frontiers in Blockchain

COMMUNITY CASE STUDY
published: 29 April 2021
doi: 10.3389/fbloc.2021.624258

Decentralized, Self-Sovereign, Consortium: The Future of Digital Identity in Canada

Andre Boysen[1,2]*

[1] SecureKey Technologies Inc., Toronto, ON, Canada, [2] Centre for International Governance Innovation, Waterloo, ON, Canada

This article introduces how SecureKey Technologies Inc. (SecureKey) worked with various network participants and innovation partners alongside government, corporate, and consumer-focused collaborators, in a consortium approach to create a mutually beneficial network of self-sovereign identity (SSI) principles with blockchain in Canada. These principles are based on giving users ownership and control over all of their digital identity attributes as an alternative approach to the current *status quo* of centralized digital identity, which focuses on discrete identities are made within individual online properties. Blockchain is used as the foundation for its strong security protocols to prevent information from being identified, accessed, or misused and uphold SSI principles. This article will consider the current *status quo* of digital identity known as centralized digital identity and comparisons to the case study's emphasis on the alternative thinking of SSI with principles with blockchain, which prioritizes a decentralized, self-sovereign, consortium approach as opposed to discrete identities within individual online properties. Each of these principles will be explained in detail before highlighting the practical implications, lessons learned for future applications, and how both the Canadian and global identity landscapes should proceed for wider acceptance of SSI with blockchain. The case study detailed – that of Verified.Me – will demonstrate how blockchain developers can actively work to help partners transition from current identity silos to instead collaborate across varied industries and create a cohesive, secure service and digital identity network that benefits users through SSI principles and the benefits of blockchain. We also offer recommendations for how both the Canadian and global identity landscapes should proceed for wider acceptance of SSI with blockchain, the benefits of doing so, and anticipated barriers affecting the adoption of future decentralized identity initiatives.

Keywords: digital identity, identity, blockchain, self-sovereign, decentralized, identity verification, data, data privacy

OPEN ACCESS

Edited by:
Alan Sherriff,
Consultant, London, United Kingdom

Reviewed by:
Iain Barclay,
Cardiff University, United Kingdom
Ian Taylor,
University of Notre Dame, United States
Uyen Trang Nguyen,
York University, Canada

***Correspondence:**
Andre Boysen
andre.boysen@securekey.com

Specialty section:
This article was submitted to Blockchain for Good, a section of the journal Frontiers in Blockchain

Received: *31 October 2020*
Accepted: *02 March 2021*
Published: *29 April 2021*

Citation:
Boysen A (2021) Decentralized, Self-Sovereign, Consortium: The Future of Digital Identity in Canada. Front. Blockchain 4:624258. doi: 10.3389/fbloc.2021.624258

INTRODUCTION

The increased prevalence of today's data breaches and cyber security incidents, the detriments of data silos, and the benefits of proper protocols enforcing security and usability have been important considerations amid the heightened interested in and developments of modern digital identity systems. Our rapidly growing digital world, with subsequent increases in fraud and privacy

concerns, requires evolved efforts and advancements in thinking to keep up with these threats and take advantage of opportunities as they develop. The approach of ever-increasing vigilance on the part of users and online properties has well past the peak of diminishing returns. A different approach is needed, an approach of simplification for users that removes the "user-sophistication" requirement of understanding the security model in order to keep data safe.

People need methods to establish the same or better levels of trust for online interactions than we have with in-person transactions. For example, Smits and Hulstijn (2020) detail that a blockchain application may affect the decision to enter the network and engage in a transaction in four ways:

1. The actor believes the institution(s) offering the blockchain-based platform to have properly implemented the blockchain, and for each transaction, to faithfully represent the agreement on the blockchain (party-based trust).
2. The actor believes the blockchain-based network can be monitored and subsequently that the blockchain application helps to reduce transaction risks (control-based trust).
3. The actor sees potential gains because of the blockchain application in the business network. More potential gains enhance engaging in business network transactions.
4. The actor sees transaction risks in the original business network and believes that a blockchain application may reduce those risks, through blockchain-based controls.

The most important principles to establish this trust and increase adoption are security and usability. Consumers want to know their data are safe with proper cyber security measures while having the ease of use required to access services in a way that is not prohibitively complicated. The ability to access different services with the same credentials while staying protected has similarly been a priority for people to increase convenience.

