BLOCKCHAIN, DIGITAL IDENTITY, AND HEALTH RECORDS //

Considerations for Vulnerable Populations in California

Maitreyi Sistla &
Camille Crittenden
October 2020

CITRIS AND THE BANATAO INSTITUTE | CITRIS POLICY LAB

Blockchain, Digital Identity, and Health Records

Considerations for Vulnerable Populations
in California

Maitreyi Sistla &
Camille Crittenden
October 2020

Contents

Executive Summary 1

01 // INTRODUCTION 4

02 // CONTEXT SETTING 6

A brief history of blockchain technology 7

Blockchain technology for social impact 9

Criticism of blockchain technology since 2018 11

Overview of the California Blockchain Working Group 13

03 // PURPOSE OF THIS REPORT AND PROBLEM STATEMENT 15

04 // METHODOLOGY 17

05 // OVERVIEW OF BLOCKCHAIN TECHNOLOGIES 20

Definition of blockchain technology and its key features 21

Main types of blockchain technology 22

When should a blockchain be used? And what are its alternatives? 24

06 // OVERVIEW OF BLOCKCHAIN TECHNOLOGY AND DIGITAL IDENTITY 26

Overview of digital identity 27

Overview of blockchain technology's role in digital technology 29

Overview of California's digital identity proposal 30

07 // OVERVIEW OF BLOCKCHAIN TECHNOLOGY AND HEALTH RECORDS 32

Interoperability and privacy concerns with existing health records systems 33

Existing solutions 34

Blockchain technology as a solution 35

08 // OPPORTUNITIES 38

Opportunity #1: Streamlined service provision 39

Opportunity #2: More comprehensive health records 42

09 // CHALLENGES 45
Challenge #1: User authentication 46
Challenge #2: Existing solutions 47
Challenge #3: Long-term data security 48
10 // DISCUSSION AND QUESTIONS 50
ACKNOWLEDGMENTS 53
APPENDIX: A NOTE ON OPPOSING VIEWS 54

Executive Summary

In 2018, the State of California established a Blockchain Working Group (BWG) to evaluate blockchain technology uses, risks, benefits, legal implications and best practices; define the term blockchain; and recommend amendments to California statutes that may be affected by blockchain development.[1] The BWG was charged with exploring the potential of blockchain technologies to improve state government operations and to provide guidance for an appropriate regulatory framework.

Possible applications of blockchain technology in the public sector examined by the Working Group included healthcare, education and workforce credentialing, digital identity for vital records, property tracking and tax collection among others.

This report explores the overall potential of blockchain's use in the public sector and specifically focuses on two use cases that have received less attention: the effect that blockchain-based digital identity and health records management systems may have on the homeless and other vulnerable populations in California. What are the risks and opportunities of implementing these technologies in programs designed to serve those in precarious financial circumstances like the homeless? We explore this topic through a combination of stakeholder interviews, surveys, and an in-depth literature review.

We find two main opportunities of blockchain-based identity and health records management systems for the homeless:

1. **These technologies have considerable potential to streamline applications for public benefits for homeless individuals.** Roughly 50% of the homeless in California lack a physical ID at any given time, leading to delays in receiving critical public assistance.[2] A blockchain-based ID system would allow individuals to store and transfer documents digitally, reducing the administrative burden required to apply for and process public assistance.[3]

1. The BWG was established in the State of California through Assembly Bill 2658 (Calderon).

2. Alameda County Health Care for the Homeless, Personal Interview, April 2020.

3. For an in-depth discussion of the complications for the homeless to secure and retain photo

2. **Blockchain could greatly improve the management of medical records and delivery of medical and mental health services if physicians gain easier access to complete information when providing care.** A client-centered and blockchain-based health records management system may assist with data sharing between health care and social service agencies, and may allow physicians and social service providers to better coordinate care for the homeless.

However, we also find considerable challenges with implementing this technology for vulnerable populations, including:

1. **User authentication.** Current blockchain-based ID or health records management systems require a smart card (or similar physical device), password, or biometrics for login. The same circumstances that make it difficult for homeless individuals to retain their physical IDs will also make it difficult for them to retain a smartcard or password, and most evidence shows that these individuals would not be willing to use biometrics for login.

2. **Sunk costs of existing solutions.** The state has already spent tens of millions of dollars developing databases (such as the Homelessness Management Information System and Health Information Exchanges) that aim to improve data sharing across health care and service providers. It is unclear whether state governments will be willing to attempt a new solution for data interoperability problems when considerable effort has already been made on existing solutions.

3. **Concerns with data security.** Blockchain technologies utilize cryptographic hash functions to store sensitive data. Many computer science researchers believe these hash functions will be easily re-engineered in the next 30-50 years through technologies like quantum computing. Governments should be especially careful with supporting solutions that place sensitive information, such as medical data, for vulnerable populations on these blockchains.

Overall, we believe that blockchain technologies could improve public service provision and healthcare delivery for the homeless and other vulnerable populations in California. However, there are many barriers,

---

identification, see "Photo Identification Barriers Faced by Homeless Persons: The Impact of September 11," Report by the National Law Center on Homelessness and Poverty, April 2004: https://nlchp.org/wp-content/uploads/2018/10/ID_Barriers.pdf.

including issues with user authentication, cost and political feasibility, that must be addressed before these benefits can be realized.

01 // INTRODUCTION

01 //

INTRODUCTION

Blockchain technologies are regarded as a promising innovation with the capacity to transform the financial industry, supply chains, and identity management. However, the impact this technology may have on the public sector, and on vulnerable populations specifically, is less explored. Most blockchain use cases until now have been in the private sector.

To address this gap, the State of California established a Blockchain Working Group in 2019, charged with providing recommendations for the California legislature on potential uses of blockchain technologies in state government operations and offering guidance on regulatory frameworks for the technology for California businesses. This report explores the use of blockchain in the public sector more broadly, and specifically looks at two case studies—blockchain-based identity systems and health records management systems—and how these uses could affect vulnerable populations like the homeless in California. This information will help legislators, service providers and advocates evaluate the potential risks and opportunities of these technologies on California's most vulnerable.

The report first provides a short overview of the history of blockchain to set the context for why California's Blockchain Working Group was established. Next, the report turns to the California Blockchain Working Group's purpose and structure, and a description of the methodology used to address our specific research question, as well as an overview of blockchain technologies, digital identity systems, and blockchain-based health records management systems. The opportunities and risks of implementing these systems on vulnerable populations within California are evaluated. Last, the report offers recommendations for government entities in California and a list of questions that require further research.

02 //
CONTEXT

02 //
CONTEXT

A brief history of blockchain technology

In the early-to-mid 2010s, blockchain technology took the world by storm. Though computer scientists and economists had been toying with the idea of a digital currency for decades, researchers had not yet been able to build such a system. A key barrier for computer scientists was the problem of "double spending." When a currency was deployed digitally and did not have an actual physical tender, how could one ensure that a "digital dollar" wouldn't be duplicated and spent more than once? This double-spending problem halted the development of a digital currency for years.

In 2008, developer Satoshi Nakamoto published a canonical paper that solved just this problem.[4] Titled "Bitcoin: A Peer-to-Peer Electronic Cash System," the paper provided a theoretical framework for a payment system that utilized a peer-to-peer system to solve this infamous double-spending problem.[5] By linking each transaction to its preceding transaction, and requiring that new transactions be "approved" by a network of peer computers, one unit of digital currency could only be spent once.

And so began the bitcoin and cryptocurrency movement. By early 2009, Satoshi Nakamoto actually built the bitcoin protocol envisioned in his 2008 paper, and formal bitcoin marketplaces began to emerge 2010. Investors began "mining"[6] and frantically trading bitcoins, and by the end of 2017, the value of one bitcoin had skyrocketed to $20,000—over twenty times its value at the beginning of the year.[7]

---

4. Satoshi Nakamoto is the pseudonym for the first bitcoin developer. The actual identity (or identities) of Satoshi Nakamoto has not been released to this day.

5. Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." Satoshi Nakamoto Institute, (October 2018): https://nakamotoinstitute.org/bitcoin/.

6. Cryptocurrency mining is a process by which users can add transactions to bitcoin's ledger. More information can be found here: https://cointelegraph.com/bitcoin-for-beginners/what-is-mining.

7. Stan Higgins. "From $900 to $20,000: Bitcoin's Historic 2017 Price Run Revisited." CoinDesk,

Amid the bitcoin hype, computer scientists began looking at the underlying framework of the currency and realized that its use could span far beyond cryptocurrency. The peer-to-peer database that solved the "double-spend" problem could potentially solve a variety of problems plaguing other industries, from supply chain management to international remittances. Researchers named this distributed database a "blockchain" system, and a variety of blockchain startups emerged in the mid-2010s. The first and most successful to date—the Ethereum blockchain, supported by the Ethereum Foundation—was created in 2013, with the primary goal of building a distributed database system much like bitcoin's that could be deployed in a wider range of use cases. The Ethereum network's significant contribution was creating a programmable blockchain that enabled a variety of smart contracts.[8]

In the years after bitcoin was prototyped, a variety of financial institutions began accepting the currency as payments. Government institutions began researching the viability of cryptocurrencies, and even major banks began investing in blockchain technology working groups. As of 2020, major private technology companies that have either invested in or explored the use of blockchain technology in their operations or products include IBM, Facebook (through the infamous Libra technology), Microsoft, JP Morgan Chase, and PayPal. Six out of ten large corporations are said to either be considering using blockchain technologies in their operations or are already in the process of deploying it.[9]

December 29, 2017. https://www.coindesk.com/900-20000-bitcoins-historic-2017-price-run-revisited.

8. As defined by IBM, smart contracts are: "lines of code that are stored on a blockchain and automatically execute when predetermined terms and conditions are met. At the most basic level, they are programs that are run as they've been set up to run by the people who developed them." See: Nigel Gopie, "What are smart contracts on blockchain?" IBM Blockchain Blog, July 2, 2018, https://www.ibm.com/blogs/blockchain/2018/07/what-are-smart-contracts-on-blockchain/.

