlé and Carrefour[8] are tracking infant formula using the IBM Food Trust blockchain. 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[3]

Adapted from Enterprise Blockchain Has Arrived, by Jorden Woods and Radhika Iyengar, Chapter 11

Blockchain-based systems can provide visibility and better data across supply chains. Common applications relating to Food and Ag 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, which may lead to significant losses for food producers and distributors when products are pulled from shelves en masse 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. 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 security is one specific use 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.

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 RFID technology to track items. These systems rely on centralized certificate authorities and centralized databases. They 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 product tracking to its origin (traceability) and through every step of the supply chain (authenticity). Building on this foundation, 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 a food product, is in fact authentic. The dApp enables a user to scan a QR code on the product which provides a full trace and validation of the product's authenticity.

Such an approach tracks the product or a product's components through every step in the chain, for example via an embedded RFID or NFC chip. At each step in the chain, 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. Each entry in the blockchain ledger is cryptographically signed and encrypted which deters fraud and reduces the chance of hacking. Since the entire supply chain process is transparent, it becomes possible to quickly and inexpensively validate product authenticity. Any product that does not enable dApp-based authenticity becomes suspect, which discourages fraud.

Provenance takes authenticity one step further by also providing information about the entire history of a product through the supply chain. For example, the location history, the custody history, and the environmental conditions during the journey can be tracked and stored immutably on the blockchain. This type of information—GPS coordinates, custody IDs, temperature data, accelerometer information (for damage assessment)—is typically provided by Internet of things (IoT) devices. These devices send out data streams that, in combination with decentralized consensus, are written to

the blockchain. Since blockchain technology reduces verification costs, it will likely gain widespread adoption and make checking product authenticity and provenance commonplace.

Examples of this capability include Walmart China's WCBTP (above), and an offering from Carrefour for over 20 different products including milk, meat, eggs, and fruit sold in their stores. 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. As a result, they are now introducing the same capability to 100 more products. The feature has been most popular in China and in Europe.

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 not be possible to know where in the chain the damage occured. 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.

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 continuously measure temperature and store the log, via a hash on the blockchain. This log then provides an immutable and independent temperature record that can be used for 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."[10]

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 over 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"[11] pilot, and by IBM through FarmerConnect,[12] 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. 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.[13]

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 is evolving quickly.[14] In addition to tracking provenance, proper lab testing and labelling 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, these labels must be understandable and trusted by average consumers.

Already a startup community in the blockchain and cannabis space is emerging, and they 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.[15] 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.[16] 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.

Labor Rights and Social Services for Farm Workers

California's agricultural economy substantially depends upon lower-income and seasonal workforces, many of whom move between locations depending on the crop and time of year, sometimes across national borders. Often these workers lack formal identification, a Social Security ID number, or knowledge of available social services, and are vulnerable to abusive employers. And when obtaining those social services, a lack of formal identity can make it difficult to develop a care record, while also opening up the service providers to the potential for abuse. And yet this population may be resistant to exclusively government-tracked systems due to a lack of trust.

Several projects are looking at the use of blockchain-based identity, in particular the application of user-managed or "self-sovereign" digital identity systems backed by blockchain technology, as a way to provide both identity cards and social services to vulnerable populations. A substantial amount of research into this work in the Netherlands, from a project on ensuring GDPR compliance in the provision of services and assessing fines conducted by TU Delft and Ledger Leopard[19], to more generalized efforts like the non-profit ID2020[20] and the for-profit Tykn.tech.[21]

One promising project for monitoring labor abuses in challenging environments is being conducted now by Coca-Cola and the U.S. State Department in conjunction with the Blockchain Trust Accelerator[22] regarding Coca-Cola's supply chains in the Asia Pacific region. This project employs "blockchain and smart contracts to deliver greater transparency and record-keeping regarding laborers and their contracts [...] The group hopes, however, that a clear trail of evidence will make compliance a more likely outcome."

Finally, it is worth noting that migrant workers who cross national borders are likely to be large users of remittance services, often provided by operators who demand cash and levy substantial transaction

fees. Remittances via cryptocurrencies or stablecoins may slash those transaction costs and complexity. Safe and appropriate adoption of such technologies could also be included in training and education.

There are lesser but still substantial aspects to the agricultural business in California that merit special attention for blockchain activity by policymakers and regulators:

-

PHARMACEUTICALS

Key Recommendations

- 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. This approach can combine practices of PharmaLedger with consortia in the U.S. private sector.
    - 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.
    - Compliance will be the biggest driver for many CA stakeholders in the pharmaceutical industry. Many California pharma companies as well as their partners, such as distributors and retail pharmacies, are already 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 residents.

INTRODUCTION – CALIFORNIA PERSPECTIVE

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.

Fake drugs for every therapeutic treatment exist, with a majority of falsified drugs targeted to chronic illnesses, antibiotics, antivirals, as well as alimentary drugs such as cholesterol and diet pills. In the US, we are also seeing demand for opioid drugs, particularly those with fentanyl, a synthetic opioid. According to the Centers for Disease Control (CDC), fentanyl-related overdose fatalities are rising exponentially – from 2013 to 2016 fatal overdoses involving fentanyl have doubled each year, leading to tens of thousands of deaths.

With the mega billion-dollar global counterfeit drug market annually, there is a clear motivation in the pharma sector to fight counterfeiting. What is also at stake are human lives, with adverse reactions and effects to these fake drugs leading to illness and hospitalization and fatalities. In emerging markets, 10-30% of prescription drugs are counterfeit, and in certain parts of the world, up to 50% are fake. Issues range from tampered drugs to drugs with incorrect, often toxic, ingredients or incorrect proportions of ingredients.

Today, pharma supply chains are becoming increasingly complex and globalized with the increased demand for more affordable drugs. "Since the 1990s, the pharmaceutical industry has increasingly used factories in lower cost economies to manufacture their products; according to the US Government Accountability Office 40% of finished medications are now made outside of the US." Furthermore, with nearly 90% of the pharmaceutical drug ingredients being sourced outside the US, the impact on generics is significant.

With the increased demand for generics which are more affordable, there is a greater responsibility to safeguard consumers in the US as well as to make the supply chains more transparent in the case of drug recalls. An unprecedented number of recalls of various generic drugs like blood pressure medications such as Losartan (one of the 10 most prescribed drugs), Valsartan, and Irbesartan. These recalls have taken place since July 2018 because the detection of carcinogenic impurities. [2]

There is also a rising awareness of the impact of counterfeit drugs on public health, and FDA regulations are forcing the pharmaceutical industry into compliance. In the US, the Drug Supply Chain Security Act (DCSA) was passed in 2013 to require electronic serialization and traceability of all pharmaceutical drugs from manufacturer through distributor to consumer. The DSCSA was passed to safeguard the safety of prescription

drug supply chains. Product information, manufacturing information, logistics routes and other key information must be shared with all supply chain partners involved in the delivery of the particular drug to the patient. The first critical milestones were reached in November 2019, with full compliance expected in 2023.

To assist with achieving compliance with the 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, The Optimal Solution, TraceLink, and IDLogiq. These initial pilots showed positive results and suggest that a blockchain-based solution will enable compliance with the Drug Supply Chain Security Act (DSCSA) while improving operations and reducing the supply of counterfeit drugs.

As discussed in the Food and Agriculture section of this report, at the root of global pharmaceutical fraud is a supply chain transparency and product authenticity problem. 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 also be much more difficult for bad actors to tamper with the process or for pharma companies themselves to market fraudulent products. It is for this reason that the blockchain community in China has called for placing all vaccine data on a transparent blockchain system.

With 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 as bring operational efficiencies to pharmaceutical companies. Some might wonder whether the benefits outweigh the

risks or costs. While we are still in early days for implementing blockchain solutions, early results from pilots in 2019 provide support for optimism.

For example, the MediLedger Project, which comprises 25 major pharma manufacturers, distributors, logistics partners and other stakeholders, was approved by the FDA for a pilot in 2019. 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." (MediLedger DSCSA Pilot Project Final Report, February 2020)

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, utilize ZKP to preserve privacy and confidentiality while still providing transparency along the supply chain.

NOTE: There are other use cases for improved drug discovery and development processes, and clinical trials. These, however, are not in scope of discussion in this section.

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). MediLedger was started in 2017 and was accepted into the FDA pilot program in 2019. It includes 25 members that span many major pharmaceutical companies, retail pharmacies, and medical distributors such as Pfizer, Amgen, Genentech, Lilly, Gilead, Novartis, Sanofi, GlaxoSmithKline (GSK), Walmart, Walgreens, McKesson, Cardinal Health, Amerisource Bergen, FedEx, and others. Chronicled is the main technology partner. Product authenticity is required under the law by November 2019 for saleable returns, a $6 billion market in the US. The network plans to launch just prior to the deadline.*

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 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. The pilot project results will be available in Q4 2019.*

CONSIDERATIONS AND OPPORTUNITIES FOR BLOCKCHAIN APPLICATION

Since 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.

Concerns over contamination have been a major issue since health officials have recently overseen recalls in 30 countries of blood-pressure medications made with tainted ingredients. Congresswoman Eshoo's office issued a press release which cites her Sept. 10, 2019, Washington Post Op Ed, "China's Grip on Pharmaceutical Drugs is a National Security Issue": "the supply chain already poses a significant public safety issue to the quality deficiencies that keep arising in the manufacturing of drugs overseas." The only time consumers find out they have consumed a contaminated active ingredient pill is when there is a recall and crisis.[3]

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. Finding common ground with competitors is a new type of thinking required in blockchain consortia. As noted in the MediLedger pilot, benefits include improved efficiency and greater interoperability which can be attractive to participating members.

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 pharmacies, hospitals/clinics, and consumer or patient advocacy groups.[4]

One of the highest priorities in any system is patient safety. Safeguarding patient safety is currently motivating all stakeholders to successfully solve systemic supply chain issues in the US. Certainly, as we are writing this report in the midst of the Coronavirus pandemic, patient safety is at the top of our minds. Anything that can mitigate health risks to patients is always important; during a public health crisis, it is critical. Safe treatment and sufficient supply are tremendous responsibilities and top priorities for the government and regulatory bodies.

Well-managed pharmaceutical supply chains ensure that medicines are accessible to all. When patients need their prescriptions, they should be assured that their medications will be available. Transparency across pharma supply chains ensures visibility of prescription drugs along the chains to prevent product shortages. Supply chain visibility also helps pharmacies and other 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 likely 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, 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.