The Commission on Enhancing National Cyber Security established six main imperatives to secure and grow the digital economy (Commission on Enhancing National Cybersecurity, 2016):

1. Protect, defend, and secure today's information infrastructure and digital networks.
2. Innovate and accelerate investment for the security and growth of digital networks and the digital economy.
3. Prepare consumers to thrive in a digital age.
4. Build cyber security workforce capabilities.
5. Better equip government to function effectively and securely in the digital age.
6. Ensure an open, fair, competitive, and secure global digital economy.

This set of principles is full recognition of the inextricably intertwined interests of everyday consumers, the businesses they interact with and the wider economy including government in its own online transactions, as well as in its national cyber-security strategy. User passwords, widespread data breaches, and national cyber security are all facets of the same problem. In short, you cannot have a digital economy without digital identity. Each of these principles is evidence that the lack of digital identity infrastructure is holding the economy back – for commerce, for employers, and for government.

Before going further, it is worth noting what does work well in "street identity" – the identity that is used for in-person transactions today. This allows for a plurality of providers where every business can make its own rules, individuals all make their own choices about what to bring to join the service, and there is some inherent privacy with today's digital identity methods. With street identity documents today, the issuer is blind to where and when the user chose to present the document to a service destination – this is a good thing we want to preserve as we forge ahead.

This plurality exists because there is more than one provider of identity information and more than one sector providing it – driver's licenses, bank statements, and utility bills are all accepted in some transactions but with different providers. Every business can make its own decisions about what is sufficient for them to achieve the requisite level of trust to proceed. The issuing authority is blind to the transaction when the driver's license or bank statement is used in a transaction, which adds to the level of privacy for the user.

Street identity takes a village to make it work. Neither private nor public sector solves the whole street identity problem individually – they solve it together in the hands of and under control of the user. This emphasizes a high level of commitment between the public and private sectors that requires cooperation and collaboration between the two to enhance the state of national cyber security, which is especially important considering that the digitalization of government services includes the need for a safe, portable, and easily accessible digital identity (Zwitter et al., 2020). The advancement of technology continues to outpace security – as such, changes are required in how these sectors approach and implement cyber-security strategies and practices while preserving innovation and ease of use.

The main requirement to satisfy these conditions, eliminate potential obstacles, and increase the benefits of self-sovereign identity (SSI) with blockchain is communication between blockchain organizations, partners in the public and private sectors, and consumers to show the value-add and viability of existing solutions to bring digital ID to its full potential. Transitioning from online identity silos to full collaboration in digital identity that works across the economy requires each to recognize that the benefits of participating in a scheme outweigh the perceived benefits of owning and controlling the whole identity management technical stack to the exclusion of any partnership.

SecureKey developed Verified.Me, a blockchain-based and privacy-centric digital identity verification network – along these imperatives and SSI principles to meet these requirements to provide strong authentication while protecting individual privacy (**Figure 1**).