9. Francisco Memoria. "Study reveals 6 out of 10 major corporations are looking into blockchain technology integration." CCN, August 1, 2017. https://www.ccn.com/study-reveals-6-out-of-10-major-corporations-are-looking-into-blockchain-technology-integration/.

What are digital currencies and cryptocurrencies?

Digital currencies are currencies that only exist in digital form. No physical manifestation (i.e., cash or coins) of the currency exists.

Cryptocurrencies are a form of digital currency that use encryption techniques to verify the use and transfer of funds, allowing the currency to operate outside of a central authority such as a bank. Bitcoins are a form of cryptocurrency.

Blockchain for social impact

In parallel with increased venture and private sector investment in blockchain technologies, private companies and technologists began to pitch numerous use cases for social impact. Initiatives such as Blockchain for Social Impact[10] and new start-ups like Blockchain for Change[11] emerged that promised to solve key problems in the public sector. Many of these initiatives have focused on use-cases in humanitarian aid, where the need for establishing identity and banking systems for refugees and migrants is especially dire. Enthusiasts believed that blockchains were well suited to social impact causes because it can solve a variety of coordination problems, especially in scenarios where there is no clear central actor to coordinate or provide resources.[12]

Perhaps the most notable use of blockchain technology for social impact to date has been its deployment by the World Food Programme to assist refugees in Jordan. The UN agency partnered with Ethereum to provide 100,000 refugees with a blockchain-based cryptocurrency account and identity system. This account allows the UN to deposit money directly into refugees' bank accounts, which can be used to purchase food and other necessities.[13] The system has been expanded to refugee camps in Bangladesh and Pakistan, and uses a biometric system to authenticate each refugee's identity.[14] UN officials

10. See https://blockchainforsocialimpact.com/.

11. See https://blockchainforchange.org/.

12. Justine Humenansky (University of California, Berkeley), Personal Interview, July 21, 2020.

13. Russ Juskalian. "Inside the Jordan refugee camp that runs on blockchain." MIT Technology Review, April 12, 2018. https://www.technologyreview.com/2018/04/12/143410/inside-the-jordan-refugee-camp-that-runs-on-blockchain/.

14. "What is 'blockchain' and how is it connecting to fighting hunger?" World Food Programme, March 6, 2017. https://insight.wfp.org/what-is-blockchain-and-how-is-it-connected-to-fighting-hunger-7f1b42da9fe.

found the blockchain technology appealing for cash transfers since it protects refugees' privacy and completes transactions more securely than centralized database systems can. In addition, the technology could withstand disasters that could destroy more centralized record-keeping systems.[15] The WFP and other humanitarian organizations are now debating the idea of creating blockchain-based "digital wallets," where birth certificates, education credentials, and other key documents can be stored for refugee and migrant populations.

The creation of digital identities and alternative banking systems are the most-cited use cases for blockchain technology in the social impact sphere. However, technologists have proposed other use cases in the public sector as well, including:

- **Supply chain management**, ensuring that products meet required labor and sustainability standards[16]
- **Medical records**, improving interoperability of records between and within health care agencies, and placing more ownership of medical records in the hands of individual patients[17]
- **Land and property rights**, reducing issues of corruption, lack of trust, and insecure data that often plague property records management[18]
- **Energy management**, solving an array of bureaucratic and data management problems found in smart energy grid deployments[19]
- **Voting systems**, reducing potential corruption in democratic elections[20]

---

15. Ibid, "What is 'blockchain' and how is it connecting to fighting hunger?"

16. Sheila Warren, Christoph Wolff, and Nadia Hewett. "Inclusive Deployment of Blockchain for Supply Chains." World Economic Forum, March 2019, http://www3.weforum.org/docs/WEF_Introduction_to_Blockchain_for_Supply_Chains.pdf.

17. Anuraag Vazirani, Odhran O'Donoghue, David Brindley, and Edward Meinert. "Blockchain vehicles for efficient Medical Record management," Nature—npj Digital Medicine 3, no, 1 (January 2020): https://www.nature.com/articles/s41746-019-0211-0.

18. "Blockchain and Property Rights." New America Foundation, https://www.newamerica.org/future-property-rights/reports/proprightstech-primers/blockchain-and-property-rights/.

19. Mike Orcutt. "How Blockchain Could Give Us a Smarter Energy Grid." MIT Technology Review, October 16, 2017, https://www.technologyreview.com/2017/10/16/148584/how-blockchain-could-give-us-a-smarter-energy-grid/.

20. Galen, et al. "Blockchain for Social Impact—2019." Stanford Graduate School of Business, Center for Social Innovation, 2019, https://www.gsb.stanford.edu/sites/gsb/files/publication-

A report by McKinsey & Company specifically looked at the impact and feasibility of blockchain technologies, and found that the public sector may be able to benefit significantly from these technologies.[21] According to this report, blockchain technology offers potential for transforming welfare payments, tax collecting and reporting, government records, identity, and voting systems.

Even with this excitement, however, most blockchain technology deployments for social impact have been in the developing world. Fewer deployments of blockchain technology have been explored in developed countries, and especially in the United States. Though numerous federal government agencies and state governments have examined the potential of blockchain technology to improve government operations, a large-scale deployment of blockchain technology in the public sphere in the US has yet to be implemented.

Criticism of blockchain technologies since 2018

Since the peak of the blockchain technology "hype" in 2018, the technology has seen considerable criticism from computer scientists, technologists, and ethicists. Many question whether blockchains are a technology in search of a real problem. As three USAID development professionals stated after conducting a thorough analysis of the technology, "we found a proliferation of [blockchain] press releases, white papers, and persuasively written articles. However, we found no documentation or evidence of the results blockchain was purported to have achieved in these claims… Despite all the hype about how blockchain will bring unheralded transparency to processes and operations in low-trust environments, the industry itself is opaque."[22]

The original cryptocurrency deployments were extremely energy intensive, with some estimations that bitcoin mining used as much power each year as the

pdf/csi-report-2019-blockchain-social-impact.pdf.

21. Brant Carson, Giulio Romanelli, Patricia Walsh, and Askhat Zhumaev. "Blockchain beyond the hype: What is the strategic business value?" McKinsey and Company, June 2018. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.

22. John Burg, Christine Murphy, and Jean Petraud. "Blockchain for International Development: Using a Learning Agenda to Address Knowledge Gaps." MERL Tech Blog, September 7, 2018. http://merltech.org/blockchain-for-international-development-using-a-learning-agenda-to-address-knowledge-gaps/ .

country of Switzerland.[23] Others cite the scalability problem found in many blockchain technology deployments. As of 2019, for example, the Ethereum blockchain is only able to conduct 15 to 20 transactions per second—making it impossible to use in any practical setting.[24] The past couple of years have seen a flurry of cyber-attacks against blockchain technologies as well, leading some to doubt whether claims made by technology start-ups that blockchain technologies are more secure than traditional databases actually hold true.[25] Lastly, even beyond the practical implementation challenges, some have criticized the fundamental purported value of blockchain systems and their usefulness in private and public sector applications. These critics believe that most touted use cases of blockchain technology outside of cryptocurrency either do not actually use a "blockchain system,"[26] or could be achieved just as easily with a traditional database system.[27]

In reality, most blockchain technologies are still in a research-and-development phase, and it will take a few years to determine the practical significance of the technology. Private companies that have invested in the technology are still

---

23. Chris Baraniuk. "Bitcoin's energy consumption 'equals that of Switzerland." BBC, July 3, 2019. https://www.bbc.com/news/technology-48853230.

24. Stephen O'Neal. "Who scales it best? Inside blockchains' ongoing transactions-per-second race." Coin Telegraph, January 22, 2019. https://cointelegraph.com/news/who-scales-it-best-inside-blockchains-ongoing-transactions-per-second-race.

25. Mike Orcutt. "Once hailed as unhackable, blockchains are now getting hacked." MIT Technology Review. 12 February 2019. https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/.

26. David Gerard. "The World Food Programme's much-publicised 'blockchain' has one participant—i.e. it's a database." Blog, November 26, 2017. https://davidgerard.co.uk/blockchain/2017/11/26/the-world-food-programmes-much-publicised-blockchain-has-one-participant-i-e-its-a-database/; Adrianne Jeffries. "'Blockchain' is Meaningless." The Verge, March 7, 2018. https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning.

27. Karl Wüst and Arthur Gervais. "Do you need a blockchain?" International Association for Cryptologic Research, (2017): https://eprint.iacr.org/2017/375.pdf; Gideon Greenspan. "Avoiding the pointless blockchain project." Multichain, November 25, 2015. https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/; Bruce Schneier. "There's No Good Reason to Trust Blockchain Technology." WIRED, February 6, 2019. https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/; James Mickens. "Blockchains are a bad idea: more specifically, blockchains are a very bad idea." Filmed January 23, 2019 at Harvard Business School Digital Initiative Talk, https://digital.hbs.edu/digital-infrastructure/blockchains-are-a-bad-idea-more-specifically-blockchains-are-a-very-bad-idea/; Brant Carson, Giulio Romanelli, Patricia Walsh, and Askhat Zhumaev. "Blockchain beyond the hype: What is the strategic business value?" McKinsey and Company, June 2018, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.

experimenting and solving some of the implementation challenges that have surfaced. Many experts do not think blockchains will be significantly deployed for another five to ten years.[28] As such, it may be difficult to differentiate at this time between the "hyped claims" that blockchain technology companies have made against their practical applications.

Overview of the California Blockchain Working Group

In response to the enthusiasm for blockchain technology in 2018 and the lack of understanding of blockchain technology use cases in the United States, the state of California under AB 2658 established a Blockchain Technology Working group. The group, overseen by the state's Government Operations Agency, was mandated to:

- Define the term blockchain
- Evaluate blockchain's potential uses, risks, benefits, legal implications, and best practices for applications within state government
- Recommend amendments to state statutes that may be affected by blockchain

The twenty-member working group submitted a report to the California legislature on July 1, 2020. [29] The working group comprised blockchain technology experts from the private sector, academia, civil society, and state government agencies. Since the group was established during the peak of interest in blockchain technology, it played a special role in helping the state understand its most promising and practical use cases.

