2022

# Self-Sovereign Identity and the Decentralized, Consent-Based Model

Ryan Greene

# Self-Sovereign Identity &

# The Decentralized, Consent-Based Model

Author: Ryan Greene
Published Fall 2022

**Introduction:**

The centralized third-party authentication model for digital identity validation is obsolete in light of newer and more secure means of ensuring accurate digital identification. Governments, private organizations, and citizens should be encouraged to explore the means by which they can maximize the latest in digital developments to protect themselves and their online identities. California should begin to implement the precepts of the decentralized Self-Sovereign Identity (SSI) model, which is superior to its predecessor in its simplicity, as it requires only three things to validate a digital identity: (1) a blockchain which has the information necessary to satisfy the consensus algorithm ensuring adequate replication across the network nodes; (2) verifiable credentials; and (3) decentralized identifiers.[1] Because this system is predicated on a trustless Proof of Work (PoW) model, at present, blockchains are practically immutable, thus making it impossible to falsify or forge information on them. The use of cryptographic hash functions ensures that the security of each block of data is independently secured from one another, and ultimately known only to the controller and owner of the information: the user. California should join other state and national governments in the research and implementation of SSI-compliant models of governance to better protect and support the needs of its citizenry in an increasingly digitized world.

Part I of this paper explains the current centralized model of the internet and digital identity. Part II addresses the history of digital identity and its growth toward self-sovereign identity. Part III of this paper analyzes digital identity and U.S. state laws while Part IV highlights various use cases from the United States and Estonia. Part V of this paper recommends how the California DMV can learn from these use cases and implement its own

[1] Robert MacDonald, *What is Self-Sovereign Identity*, 1KosMos, April 29, 2022, https://www.1kosmos.com/identity-management/self-sovereign-identity/

systems of SSI-compliance. Lastly, Part VI summarizes the conclusions drawn from the aforementioned sections and best practices for California and the DMV.

## I. Overview of the Centralized Model of Digital Identity

Centralization is the concept by which the modern internet operates. An example of a centralized system is a social media platform, such as Facebook, Google, or Twitter, which use systems of controls to govern their platform and their users. Centralization gives those in positions of authority near-total control over the data on their platforms. When a user accesses a social media site, that company has complete control over the different aspects of their features including the ability to decide who can and cannot join the platform. Initially, this would seem benign. In the long run, however, private entities could decide the authentication and validation of a digital identity and a user would be without recourse if the authenticator decided that the entity requesting the digital identity was not themself. This would further perpetuate any damage a faux identity would be able to do online, as they would be said to have the explicit backing of any such authenticating organization.

For example, in 2015 Yahoo became aware of a data breach relating to their email service resulting in one of the largest email breaches in history.[2] This meant that nearly 500 million people were subjected to the whims and decisions of a person who had gained access to those accounts by falsely-identifying themselves as the user.[3] The malicious actor gained access to everything Yahoo had gathered about their users, including the contents of emails, the senders and receivers for those emails and the dates and times those emails were sent. Worse still, the hackers gained access to Yahoo's records, including sign-up information like a user's full name,

[2] Jamie White, *Yahoo Announces 500 Million Users Impacted by Data Breach,* Yahoo! News, February 2021, https://www.lifelock.com/learn/data-breaches/company-data-breach
[3] *Id.*

nationality, date of birth, and any other information necessary to register on the platform.[4] As discussed in Part V below, this model of data management and security is failing both users and organizations. The need to reevaluate and pivot away from the centralized model is an increasingly expensive proposition to ignore.

## II. The History & Implementation of Self-Sovereign Data

### A. The Concept of a Digital Identity Developed Alongside the Internet:

Identity is a uniquely human concept. It is that ineffable "I" of self-consciousness, something that is understood worldwide by every person living in every culture. As René Descartes said: *Cogito ergo sum* — I think, therefore I am.[5]

In modern societies, such simple rhetorical devices fall flat in the face of legally recognized entities which can issue identification documents and other forms of validation. But the conflation of state issued credentials and identity are inherently problematic. If identity and the validating credentials for that identity were merged into one, a person could theoretically lose his very identity if a state revokes his credentials or even if he just crosses state borders. [6] Should Descartes choose to revise his infamous turn of phrase, he may instead proffer: *Puto sed non sum* — I think, but I am not.

Identity in the digital world is trickier still. It suffers from the same problem of centralized control, but it is simultaneously disparate: identities are piecemeal, differing from one Internet domain to another. As the digital world becomes increasingly connected to the physical world, it also presents a new opportunity; it offers the possibility of redefining modern concepts

[4] *Id.*
[5] Rene Descartes, *Discourse on Method*, 1637.
[6] Christopher Allen, *The Path to Self-Sovereign Identity*, April 25, 2016, http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

of identity. It might allow us to place identity back under our control — once more reuniting identity with the ineffable "I."[7]

In the Internet's early days, digital identities were solely controlled and administered via a single authority such as the Internet Assigned Numbers Authority, which coordinates the global Domain Name System Root, IP addressing, and other internet protocol resources.[8] Alternatively they could be managed via hierarchies such as those created by the Internet Corporation for Assigned Names and Numbers, which continues to organize and arbitrate domain names.[9] While these authorities were useful in their way, they represent the quintessential danger of centralization: users have no recourse and no alternative should they receive an unfavorable determination regarding their request for identity validation.

As the internet has grown and matured, the balkanization of digital identities has too. The previous system of hierarchies gave birth to Certificate Authorities, which today issue Secure Sockets Layer (SSL) certificates used to validate digital identities.[10] But this forces users to utilize multiple digital identities on a variety of sites so that they might access any given site; in so doing, users must agree to forgo *any* control over their information. This agreement to forgo ownership of their data, enabling companies to operate at a profit, creates a perverse incentive whereby the very thing which makes us human, our identity, on the internet makes us subject to becoming commercialized.[11]

---

[7] Christopher Allen, *supra.*
[8] The Internet Assigned Numbers Authority, *An Introduction*, https://www.iana.org/about
[9] The Internet Corporation for Assigned Names & Numbers, *Who We Are,* https://www.icann.org/resources/pages/beginners-guides-2012-03-06-en
[10] Secure Sockets Layer, *What is a Certificate Authority*, December 2021, SSL.com, https://www.ssl.com/faqs/what-is-a-certificate-authority/
[11] Saheed A. Gbadegeshin, *The Effect of Digitalization on the Commercialization Process of High-Technology Companies in the Life Sciences Industry*, Technology Innovation Management Review, January 2019, https://timreview.ca/sites/default/files/article_PDF/Gbadegeshin_TIMReview_January2019.pdf

At the turn of the new millennium, the internet changed in a way which is still affecting the use and organization of the internet today. It moved away from a single authoritative entity and towards one of federated identity. In the federated identity model, the new process of digital validation permitted a user to access many websites or platforms with a single identity.[12] Today these services are known as Single Sign On (SSO). When the SSO is properly authenticated, it allows a user to access a multitude of sites or content within sites without needing to validate their identity each time.[13] These improvements to digital validation and identification are clear, given the end user's ease of use and simplification of identity verification. However, the federated system still fails to resolve the fundamental issues regarding the lack of user-control and digital identities across the internet.[14]