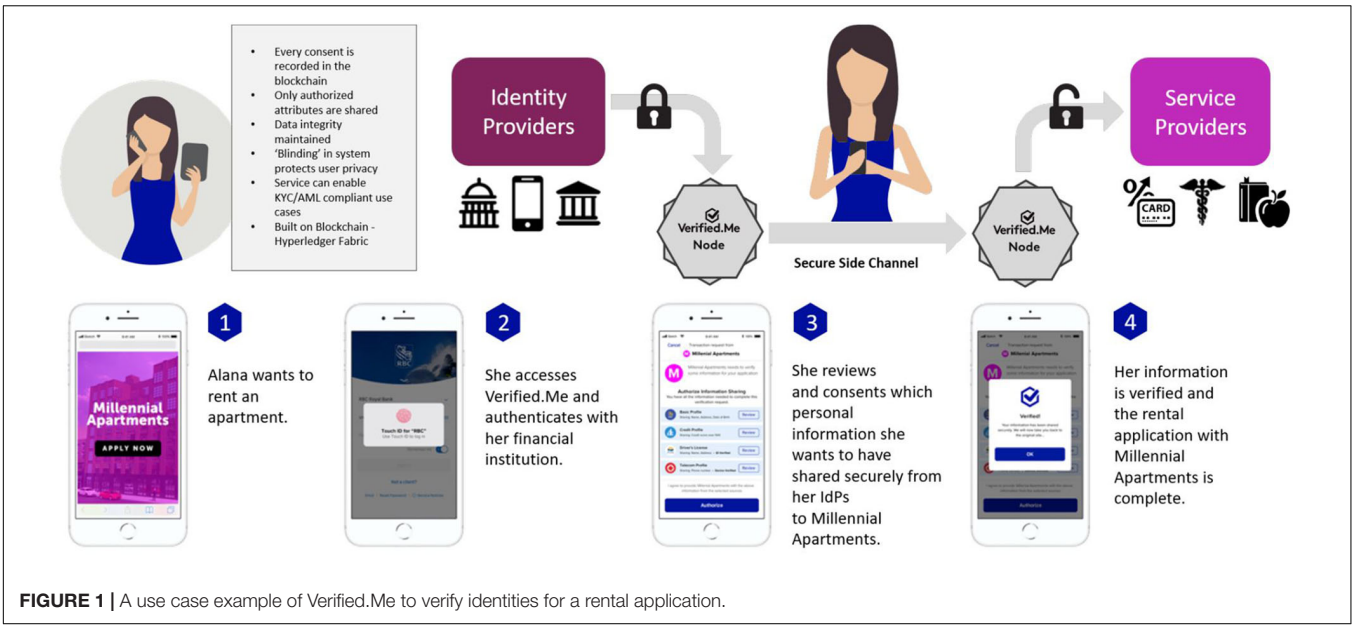

FIGURE 1 | A use case example of Verified.Me to verify identities for a rental application.

The initial work toward the eventual launch of the Verified.Me service was first backed by an applied research-focused partnership of the Digital ID and Authentication Council of Canada (DIACC) and Rutgers University Command, Control and Interoperability Center for Advanced Analysis, concentrating on model definition, business analysis, and applied research. Upon completion of the research leg, the Verified.Me service was formally developed in cooperation with seven of Canada's major financial institutions – BMO, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank, and TD – with additional partners from other industries continuing to join over time after its launch in May 2019.

CONTEXT

Currently, the state of the art in digital identity focuses on centralized models. Discrete identities are made within individual online properties, such as social media accounts, government identity issuance, and corporate management systems. In general, these typically feature one set of credentials, such as a username and password combination, which allows users to access and use platforms, services, and software. While passwords have to be secure, the recovery mechanisms to reset the complex password tend to be trivially simple, thereby defeating the purpose of a complex password. The administrative effort needed to use identities is one of the core challenges of SSI to offer solutions that help users' comfort levels (Der et al., 2017).

Fundamentally, this creates a fragmented identity experience requiring different sets of credentials for different platforms and uses. Centralized digital identity results in sensitive personal data to be stored by each platform in order to operate, which increases security and privacy risks due to how much personal data are stored on their servers (van Wingerde, 2017). The user burden to manage all of this complexity is too high, and the data required to undermine all of these services are stored across all of them. Effectively, if one service is breached, then they are all breached because the breachers replay the data at every endpoint in both password resets and credential-stuffing attacks.

This form of digital identity also lacks the ability to verify the data against the source or with the person presenting it – the system simply knows that the person accessing the system knows certain login credentials (SecureKey, 2020). The combination of a fake driver's license photograph and a real person's driver's license data (name, address, and birthdate) is effective for identity theft in both street and online identity. In street identity use cases, the destination service cannot verify the document against the issuing source, so it falls victim to the real data, fake photo document. The current online trend of taking a selfie and sending it alongside your driver's license also does not solve this problem.

Centralized digital identity also results in the oversharing of data. The documents that are available to choose from in order to verify one's identity may provide required proofs such as name and address, but they also display other personal data rather than what is required by the transaction. A bank statement verifies a name and address while also displaying bank account information and other data such as shopping and spending habits. Consumers are forced to participate in fragmented identity systems where the net benefit and authority over data sharing skew far in favor of the organization with whom they interact. Users are giving up more data than they need to, and this oversharing is a downstream risk when data breaches use the extra information to conduct replay attacks.