BIBLIOGRAPHY

1. Challener, Cynthia A. "Why the Industry is Moving Toward Blockchain Technology". *Pharma's Almanac*. Pharma's Almanac TV. Dec. 6, 2019. https://www.pharmasalmanac.com/articles/why-the-industry-is-moving-toward-blockchain-technology (accessed April 21, 2020)
2. Dr. Rut, Andrew. The Challenge of Transparency in the Global Supply Chain. *pharmaphorum*. Apr. 4, 2019. https://pharmaphorum.com/views-analysis-market-access/the-challenge-of-transparency-in-the-global-supply-chain/ (accessed April 21, 2020)

ENDNOTES

1. Woods, Jorden and Radhika Iyengar, *Enterprise Blockchain Has Arrived: Real Deployments. Real Value.* (Los Gatos, CA: Woods and Iyengar, 2019), 194
2. U.S. Food and Drug Organization. FDA Updates and Press Announcements. "Angiotensin II Receptor Blocker (ARB) Recalls Valsartan, Losartan, Irbesartan". Washington: US FDA. Web. 7 Nov. 2019. https://www.fda.gov/drugs/drug-safety-and-availability/fda-updates-and-press-announcements-angiotensin-ii-receptor-blocker-arb-recalls-valsartan-losartan (accessed April 21, 2020)
3. Congresswoman Eshoo, Anna G. California's 18th Congressional District. *Press Release: Eshoo Holds Hearing to Address Broken Global Pharmaceutical Supply Chain.* Palo Alto: 2020. Web. 30 Oct. 2019. https://eshoo.house.gov/media/press-releases/eshoo-holds-hearing-address-broken-global-pharmaceutical-supply-chain (accessed April 21, 2020)

4. Ghosh, Arun. “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 (accessed April 21, 2020)
5. Woods, Jorden and Radhika Iyengar, *Enterprise Blockchain Has Arrived: Real Deployments. Real Value.* (Los Gatos, CA: Woods and Iyengar, 2019), 196-197

ENDNOTES

1. Netstate.com. Nstate, LLC. Web. 2017 https://www.netstate.com/economy/ca_economy.htm (accessed April 21, 2020)
2. California Department of Food and Agriculture. California Agricultural Production Statistics. Sacramento: CDFA. Web. https://www.cdfa.ca.gov/statistics/ (accessed April 21, 2020)
3. Woods, Jorden and Radhika Iyengar, *Enterprise Blockchain Has Arrived: Real Deployments. Real Value.* (Los Gatos, CA: Woods and Iyengar, 2019), 172-174
4. Woods, Jorden and Radhika Iyengar, *Enterprise Blockchain Has Arrived: Real Deployments. Real Value.* (Los Gatos, CA: Woods and Iyengar, 2019), 176-177
5. Singh, Kuldeep. “Oregon Farmers Use Blockchain to Track Crops”, C#Corner. 21 Jan 2020. https://www.c-sharpcorner.com/news/oregon-farmers-use-blockchain-to-track-crops
6. Sylveser, Gerard (editor) “E-Agriculture in Action: Blockchain for Agriculture Opportunities and Challenges”. *Food and Agriculture Organization of the United Nations (FAO) and International Telecommunication Union (ITU)*. 2019. PDF. http://www.fao.org/3/CA2906EN/ca2906en.pdf (accessed April 21, 2020)
7. Ledger Insights. “Danone Uses Blockchain for Baby Formula Traceability”. Ledger Insights. Feb 2020. https://www.ledgerinsights.com/danone-blockchain-food-traceability-baby-formula/ (accessed April 21, 2020)
8. Alibasa, Benedict. “Retail Giant Carrefour Saw Sales Boost from Blockchain Tracking”. Coindesk. 4 Jun 2019. https://www.coindesk.com/retail-giant-carrefour-saw-sales-boost-from-blockchain-tracking (accessed April 21, 2020)
9. Gnetii, Vsevolod. “Icons of Italian Business Opt for Blockchain”. Bitnews Today. 6 Jun 2018. https://bitnewstoday.com/market/blockchain/icons-of-italian-business-opt-for-blockchain/ (accessed April 21, 2020)

IBM Research. IBM. New York. Web. https://www.research.ibm.com/5-in-5/harvest/ (accessed April 21, 2020)

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

Real Estate

- Continue to monitor ongoing efforts for potential applications in land titling, despite limited proof of success for solving existing problems with blockchain to date.
- Explore issuing real estate licenses on a blockchain system while continuing to run the existing process in parallel until a new system is proven. Application may offer a more efficient license tracking system that could eliminate interstate fraud and streamline interstate collaboration. Further discussions are needed with the Department of Real Estate to understand interest and readiness for this type of pilot.
- 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, we 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 visionaries 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.
- Consider whether to explore partnership with the Real Estate Standards Organization (RESO) and Consensys to pilot the blockchain unique identifier real estate license proof of concept.
- Consider further investigation into recording only new construction real property onto the blockchain to test a blockchain real estate recording system.
- 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. We recommend the procurement officials have access to skilled and unbiased technical review and assistance in order to evaluate proposals effectively.

Vehicles and Parts

- Further investigation is needed to identify whether there are specific regulatory barriers to applying blockchain technology to vehicle and parts use cases. None are known at this time.
- Discussions with the Department of Motor Vehicles should continue to determine whether registration of vehicles and parts is an appropriate use case for blockchain technology.

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.

REAL ESTATE TITLE

INTRODUCTION – CALIFORNIA CONTEXT

The titling of real property is a tremendous driver of economic empowerment. 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. 28,500 home transactions closed escrow in California in February 2020, a nine percent 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 California, a roughly one percent decrease from 2018. Even though it is widely speculated that home sales will take a hit due to the pandemic, perhaps not recovering until 2022-2023, 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. 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. Establishing ownership may be

complicated due to fraudulent transactions making it difficult for a buyer, the seller, an insurer, or the taxpaying public to bear the cost of an incorrect interpretation of the title history.

Challenges of the 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. Blockchain is considered as an approach to address weaknesses in the current common-law title process, reduce fraud, increase efficiency, and reduce costs to the end user.

PILOTS AND RELATED CASE STUDIES

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

Chicago (Cook County). Velox worked on a pilot with Chicago's Cook County to record titles on the blockchain. (Note that 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."

While individuals seem to have transacted on real estate using cryptocurrency, a promising larger scale potential use case for blockchain technology in industry is in title insurance, discussed in the Property - Insurance section of this report. Private companies have also attempted to use blockchain to buy and sell tokenized real estate.

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. 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.

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

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 US National Association of Realtors (NAR) has invested an undisclosed amount.

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

Considerations and Opportunities for Blockchain Application

Responsible Entities: 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.

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

Current IT Infrastructure. Further work is needed to understand how the 58 California counties record deeds. Each county likely has its own process, some which are more technologically up-to-date than others. The California Department of Real Estate has an online search function for public license information, though the department will

need to be consulted to understand the exact architecture of their database and personnel requirements.

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 in Oracle or mysql (with read replication available to anyone who wanted, who could annotate as they chose) or on a blockchain-based system will make title research easier and more conclusive. Easier title research, in turn, would reduce fraud which in a competitive market might lower insurance rates. 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 a firm already aggregates 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.

Security and Privacy. Since 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.

Blockchain Implementation Potential Barriers and Concerns

Permissioned blockchains as a datastore. Supposing that California decides to move to open standards, open APIs or feeds, while public, transparent data, continue to be maintained by county recorders, either permissioned or public blockchain systems may be considered as the underlying datastore.

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 can be built on either open source datastores (like mysql or postgres), on proprietary datastores (Oracle), or on blockchains.

Permissioned blockchain solutions may have advantages and disadvantages in how validation and replication are accomplished. With the advent of blockchain technology, adopting more open rules (unpermissioned or semi-permissioned) for recording property transfers, in which members of the public could directly record

property transactions in a distributed ledger should be considered. While this is intuitively attractive, absent tremendous progress in digital identity, title fraud would likely be *increased* by such a system rather than *decreased*.

Private-sector application. Further study is needed to determine if private-sector actors could benefit from blockchain technologies to promote higher convenience, lower costs, and more competition in this space and if there is a role for government to support that. Specifically, additional research is needed about the internal technology tools that would enable title insurers (or mortgage lenders and other parties) to more efficiently and confidently validate title, or technology tools that give new entrants a competitive advantage.

Trust consideration. If each state is an authorized writer to the blockchain system and each person has a unique identifier, states should be able to trust entries written by other states thereby eliminating the need for intermediaries.

VEHICLES AND PARTS – REGISTRATION AND TRACKING

INTRODUCTION – CALIFORNIA CONTEXT

The California Department of Motor Vehicles (DMV) holds customer demographics, identity, residency, and social security number (SSN verification status for 80% of Californians. 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. This was a two percent increase, or approximately 716,000 increase 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 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. When it comes to fake auto parts, the largest concern is safety since the part may underperform or fail completely, with disastrous consequences to human life.

Pilots and Related Case Studies

Several companies are innovating with blockchain in the automotive industry:

Autoblock: Uses blockchain ecosystem to buy and sell cars.

Axt: Offers a more 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.

carVertical: Reports on car usage histories.

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

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: One company is focused on using blockchain to improve government processes. 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. CHAMPtitles aims to secure state contracts.

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, is required to transfer title of a new or used vehicle to the seller. Not only are new and used vehicles subject to the transfer process, impounded vehicles up for auction and vehicles going to dismantlers and junkyards must also undergo the transfer process. The existing process is very manual 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 illegal transfers.

Vehicle recording. The blockchain system could record each vehicle as it rolls off the 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 can 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 this application.

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, complete vehicle transaction history
- Allows all parties to have the same validated record
- 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 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. Digital identity is key 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 – CALIFORNIA CONTEXT

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.

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. 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 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 (Title Insurance). First American is one of the leading title insurers in the United States, with revenues of $6.2 billion in 2019. In 2018, First American announced the launch of a blockchain system for the real estate title production process. 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 US, has agreed to participate. First American designed the system and the technology used was not disclosed. 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.

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." Therefore, some organizations like the American Land Title Association (ALTA) conclude that blockchain may enable efficiencies in the title insurance process, but would not replace the need for human oversight in the form of title insurance professionals.

Beenest. Beenest, a decentralized home-sharing platform, developed blockchain-based homeowners insurance for Beenest homeowners. 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 use similar ideas for auto insurance and claims.

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. They have 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.

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 direct perspective, security and privacy are not a significant issue unless we are considering upgrading systems of record that insurance companies rely on. In most cases, these records would be public so 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.

Efficiency. To the extent real estate property, vehicles and parts, or other property documentation use blockchain systems or are simply digitized and made more broadly available, the insurance industry could use these systems to become more efficient at confirming information and automating policy payouts. Since many insurers operate nationwide, any technological changes would likely affect not just California but the whole country.

FIREARMS

INTRODUCTION – CALIFORNIA CONTEXT

Within the United States there are both state and federally managed databases for firearm tracking and background checks. At the federal 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. The Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) operates the National Tracing Center (NTC), which tracks firearms involved in criminal investigations.

In 2019, the California Department of Justice established a state-level firearm tracking system, the Automated Firearms System. 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, Concealed Carry 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

There is not a large body of literature on potential applications of blockchain in firearm tracing.

Electronic gun safe. 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 blockchain in an immutable, time-stamped manner.

Electronic gun safes could include pertinent information about the individual, such as criminal background and mental health background. Firearms transfers, purchases, or sales could be verified through a blockchain's immutable and time-stamped ledger.

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. At this point, most blockchain-based firearm tracking applications are theoretical.

ENDNOTE

UTILITIES AND NATURAL RESOURCES V.E.

Key Recommendations

- Additional discussion and research is required to understand whether regulatory sandboxes are feasible in California.
- Review additional literature and interview government experts from the National Association of Regulatory Utility Commissioners (NARUC), National Association of Chief Information Officers (NASCIO) and the National Governors Association to complement discussions with the International City/County Management Association (ICMA) and the National Conference of State Legislatures.
- In the case of water management, we recommend that the state 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 – California Perspective

Blockchain is a flexible technology that theoretically has dozens if not hundreds of different 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 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.

California is in the early stages of integrating blockchain into utilities. Two often-cited blockchain-utility pilot projects in California are led by municipal utilities and focus on electric vehicle charging. Although these projects have limited scope, they offer a glimpse into how blockchain could be more widely used by California utilities.