The Internet evolved again in the mid 2000's into a user-centric identity model in which an individual or administrative organization controls site access across multiple authorities. This change gave rise to a new school of thought with respect to digital identity and data accumulation. With a focus on the minimization of data collection and decentralization of identity verification, Ken Jordan and co-authors penned *the Augmented Social Network,* in which they posited that the internet of tomorrow could be purpose-built to include concepts built into the architecture of the internet, such as digital identity and trust.[15] Organizations like the Identity Commons have expanded on this concept, advocating for the facilitation, support, promotion, and creation of an open identity layer for the Internet, one that maximizes control, convenience,

---

[12] Chadwick, D.W., *Federated Identity Management*, In: Aldini, A., Barthe, G., *Foundations of Security Analysis and Design V*, 2009, https://doi.org/10.1007/978-3-642-03829-7_3

[13] Sebastian Peyrott, *What Is and How Does a Single Sign-On Authentication Work,* Auth0 Blog, February 4, 2022, https://auth0.com/blog/what-is-and-how-does-single-sign-on-work/

[14] *Id.*

[15] Ken Jordan, Jan Hauser, & Steven Foster, *The Augmented Social Network: Building Identity & Trust Into the Next-Generation Internet*, First Monday, August 2003, https://firstmonday.org/ojs/index.php/fm/article/view/1068/988

and privacy for the individual while encouraging the development of healthy, interoperable communities.[16]

Today, the focus for organizations and advocates like the Identity Commons and Ken Jordan is the evolution of digital identity and the returning of control across the Internet to the user. In this stage of the Internet's development, decentralized concepts such as blockchain form the core of SSI-systems. A decentralized SSI compliant Internet is understood to be the next wave of digital identity management.[17] It requires that the user be the center of that identity's administration. In addition to user-control, these data sets must be interoperable across the Internet, with the user's consent, but also autonomously. Critically, an SSI must *also* be distributed. By its terms it cannot be kept or stored in a single place, for otherwise it would only be a portable centralized system.

This is where blockchains, which are cryptographically secured and mathematically assured, provide individual users with an opportunity to take control of their digital identity and to claim ownership over it. In this environment, a trustless Proof of Work (PoW) model ensures that the data presented is genuine.[18] This is effectuated through a decentralized consensus mechanism that requires members of a network to expend effort solving an arbitrary mathematical puzzle.[19] This process forms the consensus mechanism that allows anonymous

[16] The Identity Commons, *Purpose & Principles*, https://www.idcommons.org/organization/purpose-and-principles/
[17] Alastair Johnson, *EIDAS 2.0 Turns to Self-Sovereign Identification to Bring Users Ownership & Control*, Forbes Magazine, July 5, 2022, https://www.forbes.com/sites/alastairjohnson/2022/07/05/eidas-20-turns-to-self-sovereign-identification-to-bring-users-ownership-and-control/?sh=7cf6014d7f07
[18] Alyssa Hertig, *What is Proof-of-Work,* CoinDesk, March 9, 2022, https://www.coindesk.com/learn/2020/12/16/what-is-proof-of-work/#:~:text=Proof%2Dof%2Dwork%20is%20the,at%2012%3A25%20p.m.%20PST
[19] *Id.*

entities in decentralized networks to trust the results of the algorithmic puzzle without even knowing the actual identity of the user validating the transaction.[20]

It is critical that the individual is protected, even in a trustless system. Bad actors in a centralized system can attempt to exploit known cybersecurity weaknesses to gain entry into systems in which they are not permitted. By contrast the PoW model requires that for an entity to access information stored on the blockchain, they must first validate their identity through the consensus mechanism described above. This increase in security and privacy heightens the accuracy and verifiability of the data exchange while ensuring critical information and transactions are not impermissibly accessed.[21]

To create a self-sovereign identity within this environment, a user or organization must establish three elements: (1) a blockchain with the information necessary to satisfy the consensus algorithm ensuring adequate replication across the network nodes; (2) verifiable credentials; and (3) decentralized identifiers.[22] The first element begins with the implementation of blockchains which are further discussed below. The second element is credentials which can be verified and is already something utilized in daily life (*e.g.,* driver's license, passport, birth certificate, etc.). These credentials need only to be converted into a digital copy which simply acts as a digital watermark for the data. When combined with a cryptographic key it would ensure that the actual data is never revealed while the validation of that data is completed instantaneously.[23] To complete that instantaneous transaction, organizations must have the third element established in

---

[20] E. Napoletano & Benjamin Curry, *Proof of Work Explained*, Forbes Magazine, April 8, 2022, https://www.forbes.com/advisor/investing/cryptocurrency/proof-of-work/

[21] Allan Thompson, *The Impact of Self-Sovereign Identity on the Cybersecurity World*, Avast Blogspot, April 12, 2022, https://blog.avast.com/impact-of-self-sovereign-identity-on-cybersecurity

[22] Jimmy Snoek, *Decentralized Identifiers a Beginner's Guide*, Tykn, 2021, https://tykn.tech/decentralized-identifiers-dids/#What_are_Decentralized_Identifiers

[23] Tim Olsen, *Blockchains For Trusted Security Labels*, IBM Blockchain, November 5, 2019, https://www.ibm.com/blogs/blockchain/2019/11/blockchain-for-trusted-security-labels/

the decentralized identifiers. These are global, unique, and persistent identifiers.[24] These identifiers allow for the creation of unique, private, and secure peer-to-peer connections between two parties. Moreover, their decentralized nature makes credentials always available for verification while each party, an individual or organization, can create as many different identifiers as they wish which ultimately allows a single user to use a single credential for any transaction or interaction without a need for a second or alternative identification method.[25] This individualization of identification in fact only heightens the security around the user, as using separate identifiers for different digital relationships and contexts prevents data correlation.[26] Lastly, these identifiers are entirely controlled by the identity owner. They are independent of centralized registries, authorities, or identity providers.[27] Thus, to establish a genuine SSI model, an organization must implement the three elements of (1) blockchain technology; (2) verifiable credentials; and (3) decentralized identifiers.