This is the essence of the flaw of the existing identity architecture we have today – it is a double-diffusion issue. Neither users nor business can tell what is real and what is not because there is so much fraud noise caused by too many endpoints. The business remedy to fraud noise is to ask for lots of user data to mitigate risk. Thus, crooks then harvest ample user data because they can make money from the data by pretending to be real

people. The best way to shut down identity fraud is to make the identity data worthless – mere possession of user should not be sufficient to mount a masquerading or takeover attack of real people. An additional benefit of this approach is that synthetic fraud will also go away because only real people will possess the requisite tools to transact.

Here is an alternative to today's approach, a trusted network approach to digital identity that has demonstrated the ability to solve these negatives (**Figure 2**). Rather than forcing a counter visit, where the documents cannot be verified anyway, a network approach to digital identity with a user-controlled sharing mechanism to present trusted and verified data would serve both the user and the service they want to connect to.

As an example, the registration application can be completed online through the financial institution's online systems by invoking a trusted network service. Street identity verification, while it can be cross-checked with online services, requires an in-person process to confirm that the owner of the credentials is the one giving his/her own information. Network services attempt to solve this limitation of requiring in-person visits by allowing users to collect and present trusted and verified digital assets to and from network participants. Trusted and verified data mean that the data come from an existing, known source that does this already for street identity today.

In that context, these networks have the potential to secure the following (SecureKey, 2019):

- A user's right to privacy of activity.
- A user's right to decide when and what information about themselves is shared between organizations.
- Cryptographic protection of digital assets for confidentiality and integrity.
- That all digital asset exchanges and transactions are cryptographically auditable.
- No central point of failure or trust: a distributed network of trusted organizations runs a cryptographically protected consensus protocol that collectively determines the state of the networks, the participants, the digital assets, and the users.
- Permissions, authentications, and auditability of network participant activities.

DETAIL TO UNDERSTAND KEY PROGRAMMATIC ELEMENTS

Self-sovereign identity is a digital identity philosophical perspective that emerged based on providing users with ownership and control of their digital identity information. This allows them to retain sole control over the management of their digital identity. In comparison to the current philosophy used by centralized digital identity methods, this shifts decision authority to the user through secured distributed ledger – blockchain – technology. It also means that data-replay attacks that are prevalent with user data today are much harder to mount.

While the 10 principles defined by Christopher Allen (Allen, 2016) are abstract and arguably require further development and operationalization (van Wingerde, 2017), these attempt to better conceptualize standards for SSI. Most digital identity projects will not meet all of these criteria, but the 10 principles serve as a preliminary benchmark to assess existing SSI solutions (Wang and De Filippi, 2020):

1. *Existence*: Users must have an independent existence.
2. *Control*: Users must control their identities.
3. *Access*: Users must have access to their own data.
4. *Transparency*: Systems and algorithms must be transparent.
5. *Persistence*: Identities must be long-lived.
6. *Portability*: Information and services about identity must be transportable.
7. *Interoperability*: Identities should be as widely usable as possible.
8. *Consent*: Users must agree to the use of their identity.
9. *Minimalization*: Disclosure of claims must be minimized.
10. *Protection*: The rights of users must be protected.

Understanding the current state of digital identity and alternatives to it requires understanding federated identity management. Federated identity uses one system or organization as the main source of managing user authentication as a platform for a group of organizations that offer many different services. Users in this group of organizations can then leverage the same credentials and data to access resources from every organization within the group for the repurposing of identity credentials. One of the biggest challenges of siloed approaches of central and federated systems is overburdening users with identity management (Zwitter et al., 2020). Compared to conventional centralized digital identity models, these credentials allow for access to more than one system as opposed to being limited to one organization per credential. Federated identity management requires the group to trust the one organization designated to manage the user authentication.

Eighty-eight percent of United States consumers have used social logins such as Facebook or Google to conduct authentication through an existing user account (Gigya, 2015), representing the most prominent examples of federated identity management. This information and data are used by an array of other organizations for their own login and authentication processes with the responsibility of managing identities held by Facebook or Google.

Verified.Me takes a hybrid approach, expressing SSI principles within a federated and decentralized identity management system for digital identity verification. Multiple participants work together within a common ecosystem to securely and privately verify the identities of users across the participating organizations with others within the group. SecureKey manages the underlying network to ensure Verified.Me is safe, private, and useful, while upholding the SSI principles.

Federated identity means one identity provider with lots of service destinations. Hybrid means many identity providers with many service destination bound together in a scheme – or trust framework. Hybrid also relates to the method of data sharing.