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."[1] Duncan McGregor, a Power Ledger Analyst, explained that Power Ledger's blockchain platform was used to help Silicon Valley Power prepare and submit regulatory reports.[2]

"Using the Power Ledger platform, Silicon Valley Power tracks production and use of energy at the solar-PV- and battery-equipped six-story parking garage in the heart of the city's entertainment district. Digitizing electric vehicle (EV) charging transactions helped the utility earn credits under the California Air Resources Board's (CARB's) Low Carbon Fuel Standard (LCFS)." [3] Charging data is tracked in real time and secure from alteration.[4]

The proof-of-concept project was ultimately a success, simplifying the LCFS crediting process for participants, and it ended in 2019.[5] Power Ledger hopes to continue the partnership with Silicon Valley Power in the future and is currently working with renewable energy developer, owner, and operator Clearway Energy Group to create a platform to trade Renewable Energy Certificates (RECs) in California.[6]

Sacramento Municipal Utility District Electric Vehicle Pilot Project. The Sacramento Municipal Utility District (SMUD) "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."[7] The charger automatically begins charging when a surplus of energy is available, and consumers are charged a discounted rate. [9] Consumers will be offered "rebates or credits on charging that they can accumulate as blockchain-enabled tokens."[10]

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.[18] 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. 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. 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, Director of Innovation and Insights at the World Energy Council.[20]

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 a single centralized utility. A smart grid enables "bidirectional flows of energy and uses two-way communication and control capabilities that will lead to an array of new functionalities and applications."[21] "A microgrid is a localized energy system that can operate independently of the traditional electrical grid that delivers electricity from public utilities to consumers."[22] And peer-to-peer energy transfer enables "direct energy trading between energy consumers," such as consumers with their own solar panels. [23] All of these modernized grid concepts may be used separately or simultaneously within a system. They allow for a more flexible grid that 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 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.[24]

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."[25]

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."[26]

Julie Hamill of the International County/City Management Association (ICMA) writes that although blockchain isn't necessary for a microgrid to function, "blockchain in a microgrid system will provide more transparency and efficiency."[28]

Improved Data Collection and Transparency. Even without restructuring distribution systems, utilities could use blockchain to improve data collection, which might streamline administrative functions like billing and data validation.[29] 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.[30] A benefit to exploring blockchain-enabled back-office solutions is that these administrative applications are far less likely to encounter regulatory restrictions compared to the front-end applications that may affect how energy is used or sold.[31]

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.[32] 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."[34] Data could also be shared with auditors, helping to reduce auditing costs and other administrative costs.

Security and Privacy. It is hard to say whether blockchain will add value to security in the utilities sector. Hamill (ICMA) explains:

> "There is no such thing as a purely immutable and unhackable system, in any context. Depending on the type of blockchain utilized (public or private), there are risks of a bad actor accumulating 51 percent of CPU power in a network and manipulating data, or it is possible that an authorized administrator of a private network is hacked or corrupt and manipulates or releases data. However, if the technology experts are to be believed, blockchain technology greatly reduces the chance of data manipulation, and any such manipulation could not occur undetected."[35]

Depending on the security of a utility's database technology, the immutable nature of blockchain alone could provide improvement. However, to understand where blockchain can add specific security value, areas of vulnerability in the system must first be identified. Amy Ahner of the ICMA suggests that users first identify the points of risk in an operation, and then evaluate whether blockchain can fill those gaps.[36]

In terms of personal privacy, only some applications of blockchain within these sectors raise concerns. Blockchain in smart devices could track individual home power use, such as when and for how long phones are charged or the stove is in use.[37] However, this privacy concern is more closely related to the smart devices, rather than the blockchain platform the information is stored on. Blockchain used in back-office systems would likely have little impact on personal privacy.

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."[38] 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 came across 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." 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."[39] 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.[40] 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 be unallowable whether the technology that enabled 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. Duncan McGregor, an Analyst from Power Ledger, a blockchain-based energy trading platform, indicated that ambiguity and uncertainty around regulations can pose a barrier to blockchain projects in the sector, especially regarding the tokenization of energy credits. [41] Power Ledger is based in Australia, but has active energy and blockchain projects across the globe, including a partnership with the municipal utility Silicon Valley Power in Santa Clara.[42] McGregor explained that blockchain is easier to experiment with in Australia because the government has been enthusiastic and encouraging about the technology.[43] Parts of Europe and Australia have developed a regulatory tool, the "sandbox," that gives companies more freedom to test new technology like blockchain.

At the same time, 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."[44]

Overcoming negative stigma surrounding Bitcoin. Some within the blockchain industry worry that cryptocurrencies and the media attention surrounding their use by bad actors engaging in illegal activities has damaged blockchain's reputation. McGregor noted that negative stigma surrounding Bitcoin has harmed the reputation of tokenizing technology; however, tokenization is a central feature of the energy trading system used in smart grids.[45] Giroti said, "many people perceive blockchain as Bitcoin, and they think we always need cryptocurrency. The fact is, you can use Blockchain technology to solve many many problems, without the use of any cryptocurrency. Because of this misunderstanding, there is hesitancy."[46]

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 the regulatory process."[47] Giroti notes that "all the current use cases right now are very preliminary."[48] 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.

Educating about blockchain. Ahner also noted the need to build a process to educate people about blockchain technology to prepare them to work more effectively in this area. [49] From a greater theoretical understanding in academia to a more practical understanding in workplace training, "the pipeline needs to become established."[50]

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.[52]

Water Management. California was the first state in the United States formally to recognize the human right to water.[53] Still, California faces significant water management challenges that intensify the impact of droughts, floods, and other water supply disruptions. Improved data collection and better access to data 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.[54]

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.[55] Johnson deployed "simple, solar powered sensors, originally developed to monitor creaky groundwater pumps in East Africa. [56] The sensors will be used to detect how much water is flowing in real-time."[57] 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. [59]

Considerations and opportunities for blockchain application

Blockchain could facilitate more effective coordination of water data and allow stakeholders immediate access to that data. The decentralized, auditable, and transaction-oriented nature of a blockchain approach could make water quality and quantity data 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.[68] Alex Johnson from the Freshwater Trust notes that there is a theme 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."[70

[1] Power Ledger. "Tokenization of renewable energy credits." Powerledger.io. https://www.powerledger.io/project/santa-clara-united-states/
[2] Interview with Duncan McGregor, Power Ledger. January 13, 2020.
[3] Power Ledger. "Tokenization of renewable energy credits."
[4] Power Ledger. "Tokenization of renewable energy credits."
[5] Interview with Duncan McGregor, Power Ledger. January 13, 2020.
[6] Interview with Duncan McGregor, Power Ledger. January 13, 2020.
[7] Ciampoli, Paul. "SMUD official details electric vehicle blockchain project." Publicpower.org. September 27, 2019. https://www.publicpower.org/periodical/article/smud-official-details-electric-vehicle-blockchain-project
[8] Ciampoli, "SMUD official details electric vehicle blockchain project."
[9] Ciampoli, "SMUD official details electric vehicle blockchain project."
[10] Ciampoli, "SMUD official details electric vehicle blockchain project."
[11] Hamill, Julie. "Blockchain Technology: Local Government Applications and Challenges." Icma.org, 11, November, 2018. https://icma.org/sites/default/files/2018-Nov%20Blockchain%20White%20Paper.pdf
[12] Hamill, "Blockchain Technology: Local Government Applications and Challenges."
[13] Hamill, "Blockchain Technology: Local Government Applications and Challenges."
[14] Hamill, "Blockchain Technology: Local Government Applications and Challenges."
[15] Hamill, "Blockchain Technology: Local Government Applications and Challenges."
[16] Hamill, "Blockchain Technology: Local Government Applications and Challenges."
[17] See Brooklyn Microgrid's Change.org petition here. Authors plan to replace this with actual petition in future iterations: https://www.change.org/p/john-b-rhodes-the-nys-public-service-commission-local-renewable-energy-now
[18] Interview with Marzia Zafar, World Energy Council. January 21, 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; Zafar, Marzia. "Blockchain/The emerging of active consumer: Developing A Smarter Network." World Energy, 58, October 2019. https://www.aboutenergy.com/en_IT/flip-tabloid/oil_44_EN/ABO_OilMagazine_44_EN.pdf
[19] Musleh, Ahmed, Gang Yao, S.M. Muyeen. "Blockchain Applications in Smart Grid – Review and Frameworks." IEEE Access, 7. July 17, 2019. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8730307
[20] Interview with Marzia Zafar, World Energy Council. January 21, 2020.
[21] National Institute of Science and Technology. "Smart Grid: A Beginner's Guide." NIST.gov, November 21, 2019. https://www.nist.gov/el/smart-grid/about-smart-grid/smart-grid-beginners-guide
[22] Hamill, "Blockchain Technology: Local Government Applications and Challenges."
[23] Andoni, Merlinda et al. "Blockchain technology in the energy sector: A systematic review of challenges and opportunities." Renewable and Sustainable Energy Reviews, 100: 154, February 2019. https://www.sciencedirect.com/science/article/pii/S1364032118307184
[24] Andoni, "Blockchain technology in the energy sector."

[25] Orcutt, Mike. "How Blockchain Could Give Us a Smarter Energy Grid." Technologyreview.com, October 16, 2017. https://www.technologyreview.com/s/609077/how-blockchain-could-give-us-a-smarter-energy-grid/
[26] Hamill, "Blockchain Technology: Local Government Applications and Challenges."
[28] Hamill, "Blockchain Technology: Local Government Applications and Challenges."
[29] Andoni, "Blockchain technology in the energy sector."
[30] Andoni, "Blockchain technology in the energy sector."
[31] Interview with Marzia Zafar, World Energy Council. January 21, 2020.
[32] Interview with Marzia Zafar, World Energy Council. January 21, 2020.
[33] Interview with Marzia Zafar, World Energy Council. January 21, 2020.
[34] Interview with Tony Giroti, Energy Blockchain Consortium. January 17, 2020.
[35] Hamill, "Blockchain Technology: Local Government Applications and Challenges."
[36] Interview with Amy Ahner, ICMA. January 14, 2020.
[37] Andoni, "Blockchain technology in the energy sector."
[38] Interview with Neil Wasserman, George Washington University. January 13, 2020.
[39] Hamill, "Blockchain Technology: Local Government Applications and Challenges."
[40] Hamill, "Blockchain Technology: Local Government Applications and Challenges."
[41] Interview with Duncan McGregor, Power Ledger. January 14, 2020.
[42] Power Ledger. "Tokenization of renewable energy credits."
[43] Interview with Duncan McGregor, Power Ledger. January 14, 2020.
[44] Zafar, Marzia. "Blockchain/The emerging of active consumer: Developing A Smarter Network." World Energy, October 2019, p. 58. https://www.aboutenergy.com/en_IT/flip-tabloid/oil_44_EN/ABO_OilMagazine_44_EN.pdf
[45] Interview with Duncan McGregor, Power Ledger. January 14, 2020.
[46] Interview with Tony Giroti, Energy Blockchain Consortium. January 17, 2020.
[47] Interview with Amy Ahner, ICMA. January 14, 2020.
[48] Interview with Tony Giroti, Energy Blockchain Consortium. January 17, 2020.
[49] Interview with Amy Ahner, ICMA. January 14, 2020.
[50] Interview with Amy Ahner, ICMA. January 14, 2020.
[52] TATA Consultancy Services. "Blockchain in Natural Resources: Hedging Against Volatile Prices." Tcs.com, March, 2018. https://www.tcs.com/content/dam/tcs/pdf/Industries/energy_resources_and_utilities/Blockchain-in-Natural-Resources-Hedging-Against-Volatile-Prices.pdf
[53] OEHHA. (2019, October 14). *The Human Right to Water in California*. Retrieved from oehha.ca.gov: https://oehha.ca.gov/water/report/human-right-water-california
[54] California Department of Water Resources. (2020). *AB 1755: Open and Transparent Water Data Platform for California*. Retrieved from water.ca.gov: https://water.ca.gov/ab1755
[55] Black, Matt. "How the Blockchain Could Protect California's Aquifer." Wired.com. April 26, 2019. https://www.wired.com/story/how-blockchain-could-protect-californias-aquifer/;
O'Connell, J. (2019, March 12). *Thirsty California May Be Wary of Blockchain Water Rights*. Retrieved from cointelegraph.com: https://cointelegraph.com/news/thirsty-california-may-be-wary-of-blockchain-water-rights