### B. Element One: The Foundation of Blockchains & Distributed Ledgers

To establish an SSI, there must be sufficient technology and ability to form a foundation which is sufficiently replicable while also sufficiently fast to maintain use of service throughout the validation process. To start, there are already several types of blockchains which could serve as an avenue for this kind of sensitive and highly private information.[28] Generally speaking these blockchains are private, decentralized, and only the user holds the cryptographic key to access the information stored on the blockchain.[29]

---

[24] *Id.*
[25] Allan Thompson, *supra.*
[26] *Id.*
[27] Jimmy Snoek, *supra.*
[28] Joe Liebkind, *Five Blockchain Platforms for Better Use of Data*, Investopedia News, October 28, 2021, https://www.investopedia.com/tech/5-blockchain-platforms-better-use-data/
[29] *Id.*

Blockchain is the technology underlying the concept of SSI. There are two types of blockchains, public and private. A public blockchain is open to anyone who wants to join and has the computing power to do so, whereas a private blockchain requires an invitation from the blockchain owner and must validate the identity of the user by the network starter or through rules established by the network starter.[30] Both kinds of blockchains permit the creation and proliferation of decentralized databases across "nodes" or other computers, which provide control over the evaluation of data between entities. This is accomplished through peer-to-peer networks relying on consensus algorithms, like PoW, which provide assurances as to the replicability to other nodes on the network. Put simply, blockchains allow users around the world to access the same source of information, with every change, edit, alteration, and adjustment laid bare for all to see.[31]

This is executed without ever revealing the underlying data to users or verifiers. This is possible because of the "Zero Knowledge Proof," which exchanges and registers the actual user data and allows two different actors, the user and the verifier, to exchange the ownership of a piece of data, without revealing the data itself.[32] The math, probability and cryptography behind this technology makes its applications useful. For example, it would allow a person to prove the ownership of a credential to the verifier, such as a driver's license, without revealing the initial

[30] Praveen Jayachandran, *The Difference Between Public & Private Blockchain*, IBM Blockchain Explained, May 31, 2017, https://www.ibm.com/blogs/blockchain/2017/05/the-difference-between-public-and-private-blockchain/
[31] Thomas Buocz, *Bitcoin & the GDPR: Allocating Responsibility in Distributed Networks*, Computer Law & Security Review Journal, December 7, 2018, https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3297531_code2785217.pdf?abstractid=3297531&mirid=1&type=2
[32] Xiao-Jun Wen, *Blockchain Consensus Mechanism Based on Quantum Zero-Knowledge Proof*, November 23, 2022, https://doi.org/10.1016/j.optlastec.2021.107693

identifying information.[33] In this instance, a person could use a QR code which could be scanned by a store employee to validate that the person is of-age and is allowed to purchase alcohol.

These proofs are predicated on the use of cryptographic hash functions, algorithms which take an arbitrary quantity of data inputs (*e.g.,* a verifiable credential such as the information on a driver's license) and then create an output in response to those inputs which is known as a "hash."[34] Once the hashing is complete, the data can be safely stored and the password to that data is no longer needed to validate the user's identity.[35]

This system of zero knowledge proofs and trustless confirmation of transactions offers many advantages over the current username and password combination, including: one-way functioning, which makes reconstruction of the hash nearly impossible; the avalanche effect, in which one change along the chain causes every block to change in response; non-predictability, meaning hash values are non-predictable from the password; and collision resistance, which makes finding two passwords that hash the same enciphered text exponentially more difficult.[36] Each of these technological evolutions serve to further advance protections and privacy for users and their data.[37]

It is necessary to highlight the real and theoretical shortcomings of this technology and its impacts if it were to be exploited. There is a single known real-world risk to the use of public blockchains and two known risks associated with the systems which blockchain employs. First,

---

[33] Kai Wagner, *Self-Sovereign Identity' Position Paper*, Identity Working Group of the German Blockchain Association, October 23, 2018, https://jolocom.io/wp-content/uploads/2018/10/Self-sovereign-Identity-_-Blockchain-Bundesverband-2018.pdf

[34] ByBit Learn, *Explained: What is Hashing in Blockchain*, ByBit Learn, December 17, 2020, https://learn.bybit.com/blockchain/what-is-hashing-in-blockchain/

[35] Anthony Scabby and Anil Pereira, *Using Hashing to Maintain Data Integrity in Cloud Computing Systems*, Southwestern Oklahoma State University, 2021, https://bulldog.swosu.edu/administrative-services/sponsored-programs/fair/files/scabby.pdf

[36] Synopsys Editorial Team, *What are Cryptographic Hash Functions*, Synopsis.com, December 10,2015, https://www.synopsys.com/blogs/software-security/cryptographic-hash-functions/#:~:text=A%20cryptographic%20hash%20function%20is,used%20to%20verify%20the%20user

[37] Jinyue Song, *How Blockchain Chan Help Enhance the Security & Privacy in Edge Computing*, October 31, 2021, https://doi.org/10.48550/arXiv.2111.00416

the direct threat to a blockchain is known as a fifty-one percent (51%) attack. It is considered inapplicable to private blockchains because of the sole-source of control which governs the private blockchain; whereas public blockchains are controlled across a nodule-system, open to anyone who seeks to join, thus allowing a malicious actor to gain control over more than their own node.[38] This attack requires that a bad actor take over 51% of all nodes to change or use the information written on a blockchain.[39] For comparison, this method is akin to the "brute-force" method employed by hackers against centralized systems. Just as with the brute-force attack, users subjected to a 51% attack are aware of the malicious action and should they desire to, may disconnect from the internet and flag the event as a bad actor.[40] These kinds of attacks are possible on small-scale blockchains but are nearly impossible as the blockchains scale up, as the malicious actor would need exponentially more computing power to control national or international blockchains.

The technologies which support blockchains, however, are just as susceptible to bad actors as their centralized forerunners because they are both tethered to human action as the source of the error. For example, "creation errors" are errors in a blockchain's execution of a smart contract.[41] The risk here is that the smart contract can become vulnerable to malicious action when the terms of the smart contract's execution are ambiguous or vague.[42] In the real world, this is no different from a contract which is poorly worded and results in unfavorable terms. However, unlike in the physical world, a creation error can be quickly resolved when

---

[38] Fredy Andres Aponte-Novoa, *The 51% Attack on Blockchains: A Mining Behavior Study*, Institute of Electrical & Electronics Engineers, October 20, 2021, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9567686
[39] Digital Currency Initiative, *Digital Currency Initiative & 51% Attacks*, MIT Media Lab, January 2020, https://dci.mit.edu/51-attacks
[40] *Id.*
[41] Shabna Madathil Thattantavida & Sai Kanduri, *Best Practices for Debugging & Error Handling in an Enterprise-Grade Blockchain Application*, IBM Developer Blog, March 24, 2022, https://developer.ibm.com/blogs/debugging-and-error-handling-best-practices-in-a-blockchain-application/
[42] *Id.*

identified by providing clarifying guidance to the smart contract to better execute its task.[43] The second known risk to blockchain implementation is insufficient security.[44] Because blockchains themselves are secure, there have been many reported breaches of entities which employ the use of blockchains, such as cryptocurrency exchanges.[45] However, these breaches in many cases have been as a result of a failure to properly secure and protect the network from external threats and bad actors.[46] Therefore, just as with creation errors, human error or complacency pose more risks to blockchains than the blockchains themselves.[47]

Alternatively, the theoretical risks to blockchains are not insignificant. For the time being, these threats are speculative, but could become at-risk should quantum computers[48] or optimized hashing tables[49] become commonplace. These risks are also a threat in a centralized system of digital identity and therefore should not be seen only as a threat to an SSI-compliant system.[50] The final theoretical risk to blockchains are "past-known collisions," which when charted across enough time and data can help a malicious actor to better guess at the underlying algorithm employed by the particular blockchain in ensuring security.[51] Each of these risks are means by which entities would seek to use the mathematically-immutable nature of a blockchain against