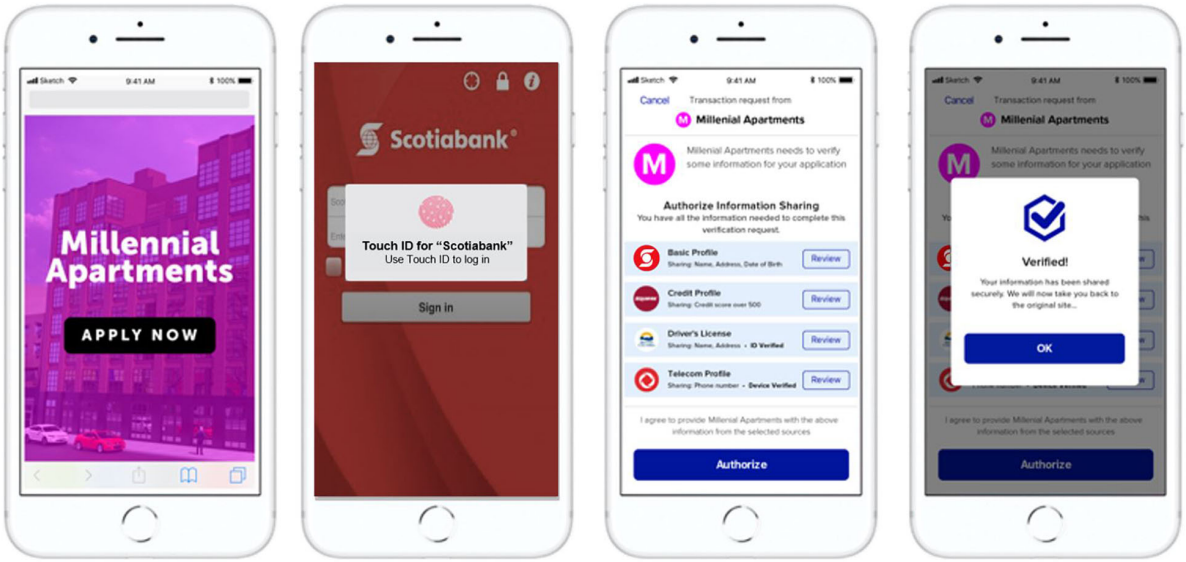

FIGURE 2 | The screens a user will see while accessing Verified.Me to verify their identity.

From a data sharing perspective, SSI operates as a store-and-forward model. Users gather claims from identity sources and store the claim in a wallet they control and later share those claims with the service destination. These claims are static as they are created and dated.

While Verified.Me accommodates these types of claims, it also supports real-time claims. With real-time claims, the exact location of the phone the user uses to transact on can be provided, which is harder in a store-and-forward approach. Proof that the user has logged to the user's registered bank account, without divulging the bank details, combined with proven location of the phone, adds additional integrity to static claims and mere possession of the phone. Hybrid also allows for privacy innovation. SSI is a double-blind sharing scheme – the source does not know where the data are sent, but the receiver knows where it came from. With Verified.Me, there is a triple-blind sharing mechanism that blinds the source and destination to each other while also blinding the network to the contents of the transaction. This helps properly account for one of the main caveats associated with decentralization with everyone's interactions typically being made visible to all network nodes (De Filippi, 2016).

"Making Sense of Identity Networks" is an expanded white paper discussing different types of identity networks that has been authored by DIACC[1]. It discusses different approaches, including the approach taken by Verified.Me. What is salient is that it enumerates and discusses the different stakeholder interests in creating digital identity and provides guidance on how to properly balance the different interests with a focus given to user agency in conducting transactions. The key success ingredients are identity portability, stakeholder collaboration, and network governance.

[1]https://diacc.ca/2020/05/13/making-sense-of-identity-networks/

DISCUSSION

One of the most important elements of SSI and federated identity management that is important to consider as a relatively new philosophy in a long-standing digital landscape is the essential role of trust and the fact that the design of a blockchain application influences the trust induced (Smits and Hulstijn, 2020). Given the amount of control users will have over their data, the number of other organizations required, and the principles dictating that the freedoms and rights of users should be preserved over the needs of the network, all the parties involved placing a large deal of responsibility on organization managing the user authentication – "the data is real, but is it the real user?" In the real world, the practical implication of this is that the initial coordination process and gathering funding can be a significant undertaking to prove the organization's capabilities, while also having enough partners involved to showcase the value-add of choosing this model over the current DIY model that may be immediately more convenient, but is more problematic over time.