[56] Black, "How the Blockchain Could Protect California's Aquifer."
[57] Black, "How the Blockchain Could Protect California's Aquifer."
[58] Black, "How the Blockchain Could Protect California's Aquifer."
[59] Black, "How the Blockchain Could Protect California's Aquifer."
[60] RCS Global. "Blockchain For Traceability In Minerals And Metals Supply Chains: Opportunities And Challenges." Rcsglobal.com, December, 2017. https://www.rcsglobal.com/wp-content/uploads/2018/09/ICMM-Blockchain-for-Traceability-in-Minerals-and-Metal-Supply-Chains.pdf
[61] RCS Global, "Blockchain For Traceability In Minerals And Metals Supply Chains."
[62] RCS Global, "Blockchain For Traceability In Minerals And Metals Supply Chains."
[63] Marr, Bernard. "How Blockchain Could End the Trade In Blood Diamonds – An Incredible Use Case Everyone Should Read." Forbes.com, March 14, 2018. https://www.forbes.com/sites/bernardmarr/2018/03/14/how-blockchain-could-end-the-trade-in-blood-diamonds-an-incredible-use-case-everyone-should-read/#6c0875e8387d
[64] Marr, "How Blockchain Could End the Trade In Blood Diamonds."
[65] Marr, "How Blockchain Could End the Trade In Blood Diamonds."
[66] Rizzo, Pete. "World's Largest Mining Company to Use Blockchain for Supply Chain." Coindesk.com, September 23, 2016. https://www.coindesk.com/bhp-billiton-blockchain-mining-company-supply-chain
[67] Rizzo, "World's Largest Mining Company to Use Blockchain for Supply Chain."
[68] Stinson, Callie. "How blockchain, AI, and other emerging technologies could end water insecurity." Greenbiz.com, April 2, 2018. https://www.greenbiz.com/article/how-blockchain-ai-and-other-emerging-technologies-could-end-water-insecurity
[69] Black, "How the Blockchain Could Protect California's Aquifer."
[70] Black, "How the Blockchain Could Protect California's Aquifer."

V.F. Finance, Payments and Commercial Business

This section includes analyses of blockchain application in public finance (Muni-Bonds), public banking, digital asset banking, cannabis banking, CalCoin for benefits distribution and public assistance for the unbanked, and remittances.

1. Bonds and Public Finance

Key Recommendations

- **Consult with the following:** Finance department officials at the State, County, and City levels; Municipal advisors already engaged by Municipal debt issuers; and Municipal bond counsels. Perspectives should be collected from *issuers* (both large state and small infrequent issuers), *Investors (*Institutional investors, community banks, registered investment advisors, individual investors and retail); and *Service Providers (*Municipal advisors, bond counsel, underwriters, clearing and settlement agents, custodians, banks).
- **Monitor existing efforts**. For example, the Berkeley Microbond Financing Program, currently at the RFP stage.
- **Create a consortium**. The State of California should research the creation of a consortium to manage the negotiation of the bond issuance fees for the State of California. These universal fees would be implemented via blockchain. [1]
- **Address the challenges for small municipalities**. Municipal finance is about to face its biggest challenge in over a century. The current proposal from the Federal Reserve to expand its plans to buy municipal bonds under emergency powers has limits for counties with fewer than two million people or cities with fewer than one million residents. States may be faced with the need to enable smaller municipalities in order to effectively raise finance. By expressly supporting the adoption of blockchain-based digital municipal bond issuance programs, the State can help address communities' inevitable financial stressors, while supporting enterprise-class adoption of blockchain technology in California.

Introduction – California Perspective

California is the fifth-largest economy of the world and the largest issuer of municipal debt in the country ($60.6 billion in 2019). 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 stated 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.

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, who, 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 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.[2]

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 institutions like international banks leverage these markets to the detriment of other investors. This reality hampers transparency and prevents genuine public oversight.

Borrowers are underserved. For municipal borrowers, the existing mechanisms for accessing capital contain multiple frictions, 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 like state infrastructure. Short-term cash flows are used 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: underwriting costs and costs of issuance. Costs of issuance is 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 each of these costs individually with guidance or set thresholds as what they should be. The municipalities could join and negotiate as a group for better rates. Blockchain can facilitate transparency regarding rates and manage the costs of issuing bonds.[4]

Another important dimension of the municipal market is the cost to issue and trade. In a 2015 report by the Haas Institute, it was 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%.

Muni Loans. The municipal loan market is substantially less transparent. While there is no good data source for municipal loans, studies by Stanford University and the Brookings Institute have shown that use of the instrument has grown substantially since the financial crisis, with estimated outstanding loans of approximately $173.5 billion as of 2016. Furthermore, it is estimated that approximately 12% of outstanding municipal loans, or $21 billion, was represented by California as of year-end 2016.

California can lead a technology update that enables greater transparency in all aspects of municipal loans and bonds, expands investor access, deepens engagement with local financial institutions, improves efficiencies, and lowers cost.

Studies, Pilots and Related Use Cases

The relevant literature on this topic falls into two categories – studies on frictions in the municipal debt markets and blockchain innovation in the financial system. While some news articles investigate the overlap of munis and blockchain technology, we are not aware of any academic literature on the topic.[5]

Minibonds. As the asset class with the least innovation since the 1970s, there have been many attempts to "democratize" the municipal bond with minibond offerings (smaller denominations down to the $100 level), retail offering periods (common in California), geographic limitations and combinations of these. While most of these pilots have demonstrated interest among voters/investors who value access, tax-free returns, and

local impact, the cost of these issuances have come in well above traditional offerings, limiting adoption.

Neighborly. The most notable pilot project related to municipal finance is Neighborly, a high-profile start-up focused on the development of retail bond issuance portals. The business launched in 2012, but ultimately closed in 2019 after failing to secure additional funding. Neighborly's original business strategy was not based on blockchain infrastructure for the municipal market, although their strategy evolved to incorporate blockchain capabilities. The challenges with Neighborly's business strategy were unrelated to blockchain integration itself, but instead were related to two other factors: using retail distribution as the starting point and trying to innovate within constraints in the existing system. The potential for blockchain integration in municipal finance requires that systemwide frictions be addressed.

Jefferson County, Washington. The Brennen 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. [8]

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 technology is valuable because it provides investors with certification upon purchase of assets in real-time, while appropriately recording and reporting the transaction with minimal fees.

IT considerations. The current IT infrastructure is well developed. 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 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 considerations. 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 already well understood and defined in terms of responsibility and procedures. Tokenization will add improved security models to the existing mix.

Trust considerations. 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 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 all the legacy processes at lower costs and higher transparency. California can demonstrate leadership regarding cost transparency on the blockchain.

Cost transparency provides opportunities for cost reduction because it allows issuers to benchmark their expenses against their peers. For example, if we can identify the California school district that paid the lowest rate for bond counsel statewide, that rate can serve as a data point for use by other districts when negotiating the cost of future issuance services. If district staff or board members do not take the initiative to match the prices of low-cost providers, community activists can reference this data when commenting at school board meetings or support alternative board candidates more willing to pursue savings.

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[9]). 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. As a side benefit, a tokenized bond issuance allows the State to 1) achieve greater transparency; 2) execute targeted investments; and 3) serve public policy goals of financial inclusion by making bonds affordable.

Blockchain token architecture offers an excellent platform for payment systems as well as new types of financial instruments currently emerging from the Distributed Finance (or DeFi) community. Blockchain and Distributed Ledger Technology offer the potential to save issuing costs, lower the price of bonds, and increase transparency and speed.

Blockchain allows assets to be exchanged or fractionalized while adhering to market regulations. Tokens allow for quicker proof of ownership and demonstration of liquidity that will reduce market frictions. Operational costs will be significantly reduced. Blockchain will streamline settlement and clearing functions while offering community banks more opportunities and trades to fit individualized investment strategies. Eventually, blockchain will allow retail investors an opportunity to access the primary bond market.

Access. 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.

Consistency: The process will underpin moves toward contract standardization with blockchain-enabled smart contracts.

Transparency: Blockchain technology provides issuers, regulators, and investors with direct access to relevant data via blockchain nodes.

Reconciliation: Through time, blockchain eliminates the need for reconciliation of holdings and cashflows via use of blockchain nodes.

Reduce cost. Blockchain lowers overall costs for government issuers by reducing costs of underwriting, distribution, contract complexity, reconciliation and transparency.

Local empowerment. Residents gain an opportunity to invest locally through blockchain mechanisms.

Blockchain Implementation: Potential Barriers and Concerns

Digital Identity. Digital identity is critical at all levels of participation in the scheme. The device identity model should be implemented strictly to ensure that users can be authenticated at every level.

Identity is extremely important within the blockchain environment. In the future, all individuals will have a personal identity token that offers them control over who has access to their identity and when. Identity also supports regulations such as Know Your Customer/Anti-Money Laundering (KYC/AML). Use of multiple blockchain platforms to pass identity tokens will be important but, for now, token identity can be managed at a local blockchain 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 of 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). For transfers involving only a transfer agent (i.e., sale from municipality to investor, conversion to tokenized or DTC status, and final redemption) these will follow the SEC rules governing Transfer Agent activities.

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

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

- **Technology considerations**. There is no one-size-fits-all blockchain solution. Today, blockchain platforms 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. Capitalizing on blockchain technology could result in many efficiencies and cost savings.
- **Potential effects**. It is important to understand and consider potential effects such as liquidity, an important dynamic in a well-functioning muni market. 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.

2. Public Banking

Key recommendations

- **Engagement**. When the first public bank prospect is identified, all interested parties should be invited to submit public comments.
- **Blockchain technology integration**. As California implements its new public banking law, opportunities will abound to integrate blockchain technology into the underlying regulations, particularly as a means to achieve transparency requirements of the California Public Records Act (CPRA). Therefore, the State of California should monitor developments in public banking.
- **Pilot with Community Development Finance (CDF)**. CDF is excited to discuss partnership with public banks. CDF aspires to scale its operations in order to reach more vulnerable California residents; process automation and online service platforms can both be expected to help them achieve this goal.

Introduction – California Perspective

The Public Banking Act AB 857[10] 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. 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 banks are inclined to provide loans for public projects such as infrastructure and affordable housing.

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.