---

[43] *Id.*
[44] Edgar Palomino, *A Glance at the Security of Blockchain Technology*, American University, July 14, 2022, https://www.american.edu/sis/centers/security-technology/a-glance-at-the-security-of-blockchain-technology.cfm
[45] *Id.*
[46] Edgar Palomino, *supra.*
[47] *Id.*
[48] Avinandan Banerjee, *Blockchain vs. Quantum Computing: Is Quantum Computing the Biggest Threat to Crypto*, Blockchain-Council.org, 2021, https://www.blockchain-council.org/blockchain/blockchain-vs-quantum-computing-is-quantum-computing-the-biggest-threat-to-crypto/
[49] Jinhua Fu, *Security A Study on the Optimization of Hashing Algorithm Based on PRCA*, Security and Communication Networks, Vol. 2020, Article ID 8876317, September 14, 2020, https://doi.org/10.1155/2020/8876317
[50] Michaela Lee, *Quantum Computing & Cybersecurity*, Harvard Kennedy School Belfer Center, July 2021, https://www.belfercenter.org/sites/default/files/2021-07/QCSecurity.pdf
[51] David Derler, *Fine-Grained & Controlled Rewriting in Blockchains: Chameleon-Hashing Gone Attribute-Based*, The Network and Distributed System Security Symposium, February 2019, https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02A-3_Derler_paper.pdf

itself to crack its cryptographic system.[52] These risks, because of the size of computing power required to employ them, are almost certain to originate from a state-sponsor and not from individual actors or groups of actors.[53]

### C. Element Two: The Attestation & Verifiable Credentials

A verifiable credential protocol, as defined by the World Wide Web Consortium (W3C) is in essence the process for the digital watermarking of claims data through a combination of public key cryptography and privacy-preserving techniques to prevent correlation.[54] This process means that not only can physical credentials safely be turned digital, but also that holders of such credentials can selectively disclose specific information from this credential without exposing the actual data (*e.g.*, showing a QR code for scanning to validate age of a person) and third-parties are instantly able to verify this data without having to call upon the issuer.[55]

The three components required to establish a valid verifiable credential are: (1) metadata; (2) claims; and (3) proofs.[56] Metadata is cryptographically signed by the issuer. It "describe[s] properties of the credential, such as the issuer, the expiry date and time, a representative image, a public key to use for verification purposes, the revocation mechanism, and so on."[57] Claims are statements made about a subject (*e.g.,* John was born on April 1, 2000), while proofs are data about the person (*e.g.,* an identity holder like John) that allows others to verify the source of the data (*e.g.,* the issuer), validates that the data belongs to you (and only you), that the data has not

---

[52] Stuart Madnick, *Blockchain Isn't as Unbreakable as You Think*, MIT Sloan Management Review, November 2019, https://sloanreview.mit.edu/article/blockchain-isnt-as-unbreakable-as-you-think/
[53] Cynthia Dion-Schwarz, *Terrorist Use of Cryptocurrencies*, the Rand Corporation, 2019, https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3026/RAND_RR3026.pdf
[54] Nate Otto, Sunny Lee, Brian Sletten, Daniel Burnett, Manu Sporny, & Ken Ebert, *Verifiable Credentials Use Cases*, W3C Working Group, September 2019, https://www.w3.org/TR/2019/NOTE-vc-use-cases-20190924/
[55] Khalid Maliki & Jimmy J. P. Snoek, *Verifiable Credentials: The Ultimate Beginners Guide*, Tykn, 2020, https://tykn.tech/verifiable-credentials/#Verifiable_Credentials_Meaning
[56] Manu Sporny, Dave Longley, & David Chadwick, *Verifiable Credentials Data Model v1.1*, W3 Recommendation, March 3, 2022, https://www.w3.org/TR/vc-data-model/#what-is-a-verifiable-credential
[57] *Id.*

been tampered with, and finally, that the data has not been revoked by the issuer.[58] Taken together these elements provide security — even in a trustless environment — that the provided credentials are tamper-proof, portable, and verifiable anywhere, at any time. These elements ensure that the credentials and underlying information remains private to all but the data holder.[59]

### D. Element Three: Security, Privacy & Decentralized Identifiers

Currently, digital identities are validated not by an issuer or the user, but by intermediaries such as Facebook, ID.me, Google, etc. [60] Because this data must be assessed by intermediaries, the metadata gathered by those parties from the interactions over those connections are not within the user or issuer's control.[61] This loss of individual data control means that the intermediary can use that data for commercialized purposes such as advertising whether or not the individual wants it to happen.[62]

Thus, under the banner of Decentralized Identifiers (DID), there are two categories: (1) Public, and (2) Private DIDs. Private DIDs may be transferred between two parties creating a secured channel which no outside party can access. An additional benefit to private DIDs is that they are unlimited, and therefore one user may have many private DIDs and none of them rely on a centralized authority to authenticate the identities. Should private DIDs become commonplace, it would effectively destroy the current structure of the ad-based open internet because collectors of this data would be stopped by the private DID transaction from gathering data about the user.[63]

---

[58] Khalid Maliki & Jimmy J. P. Snoek, *supra.*
[59] Manu Sporny, Dave Longley, & David Chadwick, *supra.*
[60] Christopher Allen, *Decentralized Identifiers v1.0*, W3C Recommendation, July 19, 2022, https://www.w3.org/TR/did-core/
[61] *Id.*
[62] Jon Roskill, *Who Owns Your Data? Why Your Business Application Data Might Not be as Secure as You Think*, Forbes Magazine, January 4, 2021, https://www.forbes.com/sites/forbestechcouncil/2021/01/04/who-owns-your-data-why-your-business-application-data-might-not-be-as-secure-as-you-think/?sh=bdc8d15607f0
[63] Kim Hamilton-Duffy, Ryan Grant, & Adrian Gropper, U*se Cases & Requirements for Decentralized Identifiers*, W3C Working Group Note 17, March 17, 2021, https://www.w3.org/TR/did-use-cases/#intro

Alternatively, public DIDs would be items which a user would want published (*e.g.*, a valid digital driver's license). Public DIDs could also be the verifying central authority which would validate a subsequent private DID between a user and organization.[64]

The mechanism employed by DIDs to ensure the correctness of the various inputs is the smart contract. Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met.[65]

In practice, when the government issues a driver's license, they create a physical card which is intended to be carried by the user. With a public DID, the user could create a QR code which would validate their identity in the event a police officer pulled them over. This method also precludes the unwilling sharing of private information by no longer requiring another entity to individually verify the identity of the user.[66] By way of example, if a person goes to purchase alcohol, they would be asked for their proof of age. Relying on the partnership between public and private DIDs, a user could show the verifier a QR code which when scanned would reach beyond their private DID to the issuer, which is almost always the government, who would validate the private DID's interaction because of the information stored on the public DID.[67] To the user and teller, it simply looks like scanning a code and the return response indicates that the user is permitted to conduct the purchase. The effect of these systems is to expedite the interaction and increase security, privacy, and efficiency.[68]

---

[64] Credentials Community Group, *A Primer for Decentralized Identifiers*, Draft Community Group Report 11, November 11, 2021, https://w3c-ccg.github.io/did-primer/
[65] IBM, *What are Smart Contracts on Blockchain*, IBM Blockchain, https://www.ibm.com/topics/smart-contracts
[66] Kim Hamilton-Duffy, Ryan Grant, & Adrian Gropper*, supra.*
[67] *Id.*
[68] *Id.*

## III. The United States & the State of Digital Identity

The United States was created as a constitutional federal republic. The lines of authority between states and the federal government are, to a significant extent, defined by the United States Constitution and relevant case law. This separation of power between the federal and state governments creates an inherently limited central government while permitting an expansive grant of power and autonomy to the States and Territories.[69] The net effect of such a system permits states to act in disparate, and at times, incongruent ways to one another.