It is important to state the obvious in order to overcome it. The investment made in identity security today is uneven across online properties – the money available and the skill to administer user identity are not uniform. Yet, startups, internet giants, governments, utilities, and healthcare providers all possess the same essential user data required for crooks to mount successful fraud attacks at all the other online destinations. So money and skill are not a complete remedy to the problem for any online destination. Smarter investment is required in collaborative approaches.

When Verified.Me launched in May 2019, SecureKey worked with various network participants and innovation partners, alongside government, corporate, and consumer-focused collaborators, in a consortium approach to create a

mutually beneficial network that upholds the principles of SSI in Canada. This was developed in cooperation with seven of Canada's major financial institutions – BMO, CIBC, Desjardins, National Bank of Canada, RBC, Scotiabank, and TD – as part of a collaborative blockchain-based approach to help bring about the benefits of decentralized digital identity across the public and private sectors. This process, taking 4 years from the initial design phase and gathering the network of collaborators over time, was a prime example of how blockchain developers can actively work to help partners transition from identity silos to SSI principles and collaborate to create a cohesive, secure digital identity blockchain service. It is important to note that while Verified.Me took 4 years to introduce, it was against the backdrop of the existing successful federated authentication scheme called SecureKey Concierge that launched in 2012; the banks and governments had already learned from that experience.

In order to be successful, a wide variety of public and private sector organizations must be actively involved and act together in close collaboration. For example, the financial institution identity and data providers involved with Verified.Me, namely, the financial institutions listed previously, are responsible for hosting core components of the network and verifying users to service providers, also known as relying parties. Additional roles within the Verified.Me service are played by Canadian organizations that facilitate desired transactions by asking users to provide certain information through the service. Existing and anticipated service providers include, but are not limited to, financial institutions, insurance companies, telecommunications providers, online merchants, healthcare solutions, credit bureaus, legal professionals, sharing economy, online gaming, governments, and educational institutions.

The emphasis on control, privacy, data minimization, and user consent as dictated by SSI principles are incorporated into Verified.Me and advocated for by the network owner, SecureKey. These tie into the advancement of decentralized identity standards in Canada and globally through active collaboration with major institutions for an identity service used by millions of Canadians. SecureKey plans to register Verified.Me for the Decentralized Identifiers specification as set by the Decentralized Identity Foundation. In addition, SecureKey is a founding member and active contributor to the DIACC, as well as the World Wide Web Consortium, UK. Verify, OIX, Kantara, Open ID, and European eIDAS standards. As such, Verified.Me is set up for interoperability with other decentralized identity systems that adhere to these standards.

ACKNOWLEDGMENT OF ANY CONCEPTUAL OR METHODOLOGICAL CONSTRAINTS

There are still a number of challenges for widespread adoption of decentralized identity and SSI principles despite the opportunities available. Although the Commission on Enhancing National Cyber Security was a mentioned component earlier in the article for creating six main imperatives to secure and grow the digital economy, the regulatory landscape is uncertain. As awareness and adoption increase, the attention given to more definitive regulation is expected to increase as well. In particular, encouraging every online service delivery organization to see beyond the perceived safety of complete control over the user ID and password stack they have today is no small feat.

At the time of writing, North America lacks specific regulatory restrictions on SSI and decentralized identity, but private organizations must comply with data privacy regulations and industry-specific requirements (SecureKey, 2019). Decentralized digital identity is understandably and greatly impacted by data privacy regulations. Recent regulatory developments, such as the Personal Information Protection and Electronic Documents Act, the General Data Protection Regulation, and the California Consumer Privacy Act, rightfully seek to manage data portability and place great emphasis on user consent – particularly around data collection and ultimate usage (SecureKey, 2019). While regulations do not specifically prohibit digital alternatives, there are few regulations that acknowledge and encourage better digital alternatives to street identity.