The working group presented eight use cases of blockchain technology in

28. Brant Carson, Giulio Romanelli, Patricia Walsh, and Askhat Zhumaev. "Blockchain beyond the hype: What is the strategic business value?" McKinsey and Company, June 2018, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.

29. "Blockchain in California: A Roadmap." California Blockchain Working Group, July 2020. https://www.govops.ca.gov/wp-content/uploads/sites/11/2020/07/BWG-Final-Report-2020-July1.pdf.

its final report. As seen in Figure 1 below, these include: vital records; health records; supply chain (including food and pharmaceutical supply chains); property registration; utilities and natural resources; finance and payments (including taxes and welfare programs); justice and civic participation (including chain of evidence and video testimony); and education and workforce (including academic institutions and credentials). The concept of "digital identity"—a potential application of blockchain technology touted by many advocates and a prerequisite for many further applications—is a common thread that spans many of these use cases.

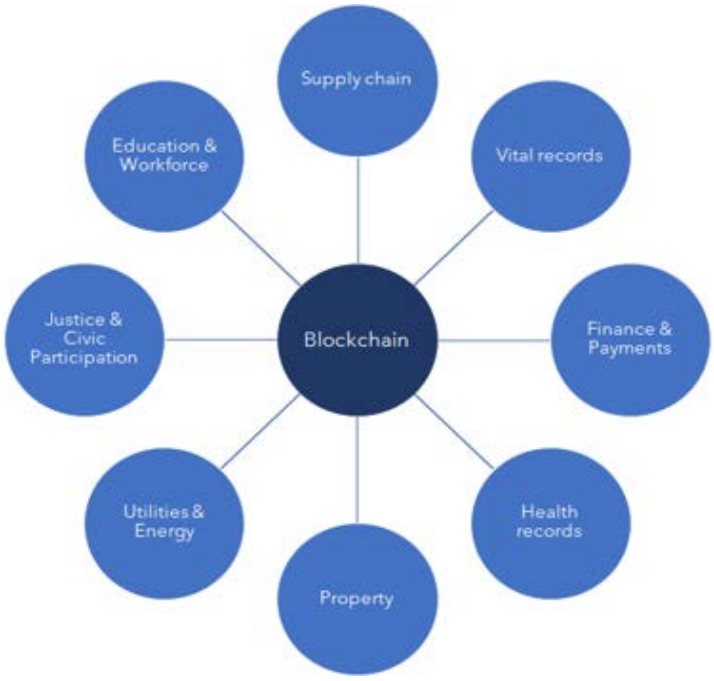


Figure 1: California Blockchain Working Group Use Cases

03 //

PURPOSE OF THIS REPORT AND PROBLEM STATEMENT

03 //

PURPOSE OF THIS REPORT AND PROBLEM STATEMENT

The remainder of this report will look at two sub-use cases within the California Blockchain Working Group — digital identity and health records management — with regard to the homeless and other vulnerable populations in California. Published literature is scant on the effects of these technologies on the homeless and other vulnerable populations in a domestic context. Most papers regarding the technology's effects on vulnerable populations focus on developing nations, where the need for an established system of identity and health records is more urgent. In parallel, current research on blockchain-based systems within the U.S. has ignored potential implications for vulnerable populations. With the exception of one attempt by the City of Austin and a related attempt by the University of Texas-Austin, no blockchain-based digital identity system has been deployed in a public setting in the United States. Given the importance of identity and health records management systems for vulnerable populations, and California's dire homelessness problem, this paper will assist policymakers in deciding whether to devote resources to implement this technology.

This paper asks: **what are the risks and opportunities for implementing a blockchain-based digital ID and health records management system on the homeless and other vulnerable populations in California?**

04 //
METHODOLOGY

04 //
METHODOLOGY

The conclusions in this report are drawn from three main sources: (1) an in-depth literature review of the state of blockchain technologies today; (2) stakeholder interviews with experts from government, academia, the private sector, and nonprofits; (3) recommendations and reports from California Blockchain Working Group experts; (4) a survey of Chief Information Officers (CIO) from various departments within the State of California; and (5) a public survey hosted on the State of California's Government Operations website that invited responses on the usefulness of this technology from the public sector, including experts in civic tech.

In order to gather a diverse array of viewpoints, we conducted stakeholder interviews with experts from academia, private sector companies, nonprofit organizations, and government agencies. Interviews were conducted with homelessness case managers and representatives of organizations with an in-depth understanding of health records management. Interviews typically lasted between 45 minutes and one hour, and were conducted using a semi-structured protocol tailored to each interview.

Of the sixteen interviews conducted, three were with individuals at private companies utilizing blockchain for digital identity systems, healthcare use cases, and in urban policy settings. One interview was with experts from a private law and professional services firm that works closely with the California state government. Four interviews were conducted with individuals affiliated with academic institutions. One interview was conducted with individuals affiliated with a blockchain social impact non-profit. One interview was conducted with a caseworker for unhoused residents in a California county. One interview was conducted with a director of a non-profit organization in California focused on improving healthcare for low-income Californians. One interview was conducted with a non-profit interested in using technology to solve issues related to homelessness. Lastly, three interviews were with government staff in California and the City of Austin.

The recommendations collected from Blockchain Working Group experts, as well as the survey with state CIOs and the state-wide public survey, were conducted for the Blockchain Working Group, and not specifically for this paper. Nonetheless, the insights gleaned from these sources are useful for assessing the risks and viability of implementing blockchain-based digital ID and health records management systems at the state level.

05 //

OVERVIEW OF BLOCKCHAIN TECHNOLOGIES

05 //

OVERVIEW OF BLOCKCHAIN TECHNOLOGIES

Definition of blockchain technology and its key features

One of the most challenging aspects of determining the practical use cases of blockchain technologies is that a standard definition of the technology has not yet prevailed. New types of the technology are constantly being created that change previously-accepted definitions. As The Verge writer Adrianne Jeffries states in a 2018 article, "There is no universal definition of a blockchain, and there is widespread disagreement over which qualities are essential in order to call something a blockchain."[30] This lack of clarity of blockchain definitions is, in part, why the State of California mandated that the Blockchain Working Group develop a state-wide definition, and why some blockchain critics hold that current deployments are no different than traditional databases.

The California Blockchain Working Group arrived at the following definition:

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

30. Adrianne Jeffries. "'Blockchain' is Meaningless." The Verge, March 7, 2018. https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning.

> business processes. These smart contracts are implemented by embedding software in transactions recorded on the datastore.[31]

Blockchain technologies have four main features. They are:

- **Immutable:** Blockchains are permanent records of transactions; once a block is added, it cannot be altered.

- **Decentralized:** Blockchains are stored on files that can be accessed and copied by any node in the network.

- **Consensus-Driven:** Each block (or piece of data) is validated via an algorithmically-determined consensus method, and must be validated before being added to the ledger.

- **Transparent:** The data on a blockchain can be accessed by any node on the blockchain, or anyone that has been given access to the blockchain.[32]

At their core, blockchains are seen as an exciting technology because they theoretically allow for multiple parties to trust a common ledger without needing a central authority. Traditional database systems are usually run by a central authority, whether a bank, government or other entity. Blockchain technologies allow these transactions to happen without a central authority, saving transaction costs by eliminating intermediaries and theoretically allowing individuals to maintain greater control over their own data.

Main types of blockchain technologies

Blockchain systems generally require two sets of permissions: read permissions, which allow someone to read data on the blockchain, and write permissions, which allow someone to write data onto the blockchain. **Permissionless**

31. "Blockchain in California: A Roadmap." California Blockchain Working Group, July 2020. https://www.govops.ca.gov/wp-content/uploads/sites/11/2020/07/BWG-Final-Report-2020-July1.pdf. We note that there is considerable disagreement on the definition that the California Blockchain Working Group has developed. For more information on the disagreement, see the "Note on Opposing Views" at the end of this report.

32. Karim Sultan, Umar Ruhi, and Rubina Lakhani. "Conceptualizing Blockchains: Characteristics and Applications." 11th IADIS International Conference on Information Systems, (2018): https://arxiv.org/ftp/arxiv/papers/1806/1806.03693.pdf. The level of transparency for blockchains depends on whether the blockchain is private or public, as discussed in the next section.

blockchain systems allow anyone who has access to the system to be able to read and write onto the system. Permission does not need to be obtained by a central authority to be able to write onto the system. **Permissioned** systems, on the other hand, allow all participants to read data, but only authorized entities can write data onto the blockchain. Usually, permission for writing on the blockchain is determined by a central authority.[33]

In addition, systems differ regarding ownership of the blockchain infrastructure itself. In **public** blockchains, the system is hosted on public servers. **Private** blockchains are hosted on private servers.[34]

Which type of blockchain technology is appropriate depends on the use case. Bitcoin, for example, is a public, permissionless blockchain technology since anyone can access the data and mine bitcoins. Public and permissionless blockchains are preferable for most cryptocurrencies. Ethereum also runs on a public blockchain system. Hyperledger, the blockchain system created by the Linux Foundation, runs on a private blockchain. Private blockchains can be useful for cases such as supply chains, where a restricted set of personnel should be able to access the overall system. Table 1 below gives examples of use cases appropriate for different types of blockchain.

It is important to stress that advantages differ for each type of blockchain system. For example, private or permissioned blockchains still depend on some type of central authority either running the server or allowing users to have certain read/write permissions. In addition, hybrid versions of blockchains can mold together the various characteristics of private, public, permissioned, and permissionless systems.[35] We note, however, that many have questioned the efficacy and notion of "private, permissioned" blockchains. Some experts believe that these blockchain technologies are no different than a simple database.[36]

---

33. Dylan Yaga, Peter Mell, Nik Roby, and Karen Scarfone. "Blockchain Technology Overview." National Institute of Standards and Technology, October 2018. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

34. Brant Carson, Giulio Romanelli, Patricia Walsh, and Askhat Zhumaev. "Blockchain beyond the hype: What is the strategic business value?" McKinsey and Company, June 2018. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.