Generally, public banks lend in a countercyclical fashion to private banks, providing credit when private banks will not. For example, 7.4% of Californian households are unbanked, and 17.6% are underbanked. California's unbanked rate is one of the

highest in the United States. These unbanked and underbanked residents are predominantly low-income people who have so few financial assets that private banks lack incentive to serve them. Their cumulative aggregate assets, however, are substantial and banking these assets may contribute to a reduction in poverty. Further, these low-income residents are commonly subjected to interest rates reaching 36% by in-state lenders, and even higher if the lender has partners out-of-state. [4]

Pilot and Use Cases

Attempts to establish public banks abound; nearly two dozen other states have also tried, unsuccessfully, to enact them, including four in 2019. Critics of public banks (such as CA Bankers Assoc. and Valley Industry & Commerce Assoc.) say it sets the stage for corruption, self-dealing, and government inefficiency, making them undesirable and unnecessary. Still, proponents argue that proper organizational structuring protects against corruption, namely: operation by professional bankers combined with an independent board of directors. Proponents also note that some of the most competitive economies have strong public banking sectors, including Taiwan and Germany.

North Dakota. The Bank of North Dakota ("BND") is currently the last surviving state-run, and state-owned American bank. The bank has an operating income of $158M and $7B in assets. Formed in 1919 to protect farmers from usurious interest rates, the Bank of North Dakota's mission has grown to support various interests in the agricultural, commercial, and industrial sectors in North Dakota. BND primarily serves the state's financial institutions and public agencies. The bank also works with individual residents to meet underserved needs, such as disaster relief, low income rural mortgages, student loans, and small business development.[5]

Proponents of public banks in California point to North Dakota as evidence of the efficacy of public banks, citing that North Dakota has six times as many financial institutions per capita as the rest of the country. In times of recession, the Bank of North Dakota has been able to step in and provide loans to stimulate the economy.

Considerations and opportunities for blockchain application

Security and privacy. Public banks are subject to the California Public Records Act (CPRA), which requires that public records be available to the public for inspection and made promptly available to any person. Presumably, they must also maintain the same level of security and privacy for financial documents and data as that which private banks must maintain.

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 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.

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 seem to be any statutory or regulatory barriers; a CA public bank's implementation of blockchain technology could readily achieve compliance with all existing statutes and regulations.

Blockchain Implementation Potential Barriers and Concerns

IT Considerations. These are all yet to be developed with the first public banks in California.

Digital Identity. Digital identity will be integral to properly securing users' financial records.

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.

3. Digital Asset Banks: Special Purpose Depository Institution

Key Recommendations

- **Regulatory reforms**. California would benefit from enacting regulatory reform to become an attractive destination for innovators and investors. Defining a framework for Special Purpose Depository Institutions (SPDI), and subsequently granting existing banks a charter to bank Digital Assets would enable greater monetization and overall growth of these new technologies. California should endeavor to lower the bar of entry to smaller companies who are still able to meet Anti-Money Laundering and other requirements.
- **Create a Charter**. California can derive significant economic growth by creating a charter for Digital Asset Banks.
- **California Digital Asset Banks offering should**:
    - Offer compliant banking services for the blockchain business community
    - Promote structured investment in digital asset products
    - Promote market adoption of blockchain technology solutions
    - Increase revenue generation to aid economic recovery

Introduction – California Perspective

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. 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 custody themselves rather than in an institution due to lack of availability. More broadly, a study by Gartner[11] stated that blockchain technology will create more than $176 billion dollars of business value by 2025 and $3.1 trillion by 2030.

While by no means all blockchain businesses depend on digital assets, many do to one degree or another. It should also be noted that 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 has a large number of 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.

Under FDIC rules, traditional banks are not permitted to custody digital assets. Trusts can take custody, but they are not allowed to receive Federal Reserve payments. This

appears to conflict with other federal rules which permit banks to have custody of digital securities, provided they demonstrate adequate customer protections, and exclusive control of the assets in the event of bank failure[12]. [6]

Many California-based digital asset businesses might benefit from a California 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 of the most successful 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.

Pilot and Related Use Cases

Kraken. Kraken, the San Francisco–based cryptocurrency exchange, has announced plans to establish a Wyoming SPDI[16]. Kraken is the eighth-largest cryptocurrency exchange in the world and routinely reports daily trading volume above $100m (April 2020), and is valued at more than $4 billion.

Other businesses are also experiencing banking problems related to digital assets that might benefit from a Digital Asset Banking Charter. The lack of regulatory clarity and prevention of institutional control of digital assets has contributed to the loss of California-based blockchain businesses and entrepreneurs.

Considerations and opportunities for Blockchain Application

Permission considerations. A key question is whether to utilize proprietary or open source blockchain-based software, whether the provider is willing to use a vault service. 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 that use case. Another critical question is whether blockchain technology is really the best software for a given use case. A common misconception is that blockchain technology is always better than well-established database software such as Apache Tools or a distributed software such as Node.js. In terms of holding digital assets in an SPDI, this is not a direct consideration as these concerns will be left to the investor, not the banking institution.

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 utilized for financial information, and indeed it is particularly important that any evolution in digital currencies not be tied to excessive disclosure of personal information.

IT considerations. Blockchain technology was established long before digital assets such as Bitcoin and Ethereum, and development of digital assets has evolved for more than a decade. These technologies now exist at an enterprise-class level and many have been adopted by mainstream companies. JPMorgan's Quorum[17], EY's Nightfall[18], Microsoft's Azure[19] are three examples and Ethereum's blockchain technology and ConsenSys's enterprise-class collaboration have been fundamental to all three. A unique aspect of Ethereum is that there are approximately 300,000 active Ethereum developers, which is at least 30 times larger than the nearest blockchain developer community by size. IBM's Hyperledger Fabric[20] is an alternative permissioned enterprise-class blockchain but with a relatively smaller developer community of about 400 people. Notably, although certain technologies such as "hardware wallets" can be used in conjunction with digital assets, no additional hardware or physical infrastructure is required to develop, use, transact, or invest with digital assets.

Security and Privacy. A broad body of legislation regulates the way financial institutions handle the non-public financial information of consumers. In the United States, financial privacy is regulated through laws enacted at the federal and state level. Federal regulations are primarily represented by the Bank Secrecy Act, Right to Financial Privacy Act, the Gramm-Leach-Bliley Act (GBLA), and the Fair Credit Reporting Act. Provisions within other laws like the Credit and Debit Card Receipt Clarification Act of 2007 as well as the Electronic Funds Transfer Act also contribute to financial privacy in the United States. State regulations vary from state to state. California Financial Information Privacy Act (CalFIPA) was enacted in 2003 to require financial institutions to provide California consumers notice and meaningful choice about how consumers' nonpublic personal information is shared and to offer greater protection than its federal counterpart the GLBA. As the SDPI's proposed here would effectively govern digital assets held as currency, as currency, there should be no regulatory conflict.

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.[21]

Trust considerations. In terms of trust, 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 deeply familiar with the technology itself. There is no appreciable impact on intermediation.

Cannabis Banking

Key Recommendations

- **Blockchain fintech benefits**. The state-licensed cannabis industry would benefit from blockchain fintech innovations and statutory changes being advocated by non-cannabis stakeholders including public banks, digital asset deposit and/or custodial institutions, and blockchain and cannabis entrepreneurs advocating for a regulatory sandbox.
- **Improve safety and efficiencies**. California should empower entrepreneurs to create technological and legal solutions to improve the safety and efficiencies of payment and settlement of legal cannabis product transactions.

Introduction – California Context

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 the Bureau 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 (up 59% from the previous years' quarter) 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.

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.

The most urgent need in the cannabis industry is access to banking and financial services. There is a pressing public goal and industry push to reduce the use of physical cash by the cannabis businesses and consumers for the payment of taxes and transactions. 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 have many similarities and seem to have many synergies:

1. Payments and lending limitations for cannabis consumer and business financial transactions need improvements
2. An abundance of data on cannabis transactions and production is collected and stored but is seldom analyzed or used to improve or verify processes
3. Federal solutions for new and popular business models are not forthcoming, so 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 consumer 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 our labor, consumer goods and commodities markets places our state economy in the top echelons of global markets. Blockchain fintech enterprises are starting up in California and will thrive in our vibrant marketplace and society. This is similar to our burgeoning state-licensed commercial cannabis industry.

In the specific subject of cannabis and banking, 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. 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 inherently 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 be compliant 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. [9]

Pilots and Related case studies

According to industry insiders, 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. Given that the industry is not yet federally legal, academic literature does not exist and only one locally sponsored pilot exists. [10]

Digital Asset Cannabis Purchase and Tax Payment, City of Emeryville. On September 11, 2019, in Emeryville, CA, Ohana Dispensary hosted the first compliant digital asset purchase of cannabis products. A dollar-backed stable coin was used to purchase cannabis. The purchaser identification, receipt, and tax payments, were instantly stored, and transmitted to the relevant agencies *at the moment of transaction*.[22]

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.

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 carry public health and public safety risks. For these reasons alone the state should remedy these risks with whatever assistance is lawfully available. 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.

From a consumer safety and biosecurity perspective, the cannabis products within the regulated supply chain in California is ensured by batch testing for contaminants, microbials, heavy metals and other adulterants to a far higher standard than regulated industries in other states and inherently better than the complete lack of testing in the still thriving illicit cannabis marketplace.

Security and privacy. Medicinal cannabis operators transmit or store Protected Health Information relating to their consumers and are generally comfortable with Health Insurance Portability and Accountability Act (HIPAA) compliance. It is worth noting medical cannabis sales have sharply declined since the onset of legalized adult use, and attendant HIPPA issues decline as well.

From a consumer privacy standpoint, the shift of consumers from a medical purchasing framework to a more "recreational" framework may seem at first to be a step backward for consumer rights. However, the transition from medical cannabis patient to adult cannabis consumer is backstopped by the new California Consumer Privacy Act in place of HIPAA.

From a different consumer privacy standpoint, however, medical patients who let their doctor recommendations lapse increase their privacy from the federal government. In

several instances medical cannabis patients have had their federal rights restricted, from gun ownership rights to unfettered air travel.

Security standards in the licensed cannabis industry are generally higher than non-cannabis businesses. This is due to the regulatory requirements related to the physical security conditions required to store or transport large amounts of cash and/or valuable cannabis product inventories. Also, operators often have advanced software and hardware infrastructure in order to comply with cannabis track-and-trace regulations. Cannabis companies have the human and cultural infrastructure of external audits from insurers, and bankers, and local law enforcement security reviews.

IT considerations. Relative to other retail, manufacturing, distribution and agriculture industries, the licensed cannabis industry has several unique factors to consider. First, the cannabis industry must track, and trace all amounts of cannabis and even waste products throughout the supply chain. This is standardized through a reporting framework of plant and product tags known as METRC (marijuana enforcement tracking reporting compliance). To account for product movement and alteration throughout the supply chain, employees of licensees log plants, batch, and sale activities with handheld barcode scanners using a variety of third-party, METRC-integrated software platforms. Most of this hardware and software infrastructure has developed quite recently, making the cannabis industry "digitally native" and free of the legacy vendor and systems lock-in of other industries.

Furthermore, as one would expect from an industry that has managed to stay operating and thrive despite contravening federal law, there is a high degree of ingenuity and openness towards innovation within the cannabis industry. Staff is generally younger and more highly paid than in other industries, and hardware is often robust by virtue of regulatory requirements.

Cannabis cultivation operations are often located in rural areas with minimal staffing, sparse technological infrastructure, and limited network reception. While this may seem a hindrance, the relatively slow pace of cultivation operations does not require as much infrastructure to collect and track data. Cannabis cultivators require less infrastructure than a busy retail storefront open 16 hours a day in an urban environment with sales, inventory, and security events to track. What the various segments of the cannabis industry share is the need to invest in their business and challenges in doing so when banking and credit are not allowed.