The lack of governance frameworks and agreements between identity providers and service providers has resulted in limited liability assurance and hesitancy by organizations to embrace decentralized digital identity (SecureKey, 2019). One example of uncertainty resulting from a lack of regulation is that financial institutions are required to conduct customer due diligence to prevent fraudulent actions. If a bad actor is permitted into the network by another party, it is unclear who would be held accountable (SecureKey, 2019). As a result, these processes cannot purely rely on SSI and decentralized digital identity until further frameworks are developed and adopted.

More recently, DIACC alongside SecureKey and more than 20 of DIACC's members officially launched and began testing for the Pan-Canadian Trust Framework – a model that will make it easier for Canadian users and businesses to interact online with a high degree of confidence and trust. This initiative sets a streamlined framework of digital ID standards and requirements in place that will guide identity innovation moving forward.

This uncertainty in liability required additional processes to be taken by Verified.Me in drafting new agreements for each network participant on the network to mandate certain performance levels, security requirements, and compliance with privacy and other laws (SecureKey, 2019). Agreements between SecureKey and service providers prohibit the use of subject information for purposes other than the approved sharing transaction (SecureKey, 2019), which also helps satisfy the SSI principle of minimalization. Trust frameworks are both procedural and contractual, but support network effects that eliminate pairwise service and contract negotiation.

In addition to the six main imperatives from the Commission on Enhancing National Cyber Security, it was also stated that preserving innovation and ease of use should be a priority moving forward, which countered the prevalent approach of pushing security to the edges of the network. The ease of implementation for other identity and relying parties, user adoption challenges, and interoperability between organizations and different decentralized identity systems are additional

challenges for any decentralized digital identity to be effective for all parties involved (SecureKey, 2020).

From a programmatic perspective, the requirement for all network participants to coordinate, align, and execute on a single launch date was an important undertaking. The planning and execution complexity required in partnership with organizations and within each of those organizations and lines of business were important considerations for the program management team to guide all of the technical, business, and operations teams from all partners. A strong project management office is essential for managing the launch and for any potential crises or detriments that occur in the prelaunch and launch periods (SecureKey, 2020).

For the postlaunch period, the necessity of ongoing management of the ecosystem is another potential constraint for the implementation of a decentralized digital identity system. Adding new parties, monitoring, managing changes and incidents, and end user support are all required elements. Designing, testing, and operationalizing these will be a long-term driver of user and partner satisfaction (DIACC, 2020). The SSI principles guiding this decentralized digital identity network must also be maintained throughout this process, requiring the commitment of all partners on the network to ensure the ongoing success of the network.

While not every digital identity ecosystem will be developed on Verified.Me's scale, it is worth noting that bringing a new system to market based on new blockchain technology will present another set of challenges given the lack of existing resources, references, and lessons to learn from in comparison to centralized digital identity networks (DIACC, 2020). The requirement for this infrastructure and new technology to be scalable to accommodate additional partners over time and resilience to cyber threats is another concern. For Verified.Me, the baseline plan was constantly adjusted to accommodate the additional time required to manage evolving operational, infrastructure, and compliance requirements (DIACC, 2020), and similar efforts will require similar flexibility.

As service delivery organizations gain further knowledge of blockchain technology, and established legal and governance frameworks are developed, there is an anticipation that the technology's prominence and level of participation will increase for businesses, as well as a need for information technology professionals to understand how to use it. The more prominent SSI initiatives with blockchain become, the more likely it will be for organizations to observe and adopt.

CONCEPTUAL BLOCKCHAIN IMPLEMENTATION

Before providing detail on blockchain is being used in the approach presented, it is important to understand that no personally identifiable information (PII) is being stored on chain. Storing PII on chain is privacy degrading in the first instance because the data would be replicated across the verifier nodes, the number of which may increase over time. Getting advanced consent is problematic in that you would be asking the user to agree to share with a party not yet identified. Second, if a user asserts the manifest right to be forgotten, the only way to honor their wish is to delete the whole blockchain.

Blockchain fulfilled three key requirements in a network approach to digital identity:

1. A method to provide triple-blind data sharing under user control and consent while maintaining high business integrity (making it trustworthy to the relying party).
2. A method to compute and record integrity proofs about the data shared.
3. A method to mitigate distributed denial of service attacks owing to the larger number of service endpoints that can provide stand-in processing.