As a result, the authority to resolve questions around privacy, data security and technology have been largely left to the individual states to resolve.[70] States from across the national and ideological divide have been more than happy to fill the gap left by federal legislators and regulators, determining for their own jurisdictions how to utilize and deploy technology to support increased user control of their information online.

### A. State Policy Actions:

State governments—in contrast to their federal partners—have begun rapidly expanding their research, use, and application of blockchain-based projects as a means of implementing a host of blockchain-powered changes. In 2021, seventeen states introduced more than 45 pieces of legislation respecting issues of blockchain and governance.[71] In 2022, 37 states introduced more than 164 pieces of legislation on these same issues.[72] For its part, California amended the Budget Act of 2021 to require, "[t]he Department of Technology shall consider the use of various technologies that support privacy protections, including blockchain technology or single digital

[69] U.S. Const. amend. X.
[70] *State Laws Related to Digital Privacy*, National Conference of State Legislatures, June 7, 2022, https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx
[71] *Blockchain 2021 Legislation*, National Conference of State Legislatures, March 16, 2021, https://www.ncsl.org/research/financial-services-and-commerce/blockchain-2021-legislation.aspx
[72] *Blockchain 2022 Legislation*, National Conference of State Legislatures, June 7, 2022, https://www.ncsl.org/research/financial-services-and-commerce/cryptocurrency-2022-legislation.aspx

identifiers, when planning and developing the Digital Identification pilot program."[73] In its current session the Legislature is discussing SB 1190, Creating the Department of Technology: California Trust Framework, which would require the department by 2024 to provide industry standards and best practices regarding the issuances of credentials to verify information about the person or a legal entity. The bill as presently debated requires that this Framework be designed to be interoperable with other government trust and governance frameworks for verifiable credentials.[74]

Shortly after passage of the 2021 Budget Act, California Governor Gavin Newsom signed Executive Order N-9-22 instructing state executive agencies in part to, "...assess how to deploy blockchain technology for state and public institutions, and build research and workforce development pathways to prepare Californians for success in this industry."[75] This order directed executive agencies to begin formally exploring how the implementation of blockchain can be utilized to benefit Californians and keep the State at the forefront of innovation.

In accordance with the 2021 Budget Act and Governor Newsom's Order, the DMV began exploration of a modernization program.[76] The DMV began its modernization program to secure a flexible and scalable Platform as a Service solution to provide workflow-based process optimization for their legacy Occupational Licensing applications.[77] In parallel to this program, the department began, in response to California Vehicle Code Section 13020's passage, to chart a path for a program which would comply with the statute's provision granting the department the ability to seek mobile or digital alternatives to driver's licenses and identification cards.[78]

---

[73] S.B. 112, *The Budget Act*, 2021-2022 Regular Session, CA Constitution, Art. IV, § 12
[74] S.B. 1190, *Department of Technology: California Trust Framework*, 2021-2022 Regular Session, Ca. 2022
[75] Office of Governor Gavin Newsom, *Responsible Web3 Innovation,* Exec. Order No. N-9-22 May 4, 2022
[76] California DMV, *Digital Experience Platform Solicitation*, No. ISD20-0066, 2021
[77] *Id.*
[78] California Vehicle Code § 13020.

However, the program did not call for a blockchain enabled platform and expressly stipulated that the database must be centralized.[79]

## IV. Use Cases Illustrating the Increasing Cost of Failure of the Centralized Model of Digital Identity & the Superiority of the Self-Sovereign Identity Model:

As the digital environment continues to develop and mature, governments seeking to maintain control and oversight must adapt or fall victim to their complacency. In 2021 IM Security conducted a global study of the cost related to data breaches resulting from single point of failure and found that the global average breach rose in cost from $3.86 million in 2020 to $4.24 million in 2021.[80] Astonishingly, the report showed that for the past 11 years the healthcare industry was the top target for bad actors costing that sector an average of $9.23 million dollars per breach in 2021.[81] During that same time, the Federal Bureau of Investigations (FBI) reported more than 847,000 complaints of cyber-crime: a seven percent increase from the year prior![82] The current system of centralized control is failing both users and holders of digital identities.[83]

In the face of unprecedented social, economic, and political disruption, 74% of respondents agreed that the traditional ways of doing business are not sustainable.[84] Technology is at the root of much of this disruption — but in the case of blockchain, it can also be the remedy. By automating redundant processes and sharing data among permissioned network members in a decentralized way, blockchain reduces traditional friction between systems and

---

[79] *Id.*
[80] *Cost of Data Breach Report 2021*, IBM Security, 2021, https://www.ibm.com/downloads/cas/OJDVQGRY
[81] *Id.*
[82] *Facts & Statistics: Identity Theft & Cybercrime*, Insurance Information Institute, 2021, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime
[83] *The European Union Blockchain Observatory & Forum*, ConsenSys AG, May 2019, https://consensys.net/blockchain-use-cases/government-and-the-public-sector/eu-blockchain-observatory-forum/
[84] Dave Zaharchuk, *Navigating the skills shortage crisis through cultivating talent,* IBM Institute for Business Value, 2021, https://www.ibm.com/thought-leadership/institute-business-value/report/skillsstorm/

unlocks the value long trapped inside hardened organizational information silos.[85] The result is newfound trust and transparency across the economy to include food supplies, supply chains, financial services, energy supplies, identity validation and more.[86] Within the public sector there are a multiplicity of organizations working at all levels to prove blockchain's value in leading the digital transformation of government. Three use cases in particular highlight the potential for government deployment of blockchain: the Estonian model for an SSI-compliant decentralized system and the European Blockchain Services Infrastructure (EBSI);[87] and Wyoming's passage of the Digital Identity Act.[88]

### A. Case Study 1: Estonia & the European Blockchain Services Infrastructure

In an effort to bring their nation online and into the modern era, leaders in Estonia after the fall of the Soviet Union in 1991 sought to digitize their nation. For perspective, the nation gained independence in 1991; at that time, more than ten percent of its population was unemployed and Estonia had a gross domestic product at nearly thirty times lower than that of its Scandinavian neighbors.[89] Thirty-two years later, Estonia has free high speed wireless internet nationwide, universal online voting, digital tax collection and online prescription filling systems.[90] They were able to do this because of the government's investment in digital identity cards and an innovation-friendly environment which fostered the third-highest number of