Cannabis businesses typically lack access to equipment leasing and financing, and their attorneys and vendors can face losing their bank accounts. These companies waste much of their time counting, storing, and protecting cash.

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 government by reducing the need for intermediaries. The regulations of the cannabis (and possibly soon hemp) supply chains in California and many other states require 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 like processes and roles within any 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.

In California, cannabis companies are regulated under the Medical Marijuana Regulation and Safety Act of 2015, which requires compliance with the Department of Consumer Affairs, Department of Food and Agriculture, and Department of Public Health. Licensed commercial cannabis businesses in California also interact with other state and local agencies, from local land use approval to water and CEQA compliance to collection and transmission of a variety of taxes and fees.

The Bureau of Cannabis Control, CalCannabis and the Office of Manufactured Cannabis Safety (under their respective DCA, DFA and DPH departments) are responsible for authorizing and continually regulating commercial cannabis enterprises. This includes criminal background checks of owners and financially interested persons, and reviews of incorporation documents of applicant entities, business contracts or leases, standard operating procedures, packaging and labeling on products, ongoing commercial transactions, and taxes collected and remitted.

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 California cannabis businesses would have greater confidence in their businesses.

Integration with other blockchain applications. The cannabis industry's emergent digital ledger innovations are primarily concerned with the tracking and tracing of 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.

Innovation Sandbox. Lastly, California could foster an "Innovation Sandbox" for blockchain and cannabis fintech, with protections for developers, could markedly add to the economic development of the state and would encourage and enable innovative and compelling new use cases beyond those imagined here.

Blockchain Implementation Potential Barriers and Concerns

Digital identity. Personal identity is implicated in multiple ways in the cannabis ecosystem, and sometimes in a negative sense when balanced against the interests of public safety as embedded in the current statutes. When drafting a state regulatory framework for commercial cannabis during the Obama era, the Cole Memo guidelines issued by the US Department of Justice outlined various factors which would require the local US Attorneys to intervene in state-licensed cannabis operations. Among these requirements were establishing and implementing systems to restrict the participation of organized crime and certain felons as owners, operators or even employees of state-licensed activities, establishing systems to restrict cannabis sales to non-adults or non-patients through checking of government-issued identification and restriction against large purchases of cannabis being made for diversion to the illicit or out-of-state markets.

At the retail level, personally identifiable information is therefore collected and retained for at least a 24-hour period to prevent customers from "looping" back for multiple transactions in the same day. This mandated storage of personal identifiable information by cannabis licensees is not optimal and will likely soon be tested, through the inevitable leak of sensitive information or an action taken under the California Consumer Privacy Act. Beyond the retail storefront collection of identification information through physical artifacts, innumerable digital identities are implicated just as they would be for non-cannabis businesses, from interaction with social media accounts, conducting of email and text marketing campaigns, membership and frequent-shopper incentives programs, online menu preferences, previous order histories, personal contact information, and delivery addresses, and debit/credit account information.

Privacy considerations. In the realm of privacy and confidentiality whatever implementations of blockchain fintech and other digital ledger technologies that provide services to and for the commercial cannabis industry must incorporate consumer privacy, the need for medical privacy, the inherent threat of cybersecurity and physical attacks on now-essential supply chains, public safety through reducing the illicit cannabis marketplace, and the private sector value of secure trade secrets and enforceable IP marks on goods, especially value added goods.

Statutory and regulatory considerations. The greatest statutory and regulatory barrier to greater collaboration between state licensed cannabis businesses and fintech and traditional financial actors is the ongoing consequences of marijuana being scheduled as a Controlled Substance. While either a rescheduling from Schedule 1 to Schedule 3 or a complete descheduling of cannabis (as occurred for hemp in the 2018 Farm Bill) would achieve these ends, Congress has proposed both omnibus and proposals narrowly tailored to address cannabis banking. The SAFE act was passed last spring by over two-thirds of the House of Representatives and presently has 46 California cosponsors. As it moves through the Senate process, either by passage of the existing vehicle or through incorporation into a continuing funding or COVID relief measures, it is imperative that Senators help address this public safety and public health matter.

In relation to cannabis and blockchain fintech at the California legislature, last year Assemblymember Ting proposed the use of "stablecoins" by retail cannabis consumers and by those licensees for settling of transactions as well as efficient, transparent and rapid collection and transmittal of local cannabis taxes via a digital currency framework. This proposal has been reintroduced as Assembly Bill 3090 however this legislative session is understood to be highly abbreviated and may only consider topics germane to disaster response, small business relief or economic recovery. Blockchain fintech solutions for the state-licensed cannabis industry could fall into the last two categories although capacity for considering such legislation is limited this year.

IT Considerations. Major conditions that do not make the cannabis industry favorable for adoption of blockchain fintech solutions relate to rural internet access and access to commercial lending services.

Engagement and buy in. Various elements of the state of California have been actively drafting cannabis industry policy for the last five years, with significant participation from public and private stakeholders. The various statewide and local cannabis industry trade associations have been a consistent voice, as have local government and state agencies.

State and local leaders have been engaged with cannabis policy reform via such groups as the League of Cities, the California State Association of Counties and Rural Counties Representatives of California. Their respective committees and representatives, when reviewing other Blockchain Working Group's recommendations, should be made aware of the blockchain's potential benefits for public health, public safety, and local economic development.

Additionally, establishing institutional buy-in and soliciting subject matter expertise from agencies such as the California Tax and Fee Administration and the California Association of Treasurers and Tax Collectors would be beneficial. Policymakers should also draw from the wider private blockchain fintech sector and various stakeholders

from other jurisdictions, particularly those with cannabis industries and/or fintech sandboxes.

CalCoin - Blockchain Enabled Benefits Distribution and Public Assistance for the Unbanked[11]

Key Recommendations

- **Blockchain application**. California should utilize blockchain technology to create a public payment and benefits distribution system for its struggling families.
    - A CalCoin digital benefits distribution system can present great value to the State of California. California could begin by conducting a digital cash and voucher assistance ("CVA") pilot project, to meet the increased needs of low-income families in emergency conditions, and then scale this digital CVA program over time in order to integrate with existing programs. Such a program calls for a proper RFP (request for proposal) process, complete with due diligence and foresight in the program's architectural design.
    - In order to accommodate regulations, CalCoin's use should be restricted to the purchase of pre-approved products and services with, initially, a limited set of partner vendors. Such restrictions could be gradually lifted over time as new use cases present themselves. It may also be of mutual benefit to partner with nonprofits that serve similar populations as those that currently use assistance programming, especially in early stages of the program.
- **CalCoin Working Group**. The State of California should impanel a working group to explore implementation of CalCoin and related programs. [12]

Introduction – California Perspective

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. As the government registers this record number of unemployment claims, the actual unemployment figure may exceed 20%.

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.[23] The package includes a one-time rebate of $1,2000 for individuals who earn up to $75,000 a year and $2,400 for couples who earn up to $150,000. Unfortunately, many Americans still await this direct deposit's arrival, weeks after the CARES Act's enactment.

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.

Even where conventional software systems handle these requests, the underlying financial infrastructure to disseminate the aid — ACH transfers — is still quite 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 (based on 128.58 million families and 110.6 million single adults potentially eligible for disbursements). Once the aid is received, additional money is deducted from actual aid on the transaction fees for credit and debit card processing. Under the present system, a significant portion of stimulus aid is lost to a slower, more expensive, and fundamentally unstable financial infrastructure.

The COVID-19 pandemic has unveiled the imminent need for a free, digital, and publicly accessible payment network to disburse aid with adequate efficiency and transparency by avoiding the cost and privacy issues of commercial payment platforms. The CARES Act had originally included a "digital dollar," a digital payment system designed to speed relief payments to families in distress[24] but this provision was removed before the bill's enactment. Several current proposals in Congress are recognizing the urgent need to enact far-reaching technological changes in order to deliver economic stimulus to Americans more effectively.

The potential benefit of instantaneous 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.

Pilot and Related Use Cases

While there have yet to be many notable digital VCA use cases for government aid, many 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.

United Nations, World Food Program. The United Nations World Food Program [25]recently used a blockchain platform to deliver aid. The UN completed its first successful trial when it transferred cryptocurrency-based food vouchers to 10,000 refugees in Pakistan. The trial was so successful that the UN plans to expand the program to 500,000 Syrian refugees in Jordan.

Alice. Alice, founded in April 2016, is a social funding and impact management platform built on the Ethereum blockchain. The organization incentivizes social organizations (charities, NGOs, social enterprises) to run projects transparently, by implementing computerized contracts to ensure their payment *only upon achieving their goals*. The performance of each project is publicly available, which makes it easier for funders (philanthropic organizations, impact investors, small donors) to identify and help scale social projects that work. The social enterprise is attending to the pressing issues of donation transparency and nonprofit funding.

Binance Charity Foundation. Blockchain Charity Foundation (BCF) is a not-for-profit organization dedicated to the advancement of blockchain-enabled philanthropy in order to achieve global sustainable development. BCF aims to transform philanthropy by developing the world's first decentralized charity foundation by using blockchain technology, in order to end all forms of poverty and inequality, advance sustainable development, and ensure that no human remains impoverished. The cryptocurrency exchange Binance created the foundation.

Sempo. Sempo is an end-to-end platform to deploy assistance payments to impoverished people in remote locations. Sempo performs beneficiary identification, cash disbursement, and automated program monitoring. Merchant partners can transact cash disbursements via SMS, physical payment cards, or Android app. The platform is multilingual, user-friendly, and inclusive of all literacy levels. Sempo has been tested on over 8,000 beneficiaries in several countries spanning three continents, in partnership with organizations such as the Red Cross, and Oxfam International.[13]

Considerations and opportunities for Blockchain Application

Efficiency, transparency, and cost savings. Digital assets like the CalCoin are programmable; therefore, they enable tighter controls on how residents spend funds by enabling the following features: (a) seamless prevention of cross-state transactions, and (b) vendor approval and verification requirements for certain services and products, enabling adequate control of both in-state and out-of-state expenditures. Programmable digital asset implementations would also provide substantially better

access to funds for those who remain unbanked to avoid banking fees because digital funds can be conveyed without a bank account.

Promoting equity. In addition to being scalable across jurisdictions, housing vouchers on the blockchain can seamlessly integrate adjustments to regularly fluctuating economic indexes — namely, the consumer price index (CPI), national median monthly income, as well as others from the stock and housing markets. As such, digitizing public benefit programs have the potential to be economically responsive while automating social services transactions across the country.

Accountability. The programmability of digital money systems makes integrating accountability assurances feasible. The government assistance agency can easily audit transactions and detect anomalies in real time under a digital money system. Such practices would significantly decrease the damages of fraud as well as the cost to police it. Digital money enables radical transparency of public spending.

Distributed ledger technology enables the two parties to a single transaction to verify each other. This eliminates the inefficiencies of third-party verification, human bias, and fraud. Seamless transactions and further cost savings are due to automated programmatic controls.

Tokenized CalCoin digital vouchers and benefits are held in online accounts (wallets) that are controlled by the holder. From here, the benefit recipient can transfer ("spend") these instruments to approved vendors for consumption or cash. The blockchain will record each of these movements, for every token from the time it is created. All transactions will be viewable, securely and in real-time, by approved government auditors.

Token-based vouchers. Creators of value distribution systems often grapple with the dilemma of whether programs should be token-based or account-based. In a token-based system, the instrument of value is created as a token with a specific denomination. The transfer of a token from one party to another does not require reconciling two databases and is instantaneous.