35. For more insight into the specifics of private, public, permissioned, and permissionless blockchains, see this McKinsey report: Brant Carson, Giulio Romanelli, Patricia Walsh, and Askhat Zhumaev. "Blockchain beyond the hype: What is the strategic business value?" McKinsey and Company, July 19, 2018. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.

36. Eduardo Beltrame (Caltech), Justine Humenansky (UC Berkeley), and Adam Wiedmann (City

Table 1: Potential use cases for types of blockchains

	Permissionless	Permissioned
Public	• Cryptocurrencies • Video games	• Voter registration • Poll records
Private	• Supply chain • Government record keeping • Educational credentialing	• Medical records • Tax use cases

Note: This table was partially adapted from the Medium post of blockchain developer Demiro Massessi and an NYU GovLab Report[37]

When should a blockchain technology be used? And what are the alternatives?

Generally speaking, the alternative to blockchain systems are traditional, centralized private databases. Usually, these databases are stored in a cloud provider such as Amazon Web Services or Google Cloud. This database system is run by a centralized entity such as a bank, company, or government agency; the controlling organization will determine permissions to read and write the data.

The incremental value of blockchain systems, and whether a given use case for blockchain technology can be equally well accomplished with a traditional database system, has been widely debated. To help answer some of these questions, NIST has developed a set of features that might indicate whether investigation into blockchain systems is warranted. These include: "many participants; distributed participants; lack or need of a trusted third party; workflow is transactional in nature (e.g. transfer of digital assets/information in nature); a need for a globally scarce digital identifier (i.e. digital art or digital property); a need for a decentralized naming service or ordered registry; a need for a cryptographically secure system of ownership; a need to reduce or eliminate manual efforts of

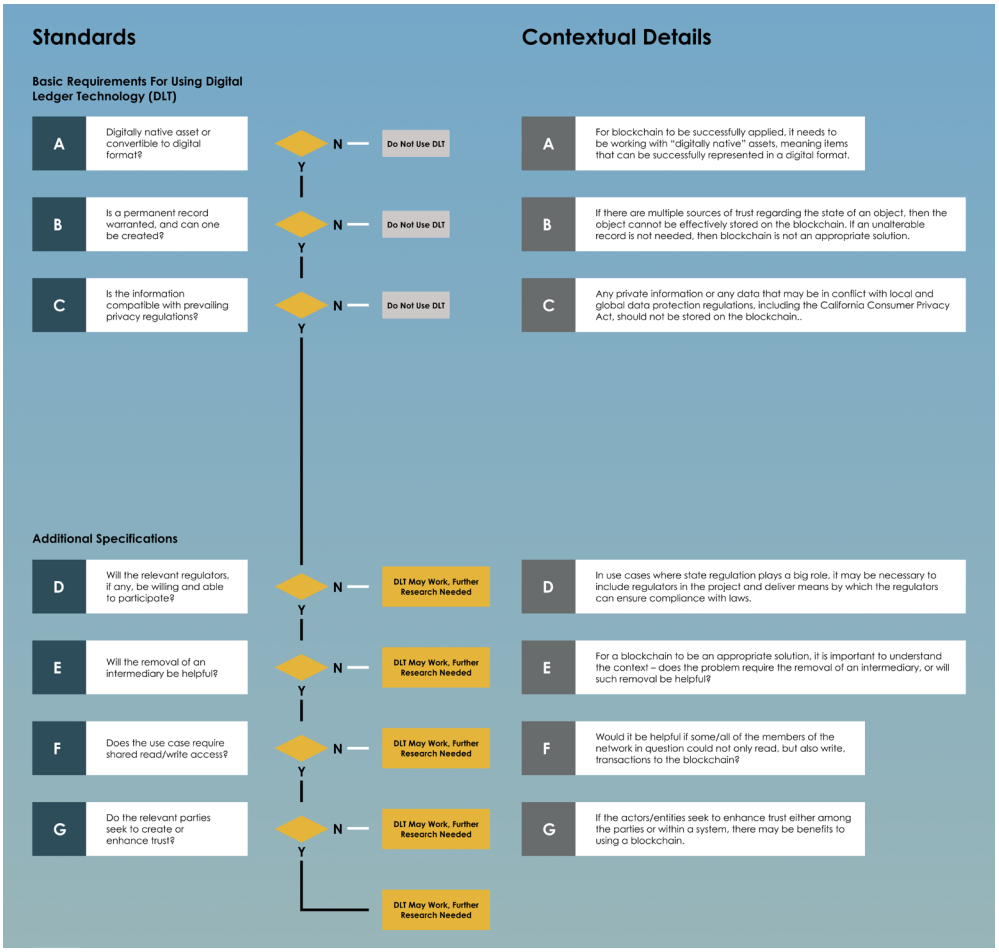
of Austin), Personal Interviews, July 2020.

37. Demiro Massessi. "Public vs. Private Blockchain in a Nutshell." Medium, December 12, 2018, https://medium.com/coinmonks/public-vs-private-blockchain-in-a-nutshell-c9fe284fa39f; Stefaan Verhulst and Andrew Young. "Field Report: On the Emergent Use of Distributed Ledger Technologies for Identity Management." GovLab. https://blockchan.ge/blockchange-fieldreport.pdf.

reconciliation and dispute resolutions; a need to enable real time monitoring of activity between regulators and regulated entities; and a need for a full transactional history and a full provenance of digital assets to be shared amongst participants."[38]

Figure 2, from the California Blockchain Working Group, is a flowchart depicting blockchain technology uses cases as well as instances in which traditional databases may be preferred over blockchain systems (or other distributed ledger technologies).[39]

Figure 2: Decision Matrix from the California Blockchain Working Group:



38. Yaga, Dylan, Peter Mell, Nik Roby, and Karen Scarfone. "Blockchain Technology Overview." National Institute of Standards and Technology, October 2018. https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

39. "Blockchain in California: A Roadmap." California Blockchain Working Group, July 2020. https://www.govops.ca.gov/wp-content/uploads/sites/11/2020/07/BWG-Final-Report-2020-July1.pdf.

06 //

OVERVIEW OF BLOCKCHAIN TECHNOLOGY AND DIGITAL IDENTITY

06 //

OVERVIEW OF BLOCKCHAIN TECHNOLOGY AND DIGITAL IDENTITY

Overview of digital identity

One of the most-cited use cases of blockchain technologies in the public sector is digital identity systems. Identity verification is a core component of effective and secure government and social institutions. Identity verification is also critical to many online systems; banks, social media companies, and email clients all need "digital representations" of individuals to send money, publish posts, or send emails.

In the developing world, humanitarian agencies have focused on the concept of establishing "digital identities" for all citizens. The World Bank, for example, estimates that as many as 1 billion people do not have official proof of identity.[40] Many of these individuals, mostly from high poverty areas, refugees or migrants, are unable to access formal government and financial systems due to this lack of identification. One of the UN's 2030 Sustainable Development Goals is to provide a legal identity for all individuals, including birth registration.[41] Organizations such as Kiva and Gravity have thus piloted digital identity systems to expand financial inclusion.[42]

40. Vyjayanti Desai, Anna Diofasi, and Jing Lu. "The global identification challenge: Who are the 1 billion people without proof of identity?" World Bank Blog, April 25, 2018. https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity.

41. See: https://www.un.org/sustainabledevelopment/peace-justice/.

42. See: https://www.kiva.org/protocol for Kiva's new digital identity system, and https://www.gravity.earth/ for Gravity Earth's digital identity platform.

What are digital identities and self-sovereign identities?

Digital identity: "A digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts."—National Institute of Standards and Technology, 2018

Self-sovereign identity: A self-sovereign identity is the concept that an individual should be able to control their identity information without an intervening central authority, like a government or company. Generally, self-sovereignty is seen as a characteristic of a digital identity platform.

Digital identities can also be managed by national governments. India and Estonia, for example, have established digital identity systems for their citizens. India's Aadhar program, launched in 2008, gives every citizen a unique identification number linked to biometric data. Aadhar numbers are used by government agencies to verify identity for civil transactions such as signing marriage certificates or paying taxes.[43] Estonia has provided every citizen with a chip-enabled card, through which all government services are conducted, including voting, ordering prescriptions, and filing taxes.[44]

Proponents of digital identity systems attest that the technology can vastly improve government services. Individuals will no longer need to show various pieces of identification, such as physical birth certificates, social security cards, or tax documents, in order to enroll for government services. According to a McKinsey study, "extending digital ID coverage could unlock economic value equivalent to 3 to 13 percent of GDP in 2030, with just over half of the potential economic value potentially accruing to individuals."[45]

For this reason, state governments in the United States have been exploring the concept of digital identity systems.[46]

---

43. Lauren Frayer. "India's Biometric ID System Has Led To Starvation for Some Poor, Advocates Say." NPR All Things Considered, October 1, 2018, https://www.npr.org/2018/10/01/652513097/indias-biometric-id-system-has-led-to-starvation-for-some-poor-advocates-say.

44. Kersti Kaljulaid. "Estonia is running its country like a tech company." QZ, February 19, 2019. https://qz.com/1535549/living-on-the-blockchain-is-a-game-changer-for-estonian-citizens/.

45. White, et al. "Digital ID: A key to inclusive growth." McKinsey Digital. April 17, 2019. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

46. For example, the State of Illinois partnered with a blockchain company in 2018 to pilot the use of blockchain technologies in administering birth certificates. For more information, see

Overview of blockchain technology's role in digital identity

Centralized digital identity systems can suffer from a variety of implementation issues. For example, cybersecurity experts have long been nervous about India's Aadhar system. With the biometric information of over 1 billion individuals stored on a centralized system, it has become a target for hackers.[47] Various civil society groups have also filed cases against the system to India's Supreme Court, stating that this type of centralized database violates the privacy and security of individual citizens.[48]

Some technologists believe blockchain technologies and other distributed systems could solve some of the issues inherent in centralized identity systems. According to our key informant interviews, digital identity systems on blockchain systems are preferable to those on traditional databases because:

1. **They do not rely on a central authority.** According to one of our key informants, a significant benefit of blockchain-based ID systems is that they are decentralized. That is, they can be implemented in a way that there is no central point of control and pieces of information are stored in different locations. This theoretically gives more power to individual users and assuages some privacy and security concerns of centralized identity systems.[49]

2. **They are more transparent.** Blockchain systems are often designed in a way that increases transparency to systems. That is, all records are documented and it is almost impossible for a single entity (such as a government or bank) to delete information once placed on the blockchain.[50]

3. **It ensures that the data stored is comprehensive and has not been altered over time.** The immutability and censorship-resistant characteristics of blockchain technology may better ensure that the data associated with an

---

this 2018 NYU GovLab paper by Andrew Young et al.: https://blockchan.ge/blockchange-birth-registration.pdf.