[85] Jonathon Fox, Tim Smith, & Ravi Kalakota, *Blockchain: Breaking Down Industry Silos*, Deloitte Tales of Transformation, May 2018, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/life-sciences-health-care/us-lshc-tot-s1-e3.pdf
[86] Jason Killmeyer & Jonathan Holdowsky, *From Siloed to Distributed*, Deloitte Insights, February 1, 2019, https://www2.deloitte.com/us/en/insights/topics/understanding-blockchain-potential/digital-supply-network-blockchain-adoption.html
[87] Toivo U. Raun, *Post-Soviet Estonia 1991-1993*, Journal of Baltic Studies Volume 25 No. 1, Spring 1994, http://www.jstor.org/stable/43211874
[88] H.R. 5, *The Digital Driver's License & Identifications Cards Act*, 2020 Leg. 65th Sess., Wy. 2020
[89] Toivo U. Raun, *supra.*
[90] *Id.*

startups per capita in Europe.[91] These benefits are not limited to Estonian citizens and are extended to e-residents too.[92] An e-resident can live outside Estonia and needs only to hold a valid government issued ID, pay a fee, and complete an online application to become an e-Estonian resident.[93] In doing so, e-residents can act and operate as owners and proprietors of businesses within Estonia without ever leaving their own home country.[94]

Estonia was slow and methodical in its application and execution of systems of digital identification, first targeting populations with significantly younger or older people (*e.g.*, schools or retirement communities).[95] Secondly, Estonia's passage of the Public Information Act of 2000 was an important step in growing its digital identity systems as it mandated a single data repository across the country, the X-Road system.[96] The Act further prohibited requesting duplicate information for public services, thereby mandating information sharing across government departments and functions.[97] Estonia raised its digital literacy rate from approximately ten percent in 2000 to nearly eighty-nine percent of all Estonians today. Nearly ninety-nine percent of all government services are now offered digitally.[98]

To achieve this feat, the Government partnered with private sector banks and telecommunications companies, who would benefit from the widespread adoption of digital ID

---

[91] Allison Berke, *New Tech in New Places: Case Studies of Public Investments in Advanced Tech*, California 100 Policy Brief, Issue 1, April 2022, https://california100.org/app/uploads/2022/04/California100-Policy-Brief-Issue1.pdf
[92] *Why Become an e-Resident*, Republic of Estonia, July 28, 2022, https://learn.e-resident.gov.ee/hc/en-us/articles/360000625098-Why-become-an-e-resident
[93] *Id.*
[94] Republic of Estonia, *supra.*
[95] *e-Identity & State Issued Digital Identity*, Republic of Estonia, 2022, https://e-estonia.com/solutions/e-identity/id-card/#:~:text=All%20Estonians%2C%20no%20matter%20where,the%20public%20and%20private%20sectors
[96] *Id.*
[97] Allison Berke, *supra*.
[98] Priit Martinson, *Estonia the Digital Republic Secured by Blockchain*, PricewaterhouseCoopers, 2022, https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf

cards and digital signatures.[99] These private partners agreed to shoulder some of the cost of the X-Road system infrastructure implementation.[100] This demonstrates the benefit of industry support; although digital ID cards had been introduced in 1998, they failed to gain widespread adoption until the industry-funded program stepped in, demonstrating the benefit of industry support.[101] To ensure sustained progress, the Estonian government slowly made adoption of digital IDs mandatory, providing free nationwide internet services to accommodate this requirement.[102] The government reported that these changes have generated approximately two percent in additional GDP annually since its implementation.[103]

To expound on the lessons learned from the Estonian experiment, the European Union (E.U.) enacted the Electronic Identification, Authentication and Trust Services (eIDAS) regulation which laid the framework for a European-wide interoperable and transparent digital identity system, prefiguring some of the SSI tenets.[104] The regulation stipulated that by 2018 all citizens of the bloc would be able to use their national electronic identification (eID) in any Member-State.[105] This was the single greatest factor in the facilitation of the creation of the European Digital Single Market, where citizens and companies can also access a European market of recognized "Trusted Services" whose certifications and authentications are legally

---

[99] *ID Systems Analyzed: e-Estonia*, Privacy International, January 12, 2022, https://privacyinternational.org/case-study/4737/id-systems-analysed-e-estonia
[100] International Monetary Fund, *Republic of Estonia Technical Assistance Report & Public Investment Management Assessment*, International Monetary Fund Report No. 19/152, June 2019, https://www.imf.org/-/media/Files/Publications/CR/2019/1ESTEA2019001.ashx
[101] *Id.*
[102] Priit Martinson, *supra*. This method of slow, methodical, and public-private partnership has enshrined Estonia as the leading nation in the implementation and execution of digital identities globally. This method is one which California would do well to mimic as it considers its steps forward.
[103] Allison Berke, *supra.*
[104] *Electronic Identification and Trust Services for Electronic Transactions in the Internal Market & Repealing Directive 1999/93/EC*, Regulation No. 910/2014 of the European Parliament & the Council of 23, July 23, 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910
[105] *Id.*

valid across the E.U.[106] Additional projects are ongoing in the E.U. and include a supra-national version of the Estonian program known as the European Blockchain Services Infrastructure (EBSI) framework, which is expected to publish its first use cases for review in 2024.[107]

### B. Case Study 2: Wyoming & Digital Identity

To engage in most aspects of civil society, a government issued identification document is necessary. While there is no nationally recognized American identification card, there are government-backed identity systems provided by different federal, state, and local entities such as drivers' licenses or birth certificates.[108] This legacy infrastructure, implemented between 1970-1989, is generally outmoded, outdated, and outclassed by the standards of today.[109] It has failed to keep up with the best practices for organizations handling this kind of information while also having the effect of lowering Americans' belief in their government to be efficient or modernize.[110] In 2016, the Government Office of Accountability concluded that "legacy federal [information technology] investments are becoming obsolete."[111] The federal systems aren't the only ones at risk, as Americans are commonly required to present their social security number (or card) for most things such as apartment applications, doctor visits, and employment.[112] Each of these uses, which were not the intended use of the social security number, includes a litany of

---

[106] Pierre Noro, *What is Self-Sovereign Identity & Should States be Afraid of it,* SciencesPro Chair Digital, Governance & Sovereignty, December 2020, https://www.sciencespo.fr/public/chaire-numerique/en/2020/12/21/what-is-self-sovereign-identity-should-states-be-afraid/

[107] The European Commission, *Roadmap: Ideas to Production,* European Blockchain Services Infrastructure, 2021, https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/Roadmap

[108] David Schultz, *National Identification Cards*, The First Amendment Encyclopedia, 2022, https://www.mtsu.edu/first-amendment/article/1133/national-identification-cards

[109] Carol Harris, *A Look at the Federal Government's Aging Computer Systems*, U.S. Government Accountability Office, August 6, 2019, https://www.gao.gov/blog/2019/08/06/a-look-at-the-federal-governments-aging-computer-systems