In an account-based system, the bank or central body holds accounts for users and, therefore, manages the debit and credits directly. Having to hold accounts for all users of the currency entails a high volume of accounts to be managed.

A tokenized model is recommended on several grounds. First, it enables new complex delivery models with minimal friction and expense because money does not change hands until final settlement. Second, it frees the state from the expensive duties of large-scale account management.

Private permissioned blockchain. The CalCoin should be hosted on a private permissioned blockchain, which would allow state agencies to administer the digital

benefits to the intermediaries and end users. Agencies may, therefore, still act as wardens of the ecosystem *but are free of the duty to provide management services*.

Interoperability. The digital voucher and distribution model should be interoperable with other blockchain platforms and databases to allow for rapid iteration of innovations.

Transparency. Govt. Finance Depts. may Benefit from Transparency, Cost Reduction, and Smart Accounting. The Department of Health and Human Services Department would be able to deliver aid to more people due to the efficiencies and cost savings — all at speeds which are exponentially faster than the traditional disbursement process. Also, accounting overall for California's public benefits programming can become automated and therefore more easily auditable and fraud resilient.

IT Considerations. Currently, private blockchain enterprise infrastructure can handle the tens of thousands of transactions per second that are needed to sustain California's leveraging welfare programming and cash aid services. Consumer interfaces (i.e., "digital dollar wallets") already exist and may also be further iterated upon to provide a more intuitive user experience for program beneficiaries.

Blockchain token architecture offers an excellent platform for payment systems as well as new types of financial instruments which are currently rolling out of the Distributed Finance (or DeFi) community.

Blockchain system technical requirements should include the following:

- ***Real-Time Asset Transfer at Negligible Cost.*** Transaction times will be fast, with transfers occurring at or near real-time, at a price below one-tenth of a cent (<0.1 EUR) per transaction.
- ***High Transaction Throughput***. The system can offer several thousand*, or several tens of thousands,* of transactions per second on the network.
- ***Large Number of Network Participants.*** The system can support vast participant networks.
- ***Robust Privacy of Consumer Data and Transactions***. In our view, central bank State agencies should have only a limited view of their beneficiary's transaction activities and associated ID's. Blockchain technology makes implementing such privacy controls seamless.
- ***Confidentiality of Business Data.*** The program should also support the confidentiality of critical business data of intermediaries on the network. While the state would retain a view of all large transactions, individual network participants would not be able to see sensitive information such as the volumes or individual transactions of their competitors.
- ***Compliance With KYC/AML And Related Regulations.*** The program can support the implementation of KYC/AML and related regulations by providing

traceability and monitoring capabilities to the relevant authorities above reasonable thresholds.

- ***Asset Recovery***. The system must permit the reversing of transactions under legally acceptable conditions, including the recovery of lost or misplaced funds.
- ***Minimal Environmental Impact.*** The system will be able to run at acceptable energy usage levels so as not to have a negative environmental impact. (Energy consumption concerns had been a product of cryptocurrency "mining" operations, which are unnecessary to, and therefore would not occur on, CalCoin.)

Immutability. The CalCoin blockchain can provide truly *immutable* records keeping. Due to the fundamental nature of blockchain technology, records (transactions, transfers, modifications, etc.) *cannot be modified* after they are created because they are constantly re-verified by every subsequent record. This eliminates the potential for any individual to manipulate, replace, delete, or falsify any data stored on the CalCoin network

Fraud. Through its assistance programs, California's state and county governments must process millions of dollars to millions of individual accounts every month. Some of the main challenges to the efficacy of these programs are to properly understand beneficiary spending habits and to proactively prevent fraud.[28]

Fraud Auditing. Another present issue of social service agencies concerns the government's need to monitor their accountability. Attempting to screen for fraud and spending discrepancies, the government sample-tests social service programs in various jurisdictions. These tests are quite costly and rely on random sampling due to limited funding allocations. Moreover, the commingled governance of bureaucratic organizations, i.e. housing voucher absorption (discussed above), makes transparent accounting infeasible.

Blockchain Implementation: Potential Barriers and Concerns

Legal Considerations. As a new approach to money, CalCoin may well require adjustments to regulations on its new properties. CalCoin will raise some novel legal questions as well. For example: in contrast to physical cash, CalCoin may restrict outsiders from using it. Policy makers will be drawn to explore optimal usage of such new capabilities, in anticipation of any issues which may arise.

Governance. Another crucial issue is 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 both the technical and design levels. Lack of clear ownership would raise many difficult

legal and regulatory questions, namely for the assignment of liability. This concern calls for a controlled and regulated infrastructure which totes clear governance structures for system design, development, maintenance, funding, upgrades, etc.

Security and Privacy. Security and Privacy is of utmost importance when dealing with benefits recipients' identities, medical benefits, and banking, and other sensitive information. Fortunately, it will be technically attainable to fine-tune CalCoin's privacy features with various mixes of anonymity versus traceability of transactions. Program implementation can ascribe to the highest privacy standards.

"Smart contracts," which are used to automate payments and carry out programmed functions, are helpful and need only to be vigorously audited, namely by third-party experts, to avoid exploits with due diligence.

Investment. The retraining and adoption phase will, like all changes, take time and money to properly execute. An exceptional user experience needs to be implemented on all government applications which aid beneficiaries use to receive and transfer CalCoin benefits.

Digital identity. The role of identity, at least initially, should not depart too far from what is expected by the average consumer. CalCoin should have standardized identifiers and identity mechanisms to simplify and reduce the cost of compliance and usage while improving the platform's effectiveness.

The CalCoin benefits distribution program is targeted at serving the unbanked. For this population, mobile-based digital Identity verification will be a highly viable access method. Accordingly, the program can ascribe to the best standards of levels of mobile cybersecurity, and encryption.

Lost or stolen tokenized aid is possible but can be easily circumvented by (1) using login credentials to access beneficiary funds, (2) automatically monitoring abnormal spending activity, and (3) reverting transfers or deleting funds that are known to be stolen. Each of these solutions are readily attainable on a professionally designed blockchain system.

Remittances

Key Recommendation

Government role. Since California has one of the largest remittance flows among U.S. states, state residents could hugely benefit from new, blockchain-based technologies that reduce the cost and improve the speed of transactions. However, since most of these technologies are built by private companies and used by private citizens, the state government has a limited role in the remittance market.

There has been considerable innovation in utilizing blockchain technologies 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.

Endnotes and References

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

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

[3]

[4] Joffe, Marc. "Doubly Bound: The Cost of Issuing Bonds." Berkeley, CA: Haas Institute for a Fair and Inclusive Society, University of California, Berkeley, 2015.

[5] Stanford University Report "Private Placement of Municipal Debt: Lessons from California's Mandatory Disclosure Rule"
https://publicpolicy.stanford.edu/sites/g/files/sbiybj9416/f/publications/commercia_final_report.07152017_0.pdf
Brookings Institute Report, "The Privatization of Municipal Debt"
https://www.brookings.edu/wp-content/uploads/2018/08/WP45.pdf
Haas Institute Report "Doubly Bound: The Costs of Issuing Municipal Bonds"
https://haasinstitute.berkeley.edu/sites/default/files/haasinstituterefundamerica_doublybound_cost_of_issuingbonds_publish.pdf
Pedvis, Andrew Bond Buyer 'Blockchain: Are Munis Next?"
https://www.bondbuyer.com/opinion/if-muni-bonds-could-talk
Leising, Matthew and Monks. Matthew "Paxos Gets SEC Nod to Use Blockchain to Settle Stock Trades" https://www.bloomberg.com/news/articles/2019-10-28/paxos-gets-sec-nod-to-use-blockchain-to-settle-stock-trades
ASX Replaces Chess Settlement Tool with Distributed Ledger Technology
https://www.asx.com.au/services/chess-replacement.htm

[6] Bank of China press release 12/04/2019
https://www.boc.cn/aboutboc/bi1/201912/t20191204_17232943.html

[7] Society Generale press release "Societe Generale issued the first covered bond as a security token on a public blockchain". https://www.societegenerale.com/en/newsroom/first-covered-bond-as-a-security-token-on-a-public-blockchain

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

[9] Joffe, Marc. "Doubly Bound: The Cost of Issuing Bonds." Berkeley, CA: Haas Institute for a Fair and Inclusive Society, University of California, Berkeley, 2015.

[10] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB857

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

[12] United States Securities and Exchange Commission July8, 2020 "Joint Staff Statement on Broker -Dealer Custody of Digital Asset Securities" https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities

[13] Wyoming Division of Banking, "Special Purpose Depository Institutions" http://wyomingbankingdivision.wyo.gov/home/areas-of-regulation/laws-and-regulation/special-purpose-depository-institution

[14] CoinDesk, "What it takes to get a crypto-friendly bank charter in Wyoming" https://www.coindesk.com/what-it-takes-to-get-a-crypto-friendly-bank-charter-in-wyoming

[15] Linkedin, Kraken jobs https://www.linkedin.com/jobs/kraken-digital-asset-exchange-jobs/

[16] Wired, "The newest haven for Cryptocurrency companies? Wyoming" https://www.wired.com/story/newest-haven-cryptocurrency-companies-wyoming/

[17] Quorum, https://www.goquorum.com/

[18] EY Nightfall, https://github.com/EYBlockchain/nightfall

[19] Microsoft Azure, https://azure.microsoft.com/en-us/

[20] IBM Hyperledger Protocol, https://www.ibm.com/blockchain/hyperledger

[21] Kraken, "Operations Director, Special Purpose Depository Institution" https://jobs.lever.co/kraken/f50b262d-9966-4083-8843-50e930e72df5

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

[23] https://www.congress.gov/116/bills/hr748/BILLS-116hr748enr.pdf

[24] https://www.forbes.com/sites/lawrencewintermeyer/2020/03/30/covid-19-economic-stimulus-get-money-to-people-faster-with-digital-dollars/#65c33b6f31fc

[25] "Building Blocks, Blockchain for Zero Hunger" https://innovation.wfp.org/project/building-blocks

[26] 'Plimmer, Gill "Use of bitcoin tech to pay UK benefits sparks privacy concerns" https://www.ft.com/content/33d5b3fc-4767-11e6-b387-64ab0a67014c

[27] Nikolova, Maria "UK sees use of blockchain as nonviable for welfare and benefits system" https://financefeeds.com/uk-sees-use-blockchain-nonviable-welfare-benefits-system/

[28] https://abc7news.com/archive/7704795/

V.G. Justice and Civic Participation

This section provides analyses for blockchain application for the Secretary of State's State Archives, The Secretary of State's Business Programs, and internet voting.

Key Recommendations:

State Archives: The Secretary of State's State Archives would be an effective first blockchain pilot project. The California legislature should work with the Secretary of State leadership to determine how best to move the state's archives online with blockchain technology. This agency is excited to further explore blockchain applications and has been successful with most previous technology pilots. This use case provides for a relatively low-risk pilot project with great potential benefits.

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.

Internet Voting Pilot: Security experts generally agree that internet-based implementations of voting systems, blockchain or not, have not overcome the inherent challenges in implementing an online voting system, particularly security challenges. California should consider small-scale or low-stakes pilots, especially those designed to

enable more people to vote, to provide transparency regarding the pros and cons of internet voting, to advance the state of voting technology, and to leverage the unique resources of California's universities, nonprofits, and technology companies.