47. Mardav Jain. "The Aadhar Card: Cybersecurity Issues with India's Iiometric Experiment." The Henry M. Jackson School of International Studies at the University of Washington, May 9, 2019. https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/.

48. Alan Gelb, Anit Mukherjee, and Kyle Navis. "What India's Supreme Court Ruling on Aadhar Means for the Future." Center for Global Development, September 26, 2018. https://www.cgdev.org/blog/what-india-supreme-court-ruling-aadhaar-means-future.

49. Eduardo Beltrame and Dylan Bannon (California Institute of Technology), Personal Interview, April 2020.

50. Ibid, Eduardo Beltrame and Dylan Bannon.

individual is comprehensive and has not been altered over time.[51]

4. **It reduces the risk of identity theft.** Blockchains can increase the security of digital identity systems. A more secure system could reduce the risk of identity theft.[52] Government agencies administering identity systems may find this especially appealing.

5. **It could allow individuals to better control data about their identity.** Self-sovereign identities are a subset of broader digital identities. As one Blockchain Working Group expert writes: "Self-sovereign identity (SSI) is the concept that individuals and entities should own and control their identity and data, independent of a central authority."[53] For example, an ideal SSI would allow someone to prove they are over age 21 (to purchase alcohol) without exposing personal information about their birth date, address, height, and weight, as is done currently with ID cards in the United States. SSI identities need to be built on decentralized systems by definition.[54] Thus, blockchains allow for self-sovereignty with identity management.

Overview of California's digital identity proposal

In part because of these advantages, California's Department of Motor Vehicles is developing pilot models of blockchain-based digital identity systems for the state. As seen in Figure 3 below, the state is modeling a system in which key identity information now stored in various government agencies' databases would be stored on a blockchain. Currently, the DMV holds information like demographics, residency, and Social Security Number verification for the majority of Californians. This information is used by numerous other parties including other government agencies (for public benefits applications), insurance companies, and employers. Instead of requiring an individual to produce numerous pieces of paperwork for identity verification, the blockchain-based system piloted by the DMV would allow an individual to upload various government documents and IDs onto a blockchain system, and then send those documents to other agencies when needed. Individuals would determine who sees their private documents and would retain ownership of their personal information.[55]

51. Interview, Justine Humenansky (University of California), Personal Interview, March 2020.

52. Interview, Justine Humenansky (University of California), Personal Interview, July 2020.

53. Radhika Iyengar and Jason Albert. "California Blockchain Working Group: Digital Identity." Blockchain in California: A Roadmap, July 2020. https://www.govops.ca.gov/wp-content/uploads/sites/11/2020/07/BWG-Final-Report-2020-July1.pdf.

54. Ibid, Radhika Iyengar and Jason Albert.

55. "Blockchain in California: A Roadmap." California Blockchain Working Group, July 2020. https://www.govops.ca.gov/wp-content/uploads/sites/11/2020/07/BWG-Final-Report-2020-July1.pdf.

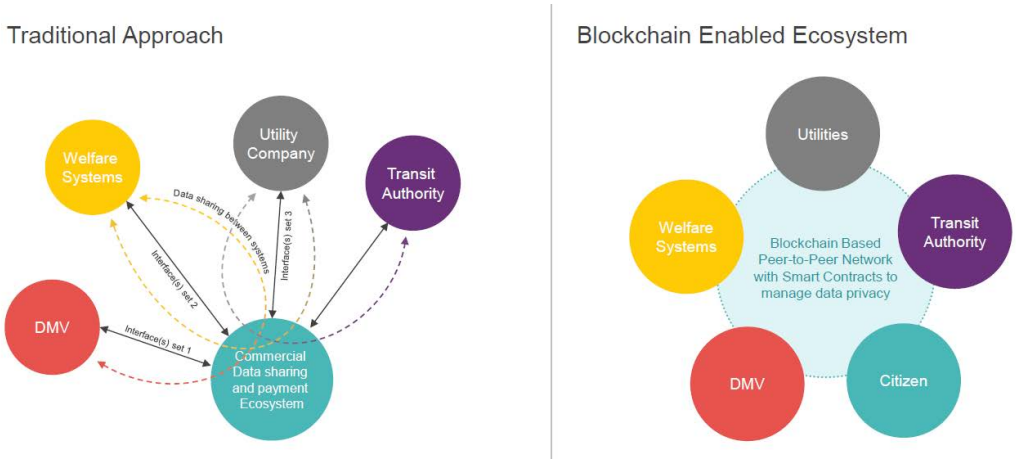


Figure 3: The State of California DMV's Citizen Verification Pilot

07 //

OVERVIEW OF BLOCKCHAIN TECHNOLOGY AND HEALTH RECORDS

07 //

OVERVIEW OF BLOCKCHAIN TECHNOLOGY AND HEALTH RECORDS

Interoperability and privacy concerns with existing health records systems

The United States lacks a complete and consistent method for storing and tracking patient healthcare records. Patients often encounter difficulty when trying to transfer their records between different healthcare providers, forced to navigate a heavily bureaucratic and burdensome process. This may result in less optimal care, as physicians may not have access to complete health information. This is especially true for vulnerable populations like the homeless, who lack the resources to submit the paperwork required to transfer records and are less likely to visit a consistent provider.

What is interoperability?

"Interoperability is defined as the ability of two or more systems to exchange information and the ability of those systems to use information that has been exchanged without special effort." — IEEE Standard Computer Dictionary

A variety of reasons lead to the lack of health-records interoperability. First, though nearly all healthcare providers now record medical information on electronic health records systems (EHRs), EHR systems vary between hospitals. Many are not interoperable, leading to difficulty in moving health records among providers.[56] This lack of interoperability is compounded by the fragmented nature of healthcare in the U.S. as a whole, where different health services—including everything from psychiatry to MRI scans—are executed by different providers. As a result, doctors with incomplete medical records can misdiagnose patients or duplicate medical tests that have already been per-

56. "Report to Congress: Challenges and Barriers to Interoperability." The Health Information Technology Policy Committee, December 2015. https://www.healthit.gov/sites/default/files/facas/HITPC_Final_ITF_Report_2015-12-16 v3.pdf.

formed. For example, a study from the Boston Children's Hospital estimates that one in three of their patients receives duplicate tests because of fragmented health records.[57]

Concerns regarding lack of ownership also plague existing medical records systems. Records are stored with providers, rather than with individual patients. Although all patients have the right to request a copy of their records under HIPAA laws, the records themselves are still stored on healthcare provider's servers. Patients also rarely have access to their entire medical record, as these records may be dispersed among multiple providers.[58] Thus, there are significant data ownership and privacy concerns with the current structure of medical records systems.

Lastly, significant security concerns with current health records management systems should also be addressed. The movement of health records onto electronic systems in the past decade has made the system vulnerable to traditional cybersecurity risks. In 2015, for example, there were 112 million incidents of breaches to health data.[59] These cybersecurity risks are especially concerning given the sensitive nature of health data.

Existing solutions

These issues with fragmentation and interoperability of health records are not new. State and federal government agencies have been working on solutions for decades. The most common solution has been for states and provider organizations to establish health information exchanges organizations (HIOs), systems that allow for providers to move clinical information among disparate providers electronically. In essence, HIOs provide a shared platform in which medical providers can share patient information in a safe and secure way. The actual structure of HIOs varies by state. In California, for example, they can be run by government agencies, nonprofits, or private companies. In recent years, especially following the passage of the Affordable Care Act in 2010, federal and

57. Stewart, et al. "A preliminary look at duplicate testing associated with lack of electronic health record interoperability for transferred patients," Journal of the American Medical Informatics Association 17, no. 3 (May 2010): 341-344. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2995707/.

58. Radhika Iyengar and Arshad Noor. "Health Records". California Blockchain Working Group Draft Report, March 27, 2020. https://www.govops.ca.gov/wp-content/uploads/sites/11/2020/04/Health-Records-Item-11.pdf.

59. Dan Munro. "Data breaches in healthcare totaled over 112 million records in 2015." Forbes, December 31, 2015. https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#3d23c00a7b07.

state governments have encouraged HIOs to solve the problem of health record fragmentation. This is a top priority of the Office of the National Coordinator for Health Information Technology (ONC), which guides interoperability efforts across state governments. However, despite considerable investments from the federal government, many argue that substantial progress has not been achieved.[60]

In addition to HIOs, the federal and state governments have also set up Homelessness Management Information Systems (HMIS) to better integrate data on the homeless population. HMIS's have been mandated by the U.S. Department of Housing and Urban Development (HUD) for local bodies to share data on homelessness case services and better coordinate care. Any homelessness provider that receives funding from HUD is required to upload certain information about its clients, including demographics, history of housing, and other important services. Again, the actual implementation of HMIS's varies greatly across jurisdictions. Some systems include health records, but issues with health data privacy laws often make it difficult to store and share health records on this system.

What are existing solutions to health records fragmentation?

Health Information Exchanges Organizations (HIOs): "Health information exchange organizations, or HIOs, are entities that facilitate the exchange of patient health information among the enterprises comprising a health care delivery system"—California Health Foundation

Homeless Management Information Systems: "A homeless management information system is a database used to record and track client-level information on the characteristics and service needs of people experiencing homelessness."— Ending Community Homelessness Coalition, Austin

Blockchain technology as a solution

Blockchain technology has been touted as a solution to these problems of identity and record fragmentation. Technologists opine that blockchain technologies are particularly suited to track health records because they transform health records from being agency-centered to client-centered.