Triple-blind data sharing allows the data to move from the source to the destination service the user chose while mutually blinding the source and destination from each other. The network functions as a blind postal service that delivers the hash address and half of the decryption key, and network address to pick up the payload. The second half of the decryption key is delivered directly from the user agent on the user's mobile phone. The relying party can retrieve the payload and decrypt the payload by assembling the two keys together. This means neither the source, destination, nor the network operator receives a complete picture of the user transaction.

Of integrity proofs, there are three key computations:

1. User chose to have a payload computed and held by the source.
2. The user directed the payload to be sent from the source to the destination.
3. The destination was retrieved and decrypted the payload (to activate the license to the user data).

There is a method for the relying party to compute a hash of the data payload and compare it to the hash that was recorded by the source of the data on chain at creation-time.

This methodology meets the three requirements of trusted data as described above. Trusted means:

(1) a known and trusted source because only trusted sources can write on chain,
(2) knowing that data have not been altered since it was issued by that source because the hashes computed by the source and destination match, and
(3) that data belong to the person presenting them because only the user agent could cause delivery of the payload to the destination.

CONCLUSION

This article introduced how SecureKey worked with various network participants and innovation partners, alongside government, corporate, and consumer-focused collaborators, in a consortium approach to create a mutually beneficial network of SSI principles with blockchain in Canada, a network based on triple-blind privacy, designed to work across the economy under

the control and direction of the user with higher integrity, lower cost, and customer experience benefits for businesses. Through Verified.Me, arguments for the usage of blockchain-based services that bake the SSI philosophy into their foundation were presented to demonstrate its benefit to organizations and users alike. Despite the challenges associated with adoption, implementation, and the current lack of regulatory restrictions, decentralized digital identity continues to increase in usage in Canada while the global identity landscape shifts to a wider acceptance of SSI with blockchain and a better understanding of the benefits of doing so.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

The author confirms being the sole contributor of this work and has approved it for publication.

REFERENCES

Allen, C. (2016). *The Path to Self-Sovereign Identity*. Available online at: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (accessed September 15, 2020)

Commission on Enhancing National Cybersecurity (2016). *Report on Securing and Growing the Digital Economy*. Available online at: https://www.nist.gov/system/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf (accessed September 15, 2020)

De Filippi, P. (2016). The interplay between decentralization and privacy: the case of blockchain technologies. *J. Peer Prod.* 7:hal–01382006.

Der, U., Jähnichen, S., and Sürmeli, J. (2017). Self-sovereign identity $-$ opportunities and challenges for the digital revolution. *arXiv [Preprint]* doi: arXiv: 1712.01767

DIACC (2020). *Consumer Digital Identity Leveraging Blockchain*. Available online at: https://diacc.ca/wp-content/uploads/2020/03/DIACC-White-Paper_Consumer-Digital-Identity-Leveraging-Blockchain_Feb2020.pdf (accessed September 15, 2020).

Gigya (2015). *The 2015 State of Consumer Privacy & Personalization*. Available online at: https://www.slideshare.net/Gigya/white-paper-the-2015-state-of-consumer-privacy-personalization (accessed September 15, 2020)

SecureKey (2019). *Consumer Digital Identity Leveraging Blockchain*. Available online at: https://verified.me/wp-content/uploads/2019/05/DIACC_Phase2_SK-2019-FINAL.pdf (accessed September 15, 2020).

SecureKey (2020). *A Primer and Action Guide to Decentralized Identity*. Available online at: https://securekey.com/wp-content/uploads/2020/07/VerifiedMe_OWIWhitepaper_APrimertoDecentralizedIdentity.pdf (accessed September 15, 2020).

Smits, M., and Hulstijn, J. (2020). Blockchain applications and institutional trust. *Front. Blockchain.* 3:5. doi: 10.3389/fbloc.2020.00005

van Wingerde, M. (2017). *Blockchain-enabled self-sovereign identity* Doctoral dissertation, Master's thesis. Tilburg: Tilburg University.

Wang, F., and De Filippi, P. (2020). Self-Sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion. *Front. Blockchain.* 2:28. doi: 10.3389/fbloc.2019.00028

Zwitter, A., Gstrein, O., and Yap, E. (2020). Digital identity and the blockchain: universal identity management and the concept of the "Self-Sovereign" individual. *Front. Blockchain.* 3:26. doi: 10.3389/fbloc.2020.00026

Conflict of Interest: AB is employed by the company SecureKey Technologies Inc.