[110] *Id.*

[111] *Opportunities to Reduce Fragmentation, Overlap, & Duplication & Achieve Other Financial Benefits*, U.S. Government Accountability Office Annual Report to Congress, April 13, 2016, https://www.gao.gov/products/gao-16-375sp

[112] Adrianne Jeffries, *Identity Crisis: How Social Security Numbers Became our Insecure National ID*, The Verge, September 26, 2012, https://www.theverge.com/2012/9/26/3384416/social-security-numbers-national-ID-identity-theft-nstic

security risks to both the individual and the organization as the data can be stolen at nearly every step of the process.[113] This outdated form of identity is overdue for modernization.[114]

Recognizing the absence of federal leadership, Wyoming decided to take it upon itself to act. State policymakers reached out to contacts in the private sector to assist the state in devising a method of digitizing records and identities.[115] In 2020 that effort culminated in the passage of H.B. 5, allowing residents to obtain a digital driver's license and an identification card to supplement the use of physical IDs in the state.[116] In doing so, Wyoming became the seventh jurisdiction in the United States to incorporate a digital identification card for use by residents and law enforcement.[117] Just one year later the state would again push the limits of digital identification by codifying the Digital Identity Act of 2021 into law. This law, the first of its kind in the United States, defines digital identity as "the intangible digital representation of, by and for a natural person, over which he has principal authority and through which he intentionally communicates or acts."[118]

Since the Act's passage, Wyoming has begun an exploration of an interstate model, like that enumerated under the Estonian and eIDAS system. Wyoming has begun soliciting other states to enroll in their pilot eID system; a trust framework with a scheme such as eIDAS instead of a federal eID could be established.[119] It remains to be seen how such an interstate network

---

[113] Sophie Bushwick, *Social Security Numbers Aren't Secure: What Should We Use Instead*, Scientific American, September 24, 2021, https://www.scientificamerican.com/article/social-security-numbers-arent-secure-what-should-we-use-instead/
[114] *Id.*
[115] Dazza Greenwood, *Wyoming Digital Identity Legislation Update*, Civics.com, September 29, 2020, https://www.civics.com/pub/wyoming-digital-identity-legislation-update/release/2
[116] H.R. 5, *The Digital Driver's License & Identifications Cards Act*, 2020 Leg. 65th Sess., Wy. 2020
[117] Ryan Johnston, *Wyoming Lawmakers Advance Digital Driver's License Bill*, StateScoop, March 4, 2020, https://statescoop.com/wyoming-lawmakers-advance-digital-drivers-license-bill/
[118] S.R. SF0039, *The Digital Identity Act*, 2021 Leg. 66th Sess., Wy. 2021
[119] Daniela Pohn, Michael Grabatin, & Wolfgang Hommel, *eID & Self-Sovereign Identity: An Overview*, Electronics, November 2021, https://www.mdpi.com/2079-9292/10/22/2811/pdf?version=1637131340

would be managed, much less funded, when no one state has any inherent authority, but the model is promising for the integration and interpolation of SSIs in the United States.

## V. A Path to Digital Deliverance: Self-Sovereign Identities and Good Governance

The State of California has a prominent history of supporting, developing, and implementing technological changes which have impacted the course of human history.[120] Producers, consumers, and users of digital material are recognizing the internet as an information superhighway which allows for anyone, anywhere, to question anything: even a person's identity.[121] Failure to protect these digital identities now will only hurt those who have already been most affected by the increasing digitization of modern life: the poor, the unbanked, the unhoused, and others.[122] For this reason, Governor Newsom's Executive Order regarding the exploration of the use of blockchains represents a powerful statement of California's values respecting the need for inclusivity.[123]

### A. Lessons for the California Department of Motor Vehicles (DMV)

The California DMV is in a unique position as one of the largest holders of Californians personal information while simultaneously being one of the only state-wide agencies capable of implementing the improvements necessary to create an SSI-compliant model of governance.

---

[120] Relevant to a discussion on digital identities is the University of California at Los Angeles (UCLA) establishment of the Advanced Research Projects Agency Network (ARPANET) in 1966. Establishing the forerunner of the modern internet.

[121] *Identity in a Digital World: A New Chapter in the Social Contract*, World Economic Forum Report, September 2018, https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf

[122] *Inclusive & Trusted Digital ID Can Unlock Opportunities for the World's Most Vulnerable*, The World Bank, August 14, 2019, https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable

[123] Office of Governor Gavin Newsom, *Responsible Web3 Innovation,* Exec. Order No. N-9-22, May 4, 2022, *noting* California will "… address public-serving and emerging needs, working with the private sector, academia, and community to present pilots for innovative policies, programs, and solutions that demonstrate and showcase the potential of adopting blockchain technologies to respond to specific challenges identified by state agencies…".

As an example, in 2018 the DMV began issuance of REAL IDs, in compliance with the REAL ID Act of 2005. The purpose of the amended licenses was to preclude holders from obtaining multiple valid licenses or social security numbers while simultaneously allowing government officials to verify immigration status.[124] But the rollout of the physical IDs was marred with reports of significant delays relating to the physical assets of the department in addition to those of its information technology division.[125] The DMV sought to address this issue directly in its 2021-2026 Strategic Plan, which included the goal of delivering a "simpler, faster way to fulfill customer needs through expanded digital services."[126] However, this goal fell short of identifying how the department intended to produce such capabilities or detail the means in which it would seek to protect and secure user data. In light of the increasing attacks against centralized systems and the costs of defending against those attacks,[127] the DMV must look to another method, other than the centralized and user-centric model which has resulted in losses of trust and security between users, third party vendors and the department itself.[128]

Thus the question then becomes: how can the DMV begin the process for validating and securing digital identities in an increasingly digitized world? To achieve a truly self-sovereign identity, the DMV need only look to schemes like that of Estonia or the broader eIDAS framework for functional workability. Digital citizenship under the Estonian framework would permit people living in other jurisdictions to access California governance structures online and/or in the metaverse, to open businesses, and to simultaneously identify with the state's ethos.

---

[124] H.R. 1268, *Emergency Supplemental Appropriates Act for Defense, the Global War on Terror, & Tsunami Relief*, 109th Cong., 2005
[125] California Department of Finance, *supra.*
[126] *Strategic Plan: 2021-2026*, California Department of Motor Vehicles, 2021
[127] Cassy Lalan, *IBM Report: Cost of a Data Breach Hits Record High During Pandemic*, July 28, 2021, https://newsroom.ibm.com/2021-07-28-IBM-Report-Cost-of-a-Data-Breach-Hits-Record-High-During-Pandemic
[128] Waldo Jaquith, *Software Co-Ops & Digital Identity: How U.S. State & Local Governments Are Adapting Login.gov to Verify Identity*, Beeck Center, October 14, 2021, https://beeckcenter.georgetown.edu/wp-content/uploads/2021/10/Software-Coops-and-Digital-Identity-2.pdf