60. Senators John Thune, Lamar Alexander, Pat Roberts, Richard Burr, and Mike Enzi. "Where is HITECH's $35 billion dollar investment going?" Health Affairs, March 4, 2015. https://www.healthaffairs.org/do/10.1377/hblog20150304.045199/full/.

Instead of agencies coordinating data sharing through HIOs or HMIS systems, a blockchain-based health records management system could allow individuals to keep track of their records and share them with medical providers as needed. However, some critics of blockchain technology state that the benefits below could still be realized through a traditional database system.[61]

Though blockchain-based health records management systems are still in development, a blockchain-based personal health system could improve the status quo by:

1. **Enhancing the portability and interoperability of health records systems.** Much like the advantages offered by digital identity systems, moving health records onto a blockchain will improve portability among service providers. By storing records on one blockchain system, records can theoretically be easily transferred from one provider to another, and can be transferred securely using smart contracts systems.[62]

2. **Allowing individuals to control their health records.** Blockchain systems are run using the cryptographic properties of private and public key access. Each individual must "open" their health records using a private key system. This allows patients to "share distinct identity attributes with health care organizations within the health care system on an as-needed basis, allowing data access time limits to be introduced by patients or providers."[63] In essence, a personalized health record system run on a blockchain would allow greater control of medical records for individual patients. Data would not be stored on providers' servers. Providers could only access data if allowed by an individual patient.

3. **Improving security.** Centralized EHR systems are a target for hackers since hackers can access multiple sensitive health records in one secure location. By placing data on a distributed network like a blockchain, hackers will face more difficulty obtaining these records.[64] Blockchain systems flip the architecture of data systems from having a hub and

---

61. See "Note on Opposing Views" at the end of this report.

62. Anuraag Vazirani. "Implementing blockchain for efficient health care: systematic review." Journal of Medical Internet Research 21, no.2 (February 2019). https://www.jmir.org/2019/2/e12439/.

63. RJ Krawiec. "Blockchain: Opportunities for health care." Deloitte, August 2016. https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html.

64. Radhika Iyengar and Arshad Noor. "Health Records." California Blockchain Working Group Draft Report, March 27, 2020. https://www.govops.ca.gov/wp-content/uploads/sites/11/2020/04/Health-Records-Item-11.pdf.

spoke model in which sensitive personal and health information is replicated to each spoke, to a hub and spoke model in which only one set of the information is stored on the hub. This has important security implications, since the points of vulnerability are greatly reduced.[65]

65. Justine Humenansky (University of California, Berkeley), Personal Interview, July 2020.

08 // OPPORTUNITIES

08 // OPPORTUNITIES

Based on our research, we have identified two key opportunities for blockchain-based digital identification and health records management systems to benefit the homeless and other vulnerable populations in California. These include: (1) allowing for more streamlined public assistance program applications, especially for housing and healthcare; and (2) solving issues created by health record siloes across county lines.

Opportunity #1: Streamlined public assistance, especially for housing and healthcare

Though (to our knowledge) no California-specific research has been published on this topic, the homelessness services case workers we interviewed estimated that about 50% of unhoused individuals in the Bay Area do not have a government-issued ID with them on a given day. This estimate is similar to those found by other city agencies. The City of Austin, for example, surveyed its homeless residents and also found that about half of them lack a physical ID.[66] According to our interviewees, most of these individuals have had a government-issued ID in the past, but find it difficult to retain either because of theft while in homeless encampments or loss when moving from location to location.

The lack of a physical identity document seems to create issues when enrolling in public benefits programs. In California, the state's major public assistance programs—including Medi-Cal (the state's public insurance program), CalFresh (the state's food assistance program, and CalWorks (the state's public assistance program for families with children)—all require some form of official identification, whether a driver's license, birth certificate, passport, or paycheck. Individuals who do not possess these documents when signing up for benefits must go to the relevant government agency to request a birth certificate or other form of identification. This can delay the processing of critical government benefits by weeks or months. In addition, this can be especially problematic when the docu-

66. See: http://projects.austintexas.io/projects/mypass-digital-identity/about/overview/.

mentation needed is from another country (such as a birth certificate). This may require individuals to visit embassy offices, which in California are often located in only Los Angeles or San Francisco.

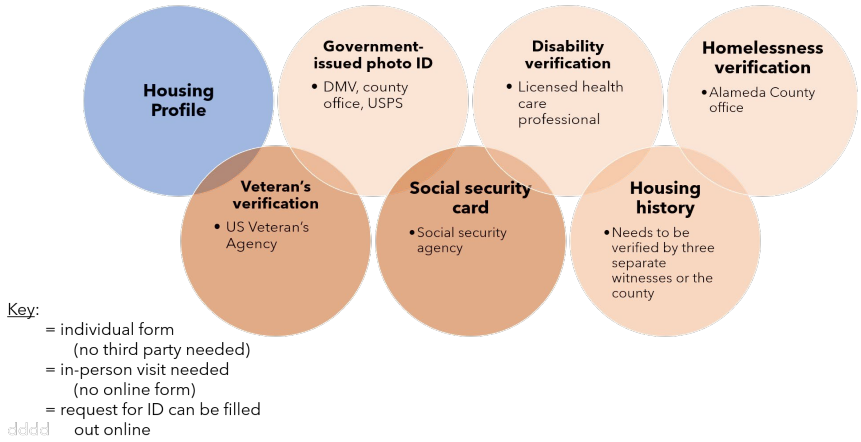
In addition, the lack of government documents seems especially problematic with housing applications. Supportive housing applications usually require many government documents, including everything from income verification to housing history. Many of these documents are stored with different government agencies. Caseworkers we interviewed stated it is often difficult for their unhoused clients to secure all the documents needed for these applications.

Figure 4 illustrates the difficulty of submitting a supportive housing application, also called Home Stretch, in Alameda County, California. (Note: Supportive housing applications are administered on a county-by-county basis in California. This example is illustrative of Alameda County, but based on our research, supportive housing applications require similar documentation in most California counties.) The application requires the following: (1) a housing profile (to be completed by the individual); (2) a government-issued photo ID; (3) a Social Security card; (4) veteran's verification, if applicable; (5) disability verification; (6) housing history; and (7) homelessness verification. Those with children must provide a social security card, birth certificate, and proof of custody for each child. Any other household members need to provide a government-issued photo ID or a Social Security card.[67] As Figure 4 shows, each of these documents is issued by a different state or federal agency. An individual might have to visit four different government offices in-person to obtain the paperwork necessary for this supportive housing application, an incredible burden for those who are unhoused.

A blockchain system such as that proposed by the DMV (see Figure 3) would greatly streamline this process. On a state-sponsored blockchain system, an individual could store documentation that has been verified by state and county agencies and send them to other entities when needed electronically. In this example, the individual could send his or her photo ID, social security card, and veteran's verification to the county office automatically without having to bring any paperwork. This benefits mobile populations like the homeless who face many barriers to retaining hard copies of these documents.

67. See: https://everyonehome.org/wp-content/uploads/2016/02/Home-Stretch-Housing-Match-Packet-2.pdf.

Figure 4: Forms Required for Alameda County Permanent Supportive Housing Application



In fact, the City of Austin is already building such a digital wallet system, titled "MyPass." The MyPass system allows homeless individuals to upload official documentation onto a digital storage system. The app allows registered public notaries to create a notarized digital version of a document, and the individual residents can send the electronically notarized version of the document to relevant agencies as needed.

Figure 5 provides an illustration of the MyPass system.[68] The MyPass system functions differently than traditional digital identity systems. According to our stakeholder interviews, blockchain technology is only being used to notarize official government documents uploaded to the MyPass system. The City is not creating a unique identity for each individual person, and thus the City does not consider this program to be a digital identity system.[69]

Finally, a lack of physical identity documents can make it especially difficult for unhoused individuals to maintain comprehensive medical records. Unhoused residents are more likely to visit the emergency room for their health needs than housed residents. If no government-issued license is present when visiting an ER, physicians will have to treat the patient without being able to track down their medical history or prior diagnoses. This could lead to duplication in treatment, errors, and overtreatment.[70] In addition, many shelters in the Bay Area end up relying on word-of-mouth medical history of people experiencing homelessness

68. Source: City of Austin MyPass GitHub website, 2020. https://github.com/cityofaustin/mypass/blob/master/docs/MyPassOverview2020.png.

69. Since there is no agreed-upon definition of a digital identity, it is difficult to say whether the City of Austin's MyPass system is a digital identity or not.

70. Anjum Khurshid and Ashish Gadnis. "Using blockchain to create transactions for persons experiencing homelessness in America: A policy proposal." JMIR Research Protocols 6, no. 8 (March 2019). https://pubmed.ncbi.nlm.nih.gov/30839279/.

since there is no comprehensive history of medical services accessed.[71] Thus, a blockchain-based digital ID system can improve health outcomes for vulnerable populations who do not possess a physical ID.