- **Technology considerations**: 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 their 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 Secretary of State

The California Secretary of State provides services in four major areas: political reform division (campaign finance); elections (including voter registration); business programs; and archives. Three of the four major areas were considered for blockchain application: voting, business programs, and archives. Of these, two areas might benefit from blockchain technology: archives (in the near term) and business programs (future application).

The California State Archives

The California State Archives has served as the repository for many significant records relating to state laws and legislation. The Archives collects, catalogs, preserves, and provides access to the historic records of state and local governments, and private collections. Each year hundreds 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 Glacier-based 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 multi-lingual 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.[5] The white paper includes useful analysis of the implications of using blockchain with records management.[6]

Considerations and opportunities for Blockchain Application

Level of risk/privacy: While this is an important historical division, this use case will 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 Archives than other Secretary of State divisions, such as elections or business programs. Because Archives are public records, privacy concerns are minimal.

Authentication: 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 do pilot projects in various areas with its IT infrastructure. With additional resources, extensive modifications would not be necessary to conduct a blockchain pilot with Archives.

Added value of using blockchain: Archives would benefit from blockchain in several ways. Archives documents are used often 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.

Blockchain Implementation Potential Barriers and Concerns

Decentralization: If blockchain technology were used to digitize the archives, the state Archives department 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."[7] 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.[8] 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."[9]

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.[10]

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 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 blockchain 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 an RFP for a digitization/authentication system, blockchain or not. The specific options could be examined on their merits.

Business Programs

The Business Programs Division has been experimenting with modules related to new technologies, featured in the new online portal at https://www.sos.ca.gov/business-programs/bizfile/. 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.

Internet Voting

Introduction – California Perspective

One potential application of blockchain is internet voting. 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.[11] These principles should be applied 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 US operate under the UOCAVA[12] including the first pilots of blockchain-based voting, in Denver, Utah County, and West Virginia.[13] This was the source of much controversy among cyber professionals who believe there are significant unanswered questions.[14]

Ironically, presumably because of heightened scrutiny around early pilots, the authentication and authorization process with Voatz, the online voting system used in these jurisdictions, is likely the most restrictive in the country – including registering in advance with a driver's license, validating a phone number and setting a PIN, and then comparing facial recognition to the driver's license photo.[15] Other enthusiasts propose composing a voter ID using fingerprint or retinal scans.[16]

Under the Voatz system, after voting using a mobile app, the voter receives an email receipt with an ID number and a record of their votes; the election administrator receives and publicizes the ID number and a record of the votes, but not the voter's identity, preserving anonymity but enabling each voter to verify that their vote was counted as cast.[17] The emailing of the candidate selections represents a breach of strong anonymity similar to that inherent in vote by mail, but replacing the email trail with an independent-verification app or similar could fulfill the same goal eventually.

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 signing names in person 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 this problem. 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.[22] As 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 your vote accurately represents your choices. The greatest single point of failure is the app, website or device itself. A compromised website could display a code that validates as a vote for one candidate but transmits something different, for example.[23] 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.[24]

- **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 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. (To the extent that a malicious actor de-anonymizes ballots, their goal is presumably to intimidate and influence voters. For intimidation to work, it requires you to *know* that your ballot will be decrypted; surreptitious decryption and de-anonymization seems to be of relatively little use. But you can imagine a skilled intelligence service putting this in the Kompromat file – if a foreign intelligence service happened to know that the Secretary of State didn't vote for the President, it's a great opportunity to ask for a favor.)
- 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 good internet systems) eliminate some single points of failure but may introduce others.
- For example, it's positive 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.[25] 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.[26] 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 example? How do we ensure that the face recognition system doesn't have racial, gender, or age bias, as has been commonly reported across such systems?[27]

Security: Few computer scientists with expertise in elections believe that implementations of elections protocols (such as voter authentication, ballot auditability,

and anonymity) are mature enough or secure enough to be deployed at scale.[28] Security breaches are ubiquitous in online systems: witness financial companies like Equifax and Heartland Payment Systems; government systems at the State Department, OPM, and defense contractors; tech companies like Yahoo and Uber, etc.[29] Election systems are among the hardest to secure, because of anonymity (among other things).

Endnotes

---

[1] Blockchain Project for National Archives Reports Successful Trial for Audio-Visual Content

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] National Archives and Records Administration, Blockchain White Paper.

[6] Id.

[7] Email from David Jefferson, March 27, 2020, 10:48 A.M., on file with author (emphasis original).

[8] National Archives and Records Administration, Blockchain White Paper.

[9] National Archives and Records Administration, Blockchain White Paper.

[10] *Id.*

[11] Verified Voting Foundation: Principles for New Voting Systems; see also ProCon.org's summary of positions on voting machines by the National Academy of Sciences

[12] https://www.fvap.gov/uploads/FVAP/Policies/uocavalaw.pdf

[13] Under the Hood: The West Virginia Mobile Voting Pilot; Voatz, the blockchain-based voting app, gets another vote of confidence as Denver agrees to try it; Utah County, Utah, begins review of mobile-app votes; WV Secretary of State – 24 Counties to Offer Mobile Voting Option for Military Personnel Overseas

[14] What We Don't Know About the Voatz "Blockchain" Internet Voting System

[15] Voatz, the blockchain-based voting app, gets another vote of confidence as Denver agrees to try it

[16] Opinion | It's Time for Online Voting

[17] Nimit Sawhney, interview with Working Group

[18] Online voting is impossible to secure. So why are some governments using it?. For a 2017 not-comprehensive list of companies doing online voting, see here: Nine Companies That Want To Revolutionize Voting Technology

[19] Security Analysis of the Estonian Internet Voting System and associated Press Release.

[20] The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election

[21] Solution Overview: Online Voting Security and Verifiability

[22] What Is a Voter Verified Paper Audit Trail (VVPAT)?; Why paper is considered state-of-the-art voting technology

[23] What We Don't Know About the Voatz "Blockchain" Internet Voting System

[24] See e.g. Election Trust and compare to Agora: Bringing our voting systems into the 21st century (Whitepaper Version 0.2)

[25] Shut up and trust them Why Moscow's new Internet voting system relies on faith, not transparency or peer review; Libertarian Party of Russia (via Telegram)

[26] Going From Bad to Worse: From Internet Voting to Blockchain Voting

[27] Voatz states that in 99.2% of approximately 100,000 cases to date, voters' faces were automatically identified, and that all of the other 0.8% have succeeded with a fail-over to human verification.[11.1] We encourage government officials to take the risk of racial bias extremely seriously. However, we are sensitive to the racial bias in existing systems – long lines at certain polling places and not others, for example – and so ask ourselves the question, would the net impact of offering driver's-license-based facial recognition internet voting be a reduction or enhancement in the ability of voters from minority groups, particularly dark-skinned voters, to express themselves equally? If we cannot establish that it is an improvement, we cannot permit such a system to move forward. However, if we conclude that new technology will reduce voting barriers faced by underrepresented minorities, we cannot ignore that conclusion either.

[28] If I Can Shop and Bank Online, Why Can't I Vote Online?

[29] Going From Bad to Worse: From Internet Voting to Blockchain Voting at 6; The 18 biggest data breaches of the 21st century; Every single Yahoo account was hacked - 3 billion in all; Krebs on Security: Target: Names, Emails, Phone Numbers on Up To 70 Million Customers Stolen; The OPM hack explained: Bad security practices meet China's Captain America; New details emerge about 2014 Russian hack of the State Department: It was 'hand to hand combat'; Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies

V.H. Education and Workforce

Key Recommendations

- California should emphasize interoperability, security, and scalability when piloting the use of blockchain for education and workforce records.
- The Future of Work Commission[1] 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.
- 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.
- A natural role for the State would be to publish a framework of key questions, considerations, and paths forward for groups interacting with the California public school system and public service. These could help identify additional blockchain-based pilot projects, as well as provide an inventory for interested agencies to leverage for their own efforts.
- Moreover, 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. Finally, illustrating the different phases of technology adoption, and encouraging discussion of risks, benefits, and "readiness levels" needed along the way will provide much needed clarity for technology developers, policy writers, and solution adopters moving forward.

Introduction – California perspective

California comprises an estimated active workforce of over 19 million[1] that connects to a variety of local and international institutions. As the American Workforce Policy Advisory Board's White Paper on Interoperable Learning Records[2] 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."

Education and workforce records are integral to a dynamic labor ecosystem. Presently, California has regulatory regimes that require licensing of numerous professions and trades. All told, the Department of Consumer Affairs alone operates more than 150 types of licenses.[3] 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

University Academic Records. Blockchain technology has been used by MIT for certificate dissemination since 2015 and for diplomas since 2017.[4] Additional efforts from Foothill-DeAnza College, Arizona State University, and other institutions have explored using blockchain and information about digital education records to help improve degree completion and student services.[5] 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.[6] 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. California has a labor market of approximately 19.5 million people, with many entering or exiting the market and switching jobs. In California, 95% of employers[7] conduct background checks on applicants that include verifying previous employment, past performance, and educational credentials. 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 a time-consuming, paper-based process. While the process of generating employment verification letters and salary verification letters has increasingly become computerized, 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 the like, and is so complex that businesses turn to intermediaries like background check companies to compile the information for them.

Skills certification. Current credentialing systems do not necessarily reflect accurately the skills of workers. 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 or represented by their degree. More important, individuals who do not complete four-year degrees have highly-valued skills and experiences gained through jobs or other means, but are unable to demonstrate these to employers in today's paper-based world.

Iterative design process. To empower all Californians with such a level of efficiency 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.

Supporting the workforce. With the ever-increasing pace of change in the labor market, workers seeking to retrain or gain new skills are unlikely to take traditional paths of going back to obtain a formal degree. 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."

Verification. Blockchain-based credentialing systems can help remove existing friction by enabling online credential sharing in a secure way, 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 issue, by verifying the issuer's signature via a public key stored in a blockchain decentralized identifier (DID). Likewise, the party can 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.

Accountability. A blockchain-based credentials system could empower a more diverse and nuanced set of credentials that reflect the pace and trajectory of modern work, including and facilitating 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.

Equity. 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 standards openly for "learner-controlled, privacy-preserving credentials, in a manner that ensures interoperability."[9]

Sparking innovation and collaboration. 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.

In doing so, one can anticipate the need for supporting open and accessible education and training about blockchain and related technologies, to build greater fluency with emerging concepts and to identify opportunities for increased productivity and innovation. Educational efforts and content 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.

Community of practice. Whether the State collaborates with other organizations or hosts formal training or certification mechanisms on its own to generate a pipeline of skilled contributors, care should be taken to support a diverse and collaborative "community of practice." By prioritizing low-barrier-to-entry paths for individuals to collectively "upskill" and develop new competencies, we 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 innovations and innovators, but also for promoting the sharing of resources and ideas.

Endnotes

[1] https://www.bls.gov/eag/eag.ca.htm

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

[3] https://www.dca.ca.gov/consumers/wll.shtml

[4] http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain- technology-1017

[5] "Boosting Degree Completion with Blockchain," Inside Higher Education, July 2019.

[6] "Dallas County Community College District Students Receive 'GreenLight' Toward Ownership, Lifelong Access to Academic Records," August 2019.

[7] https://www.esrcheck.com/wordpress/2018/07/02/napbs-survey-reveals-95-percent-employers- conducting-employment-background-screening-2018/

[8] https://www.labor.ca.gov/labor-and-workforce-development-agency/fowc/

[9] "Building the digital credential infrastructure for the future," a white paper from the Digital Credentials Consortium, February 2020.