This type of digital engagement could draw investment and entrepreneurship in emerging industries – particularly those that will address consumer needs in California, and among target demographic groups, despite individual locations. Estonia's e-residency program is a prime example of an SSI-compliant system which allows anyone in the world to access its digital identity platform while benefiting the Estonian government. Through this platform, e-residents have access to the EU's specific business environment and can use the EU's public e-services. Digital citizenship could allow California to attract resources from other jurisdictions with solid governance frameworks and diversify state budget revenue streams, even if quality of life issues lead to net outflows of talent.[129]

Under a California-compliant iteration of the Estonian scheme, the DMV, in reliance on state agencies such as the California Department of Public Health, would be able to validate a user's digital identity simply through certification of the credentials provided at the point of service or online. There is precedent for this type of project. In 2011 nine states signed onto the Health Care Compact of 2011 when they agreed to form a single standard for care, responsibility, funding, amendments, and withdrawal procedures. These states continue to work toward a universal standard for health care professionals across the United States.[130] In this system, the California Department of Public Health, already having the necessary data, would permit the DMV to simply validate the information it has and thus would promote a greater unity of knowledge among the agencies while further protecting the user's personal information. This mirrors what Wyoming, under its eID pilot program, is seeking to establish. In this way, states

[129] Henry Brady, Lindsay Maple, & Ava Calanog, *Future of Advanced Technology & Basic Research: A California 100 Report on Policies & Future Scenarios*, California 100 Report on Policies & Future Scenarios, March 2022, https://california100.org/app/uploads/2022/03/The-Future-of-Advanced-Technology-and-Basic-Research-ISSUE-REPORT-Single-pages-Round-3-2.pdf

[130] *States Consider Health Compacts to Challenge Federal PPACA*, National Conference of State Legislature, December 2015, https://www.ncsl.org/research/health/states-pursue-health-compacts.aspx

would have the power to assert the standards of digital care which they would see mirrored across all other jurisdictions within the pilot.

The DMV only needs to expand the processes and services which are offered online and ensure they are interconnected and interoperable to achieve the same effect of the X-Road system Estonia took 25 years to implement. Moreover, Estonia's development demonstrates that governments do not need to replicate one another to achieve a level of technological sophistication; rather, they stand to benefit from those who have already gone before them and can instead implement the programs which worked well. The DMV therefore could choose to enact a system similar to Estonia's X-Road system while employing Wyoming's private sector knowledge and experience to build a network which would be first rate. Similarly, a whole-society strategy provides synergies that stopping at a single department or service could not. Wherever possible, projects that connect services and will be used by the broadest possible swath of society both build momentum and create network effects that make it easier to connect increasing numbers of government departments. In fact, analysis of the number of data repositories connected to X-Road and the number of queries made suggests that exponential growth in querying takes off around the 50th data repository linked, out of more than 200 repositories currently linked through the system.[131]

As one of the largest repositories of California residents' information, the DMV would be a natural place to begin with the creation of a system which would, as the Estonian model illustrates, bring more users online and do so by means which place user security and protection at the forefront. To effectively highlight this opportunity, the Department must begin to rethink

[131] A query occurs when a validating authority makes a request for verification of a digital identity product. (W3C, *Query Defined*, W3C, 2022, https://www.w3.org/standards/semanticweb/query#:~:text=%E2%80%9CQuery%E2%80%9D%20in%20the%20Semantic%20Web,from%20the%20Web%20of%20Data)

how it approaches digital identity and storage. It need not adjust its current course of business immediately, but it should begin the process for supporting and engaging with SSI-compliant models of governance. The EBSI model is particularly useful as a benchmark, setting a five-stage process for establishing the viability of such operations within the organization.[132]

**Step One: Identify Use Cases.** The DMV need not look far to establish a plethora of use cases whereby government agencies, foreign and domestic, have engaged with issues of SSI and returning information stored on centralized government systems to users such as those of Estonia or the EBSI framework under review in the E.U.[133]

**Step Two: Select Use Cases.** Once the DMV identifies which use cases it seeks to emulate, it can employ the methods and lessons learned to navigate a path forward for itself.[134]

**Step Three: Identify the Ecosystem.** When the DMV establishes its preferred use cases, it should look to which system within its administrative control would be best suited for the role in a pilot program. There are several notable projects which the department could seek to implement this SSI-compliant system; notably its virtual wallet would be an ideal test.[135]

**Step Four: Plan the Implementation.** The DMV will need to establish the parameters of its physical capabilities and whether it might be necessary to purchase, or outsource, the necessary infrastructure to execute the pilot. Here it would be helpful to look at the Wyoming program for digital licenses, where they partnered with private companies to host their data as

---

[132] *The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers*, OECD, June 2009, https://doi.org/10/1787/222134375767
[133] *European Blockchain Services Infrastructure*, The European Commission Policy & Factsheet, 2022, https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure
[134] *Id.*
[135] Jessica Mulholland, *California DMV Digital eXperience Platform Aims for World Class Self-Service Channels for Customers*, GovReport, January 31, 2022, https://www.govreport.org/news/california-dmv-digital-experience-platform-to-provide-world-class-self-service-channels-for-customers/

"certified service providers" while the pilot for the Safe ID is ongoing.[136] However, with the onset of the California Privacy Rights Act in January 2023 and enforcement by the California Privacy Protection Agency, the DMV must also consider the impacts and limitations imposed to determine the pilot's eventual scope.

**Step Five: Execute the Pilot.** Having planned, organized, and established its purpose and goal, the Department should begin implementation of its pilot, ensuring compliance with all regulatory laws, and upon completion, evaluate the successes and challenges of the pilot and share those insights with other agencies and organizations within the state. This process of data sharing only further highlights the inherent value of transparency and clarity for all users and servicers.

The DMV has already taken the hardest step, which was to agree to start the process of exploration of the scope and application of digital identities in the modern era. The revival of the DMV's pre-coronavirus blockchain pilots would be a simple but clear commitment towards ensuring greater user security and data integrity for all Californians.[137]

## VI. Conclusion:

California has historically led the world in the discovery and application of new and exciting technologies. The application of blockchain-based security systems should be no different. Now is the time for the DMV to evaluate the value of a decentralized but still privately controlled digital self-sovereign identity system. The results of pilot programs from Estonia to Wyoming conclusively illustrate that SSI-based systems, when coupled with decentralized systems of control, are superior to the older, and increasingly antiquated, centralized models.

---

[136] *Wyoming DIgital Identity Legislation Update,* Civics.com, September 29, 2020, https://www.civics.com/pub/wyoming-digital-identity-legislation-update/release/2

[137] California Blockchain Working Group, *supra.*

With blockchain technology, information about a digital identity is auditable, traceable, and verifiable in just seconds. The benefits already exist across Europe and in at least seven states where individuals can curate their own profiles and control data sharing.[138] Issuers can easily connect with others within and from without their jurisdiction and provide nearly instant verification of credentials to verifiers. The simplicity of the SSI model makes clear that California must flex its digital power and begin the integration of digital identities for all.

[138] Ryan Galluzzo, Tim Li, Badri Nemani, Dr. Colin Soutar, *The Future of Government Rests on the Future of Identity,* Deloitte Insights, June 20, 2022, https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-agile-identity-solutions.html