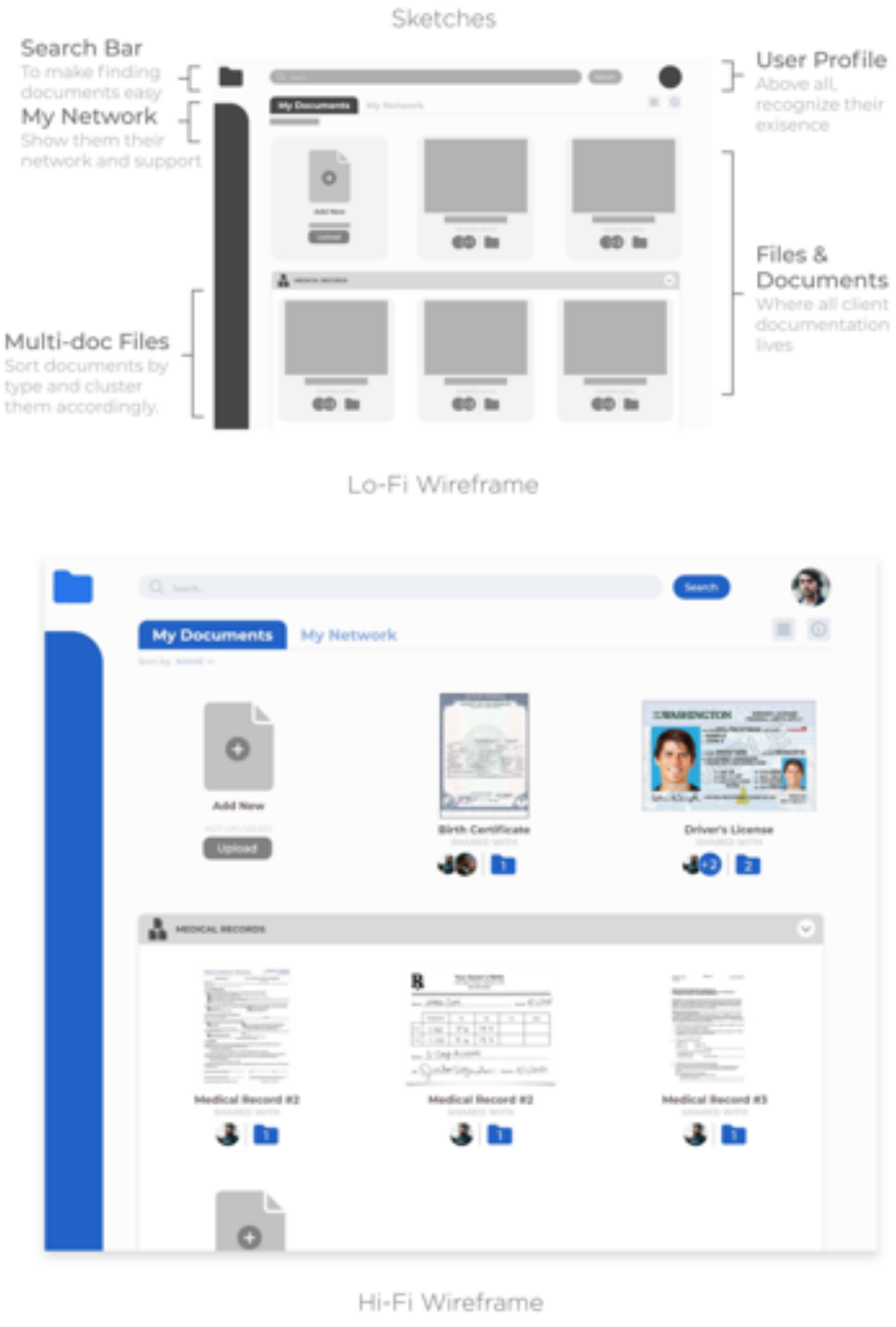


Figure 5: Overview of the City of Austin's MyPass Identity Storage System

71. Justine Humenansky (University of California, Berkeley), Personal Interview, July 2020.

Opportunity #2: Improve the sharing of health records across county lines

Blockchain technology can improve health outcomes for homeless individuals by improving the comprehensiveness of health records. In the State of California, homeless individuals are most likely to receive care from one of California's 21 public hospital systems. The California Association of Public Hospital and Health Systems estimates that these systems serve 123,000 homeless patients every year, or about 80% of California's homeless population.[72] These hospitals are run at the county-level and face significant data sharing challenges. Since homeless populations are more mobile and more likely to visit hospitals across county lines rather than one consistent provider, challenges of interoperability disproportionately affect them. A client-centered health records management system placed on a blockchain may improve health care for the homeless.

California's homeless may also benefit from a client-centered system because of the many health services they should ideally be receiving. Homeless individuals are likely to suffer from more complicated medical issues than those with permanent housing. For example, homeless individuals suffer from higher rates of mortality, poorer mental health, higher rates of substance abuse, and worse birth outcomes than non-homeless individuals.[73] Access to full medical records is especially critical to coordinate care for these residents.

What is the Whole Person Care program, and how can blockchain-based health records systems help?

The Whole Person Care program is a pilot of the State of California that aims to better coordinate health, behavioral, and social services for high-risk Medi-Cal recipients, including the homeless. The pilots encourage local regional agencies—including hospitals, social service organizations, and behavioral health providers—to coordinate care and "treat the whole person."

A critical aspect of this program is to better integrate data between all systems a homeless person encounters. This remains difficult because of traditional data silo and interoperability issues that have plagued health records for decades. A blockchain-based approach may allow individual clients to hold all these data on their own accounts, and transfer it easily to other providers when necessary. Essentially, a blockchain-based system might solve the data silo issues that sometimes prevent WPC programs from succeeding.

72. See: https://caph.org/memberdirectory/facts/.

73. Cheryl Teruya et al. "Health and health care disparities among homeless women." Women & Health 50, no. 8 (December 2009): 719-736. https://www.tandfonline.com/doi/full/10.1080/03630242.2010.532754?casa_token=qZb1xvsordAAAAAA%3AG-60VYPZSEI9E1yVIufRJQ8mARJCMLEqkXuoR7jldUQIUi2tirKxUxYlSXE9MHfKcisZypRoE5e2bw.

Indeed, improving this coordination among behavioral, physical, and social services has been an explicit goal of the state in recent years. Social service providers understand that solving the homeless problem will require a whole-person-centric approach. As such, the State of California has recently piloted the Whole Person Care program (WPC), which aims to better integrate services for vulnerable populations like the homeless. A key goal of WPC is to share data among various agencies, including behavioral health and social services agencies. In doing so, providers may be able to offer more comprehensive care that tends to the range of an individual's needs. Currently, agencies implementing the WPC are not considering blockchain technologies though it could theoretically improve services.

Though sharing data across multiple providers and sectors can be done through HIOs and agency-centered data sharing systems, a client-centered blockchain system may be better suited to solve data sharing issues. In fact, California HIO systems still have considerable room for improvement, and hospital systems have been unable to fully integrate health data with one another because of incomplete HIO participation (hospital systems are not always required to participate), implementation (often physicians must login to a separate system apart from their traditional EHR system to see records from other hospital systems, which is very cumbersome), data standardization (data is recorded in different formats depending on the hospital system), and more.[74] Moving to a client-centered health records approach may improve these issues, and may allow the state to better implement its WPC program. The University of Texas, Austin, is exploring how to integrate medical records on a blockchain platform so that individuals can more efficiently share their health records with various providers.

74. Walter Sujansky. "Promise and Pitfalls: A Look at California's Regional Health Information Organizations." California Health Foundation, January 2019, https://www.chcf.org/wp-content/uploads/2019/01/PromisePitfallsCARegionalHIO.pdf. For a complete list of challenges of current HIO systems, please see this report.

09 //
CHALLENGES

09 // CHALLENGES

Although blockchain-based identity and health records programs seem to hold promise for improving service provision and health care for the homeless, a few challenges remain. Research suggests that three key issues may impede the potential of these technologies: (1) complications of user authentication that make it difficult for the homeless to access these services; (2) political will, as the state and federal government have already spent millions of dollars improving health-record interoperability through HIOs; and (3) concerns about data safety and citizen confidence over the long-term.

Challenge #1: User authentication

Perhaps the most immediate issue with blockchain-based identity and health records management systems is that they do not solve a key problem for the homeless: retaining a physical ID or password. Blockchain-based identity and health records management systems still need a user to "log on" to a system when using the service.[75] Users can login via:

1. **A physical device** such as a smart chip-card, mobile phone, or security token
2. **A password**, pin, or verified sequence
3. **Biometrics** such as a fingerprint scan, retina scan, facial recognition scan, or voice recognition scan

Homeless individuals who have trouble retaining a physical ID will also have trouble retaining a smart card, password or pin. If a homeless individual loses the smartcard or password, they will likely need to visit a government office for a replacement, which negates the usefulness of this technology in the first place. The blockchain technology companies interviewed for this project are aware of this issue, and because of it, many are pivoting to using biometrics for login.

75. In computer science, these login systems are referred to as private key management.

Biometrics have their own challenges, however. All of the service providers identified for this project were unconvinced that their homeless clients would agree to use biometrics for logging into a system. According to them, homeless individuals associate use of biometrics with law enforcement, since (currently) the only major use of biometrics in US government entities is through fingerprinting by police or other law enforcement agencies. As many of these homeless individuals have a distrust of law enforcement, they may be reluctant to provide biometrics for login. When the City of Austin surveyed its homeless residents as part of the MyPass project, they found that 80% of those surveyed would be unwilling to register their biometrics for a digital ID or health records system.[76]

It is important to note that using biometrics for private key management does not mean the government will have access to every individual's biometric information. This sensitive information will still theoretically be controlled by the individual. However, given that most users may not have an in-depth understanding of blockchain technologies, it is perhaps unlikely that users will be convinced of the safety of biometrics without additional user education.

Challenge #2: Political feasibility given existing solutions

Another hurdle to implementing blockchain-based digital ID and health records management systems is that numerous solutions have already been sponsored by the state to solve this issue. These include homeless management information solutions (HMIS) and health information exchange organizations (HIOs).

As mentioned above, the state is mandated by the federal government to have a homeless information management system (HMIS). HMIS systems collect client-level data to coordinate data across different homelessness services agencies. HMIS systems can be used to store various identity and government documents for individuals that can be accessed by multiple providers. For example, say a homeless individual receives food stamp benefits through Alameda County, California. When signing up for a food stamp/EBT card, a case worker will scan his or her physical identification and store that ID on the HMIS system. If the individual moves to San Francisco County, the individual will need to transfer his or her benefits to San Francisco (SF) County's EBT system. Even if he or she has lost the ID in that period of time, they can just state their name and a SF County case worker will pull up the scan of the physical ID on the HMIS system, verify the person's identity with a few questions (such as date of birth), and easily transfer the benefits over. In fact, as stated by a U. of Texas, Austin researcher piloting the use of blockchain

76. Adam Wiedemann (City of Austin MyPass), Personal Interview, February 2020.

health records systems in homeless populations, "From the service provider perspective, blockchain technology is most useful for documents that are not currently stored on the HMIS database or for client personnel's use to keep track of future appointments and pending documents needed for services. The blockchain technology platform may, for the time being, complement other existing databases or information systems, allowing us to add new features that are hard to establish using legacy systems."[77] However, HMIS systems also suffer from interoperability issues caused by different data formats used by different counties. Thus, a blockchain-based identity system might still have some value for streamlining provision of public services.

In addition to HMIS systems, the state has invested heavily in setting up health information exchange organizations (HIOs) to better integrate data across different healthcare systems and among physical health, behavioral health, and social service providers. California currently has nine regional HIOs that serve just over half of the state population.[78] Recently the state has launched an initiative called the California Health Information Exchange Onboarding Program (Cal-HOP) that aims to increase the number of providers using HIOs. This initiative provides almost $50 million to encourage Medi-Cal providers to use HIOs.[79] Supplementing this state-wide effort has been considerable movement within counties to strengthen data sharing among providers. Los Angeles County, for example, is regarded as a leader in strengthening data sharing among health agencies through its regional HIO, called LANES. As the state has already spent millions of dollars as well as considerable political capital to strengthen HIOs, it is unclear how willing agencies will be to try a completely new (and untested) solution to the problem of health data interoperability through blockchain technology.

Challenge #3: Questions about data security in years to come

The last challenge with building blockchain-based identity or health records management systems for vulnerable populations is lack of clarity regarding the long-term security of data placed on the blockchain. Some believe that technology over the next fifty years will progress enough that data on blockchain will be compromised.

---

77. Anjum Khurshid, Vivian Rajeswaren, and Steven Andrews. "Austin's MyPass Initiative: A Pilot Study of Using Blockchain Technology for the Homeless." Journal of Medical Internet Research (April 2020). https://www.jmir.org/2020/6/e16887/.

78. Walter Sujansky. "Promise and Pitfalls: A Look at California's Regional Health Information Organizations." California Health Foundation, January 2019. https://www.chcf.org/wp-content/uploads/2019/01/PromisePitfallsCARegionalHIO.pdf.

79. See: https://www.dhcs.ca.gov/provgovpart/Pages/Cal-HOP.aspx.

Since blockchains are immutable and distributed, secure data such as medical information cannot be placed on the blockchain. Instead of placing personal information on the blockchain, cryptographic hashes of information are used to store data. Cryptographic hashes are unique sequences of letters and numbers that correspond to a piece of data. That is, if you take a piece of medical information, you can hash it and turn it into a random set of numbers and letters of fixed length. Because hash functions are extremely hard to reverse engineer, they have been used to store sensitive information like health records on blockchains.

However, it is widely acknowledged that cryptographic hash functions will be reverse engineered in the coming decades.[80] Though most computer scientists do not believe that hash functions will be reversed in the next ten to twenty years, many believe that advances in quantum computing will allow them to be reversed in the next thirty to fifty years. This is consequential for health or genetic data that could have repercussions for a patient's children or grandchildren. In our interviews, the California state officials stated that they would be wary of implementing a blockchain-based digital ID solution if it meant that data for sensitive populations may eventually be compromised or if citizens do not have confidence in data security. Thus, policymakers should be cautious about supporting solutions that could compromise data privacy.

Still, hash functions themselves may become stronger over the next two decades. Though quantum computing may allow hash functions to be reverse engineered, computer scientists may create technologies to better protect these data. In addition, some of these issues could be resolved using data governance and retention policies. Thus, data security on blockchains may neither be guaranteed nor ruled out.

What are cryptographic hash functions?

Cryptographic hash functions are normally how sensitive information is stored on a blockchain. Cryptographic hash functions take a piece of data—such as a Social Security number—and produce a new, unique sequence of letters and numbers that correspond to the original data. This newly hashed data can then be stored and used to verify the user without letting others know what the underlying data is. Strong hash functions are not easily reversible. It should be nearly impossible to discover the original piece of data through its hash.

80. Eduardo Beltrame and Dylan Bannon (California Institute of Technology), Personal Interview, April 2020.

10 //

DISCUSSION AND FUTURE RESEARCH QUESTIONS

10 //

DISCUSSION AND FUTURE RESEARCH QUESTIONS

Overall, blockchain technology may help vulnerable populations to access public services and manage health records. Blockchain-based identity solutions could reduce the administrative burdens of receiving public benefits, especially for populations like the homeless who face challenges in retaining IDs and government documents. In addition, blockchain-based health records management systems could help medical providers have more complete information on homeless patients, and may solve issues related to interoperability of health records that have plagued EHRs for years.

However, these benefits will not be realized until technologists make progress on the problem of user authentication. At this time, it seems as though biometrics may be the only option for making blockchain-based identity or health records systems usable for vulnerable populations. The government will likely need to spend considerable effort educating all participants on protocols for storing and accessing biometric information and how blockchain systems work in order to gain sufficient adoption from homeless populations to use these systems.

Even if the user authentication problem is solved, numerous privacy, security, and political considerations may remain barriers to realizing the benefits of blockchain technology. First, the long-term uncertainty of the security of cryptographic hash functions may make it unappealing for governments to adopt blockchain technology for health records management systems. In addition, the state of California has already spent tens of millions of dollars in improving data sharing between health care providers and social service organizations through their HMIS and HIO systems. Thus, it is unclear whether leaders will gain sufficient political will to invest in a relatively risky and expensive blockchain technology pilot when existing solutions are available.

Blockchain technology experts still need to better articulate the incremental value of this technology over traditional database systems. Stakeholder interviews made it clear that many government agencies and nonprofit organizations do not currently understand the added benefit of blockchain

systems. In fact, our survey with state chief information officers found that the majority of the technology departments felt their staff were relatively unfamiliar with blockchain technologies or their utility. The City of Austin's MyPass team—one of the only public entities that has tried to implement a pilot digital ID-like system for the homeless in the U.S.— also believes there are very few, limited uses of blockchain technology in the public sector. Private entities must do a better job of explaining the practical value of these technologies to the public sector. Questions that should be answered in the future include:

- If a centralized entity such as a state or city government is running a blockchain-based digital identity or health records management system, what is the added value of using a private or permissioned blockchain over a traditional database system?

- What features of blockchain-based identity or personalized health records systems can be implemented with a traditional database system?

- What are the costs of implementing these technologies, including software, hardware and staff training?

- How do existing and new privacy regulations—including HIPAA and the California Consumer Privacy Act—affect what can be written onto the blockchain? How do these new regulations affect data preservation and deletion rules?

- Is there sufficient alignment from state technology departments to implement this technology?

Last, we must note that although blockchain-based digital identities or health records management may not immediately benefit the homeless population in California, it may still be worth considering the technology based on benefits for other citizens. Blockchain-based digital IDs such as those used in Estonia have greatly streamlined government processes for the average citizen. However, policymakers should remain aware of how these technologies affect vulnerable populations like the homeless and design such systems for the benefit of all Californians.

ACKNOWLEDGMENTS

For their detailed review of this report in addition to expert interviews, we thank:

- Eduardo Beltrame (Caltech)
- Dylan Bannon (Caltech)
- Justine Humenansky (UC Berkeley)
- Adam Wiedemann (City of Austin's MyPass) system.

For lending their expertise through interviews, we thank:

- Eric Bryant (NetObjex)
- Daniel Culotta (City of Austin MyPass)
- Cynthia Castillo (Office of Senator Hertzberg, State of California)
- Mary Dwyer (Blockchain for Social Impact)
- Yorke Rhodes III (Blockchain for Social Impact)
- Susia Batt (Blockchain for Social Impact)
- Amanda Stanhaus (Blockchain for Social Impact)
- Wilma Lozada (Alameda County Healthcare for the Homeless)
- Frans Tjallingii (New Leaf Project Foundation)
- Raymond Cheng (University of San Francisco)
- Michelle Schneidermann (California Health Care Foundation)
- Sean Manion (ConsenSys Health)
- Jonathan Holt (ConsenSys Health)
- Anjum Khurshid (University of Texas, Austin Dell Medical School)
- Robert Rebitzer (Manatt Health)
- Jonah Frohlich (Manatt Health)

We thank Gabriela Montano (California Government Operations Agency), Stuart Drown (California Government Operations Agency), and Orit Kalman (California State University - Sacramento) for facilitating meetings that resulted in some of the information referenced in this report.

We thank Ryan Olson for designing the report.

Finally, we thank CITRIS & the Banatao Institute, Karin Bauer and the University of California, Berkeley's University Blockchain Research Initiative, and Ripple for funding.

APPENDIX: A NOTE ON OPPOSINING VIEWS

We solicited reviews of the report from individual experts, some of whom disagreed with aspects of our conclusions. In the interest of transparency, we provide a summary of the opposing views here.

- Two reviewers disagreed with the California Blockchain Working Group's definition of blockchain and felt it is too broad. Using the official Blockchain Working Group definition, they argue, allows for any technology that uses cryptographic authentication of history (such as GitHub) or Merkle Trees (such as Amazon Web Services) to be classified as a blockchain technology. More information about how the California Blockchain Working Group arrived at their definition can be found in the final report.[81]

- One reviewer stated that traditional database systems could be used to implement personalized health records. That is, the characteristics dis-cussed here regarding use of blockchains to improve health data interoperability can also be realized with traditional database systems. If true, traditional databases could be preferable to blockchain systems since a variety of off-the-shelf products could be customized for healthcare organizations.

- One reviewer noted that there are differences between using blockchain technologies as a data repository (such as Polkadot and factum) and using blockchain technologies as a distributed public key infrastructure (such as Ethereum). This reviewer noted that our report focuses on the first group (blockchain as a data repository), even though the majority of blockchain use cases would be categorized in the second group (blockchain as a distributed public key infrastructure). This distinction affects many of the data security implications we discussed in this report, as well as the blockchain use cases.

---

81. "Blockchain in California: A Roadmap." California Blockchain Working Group, July 2020. https://www.govops.ca.gov/wp-content/uploads/sites/11/2020/07/BWG-Final-Report-2020-July1.pdf.

Finally, we note that many of the experts we interviewed had differing opinions on blockchain overall. Some believed that blockchain technologies offered no substantial improvements over traditional database systems, while others strongly believed that this technology could revolutionize systems for digital identity and health records. Blockchain research and development in the coming years will likely shed more light on these questions and cautions.