Verified.Me®

A Primer and Action Guide to Decentralized Identity

Introduction

In an increasingly digital world affected by ever-mounting fraud and privacy concerns, digital identity and the security and assurance of identity data is becoming a crucial consideration for public and private sector organizations. However, digital identity as it currently exists with its centralized username and password focus, is insufficient for solving the identity problems we face. When stark use cases like data portability and user control are presented, it's clear that our existing solutions don't represent true identity – standalone biometric selfies matched with photo IDs do not make a strong digital identity – and that decentralized digital identity enables much more flexibility.

Along the spectrum, there are solutions that repurpose physical identity modalities for digital credentials. These "point solutions" (i.e. Jumio, Yoti and Plaid) act as placeholders but do not fulfill important principles of identity. Most recently the self-sovereign identity (SSI) community has entered the fold with a renewed interest in creating user-centric identity solutions that adhere to technological principles. Verified.Me by SecureKey Technologies Inc., aims to bridge the gap between these two approaches by providing a robust, principled identity network that relies on technical standards, governance frameworks and active user behaviour as the three pillars of a trusted ecosystem.

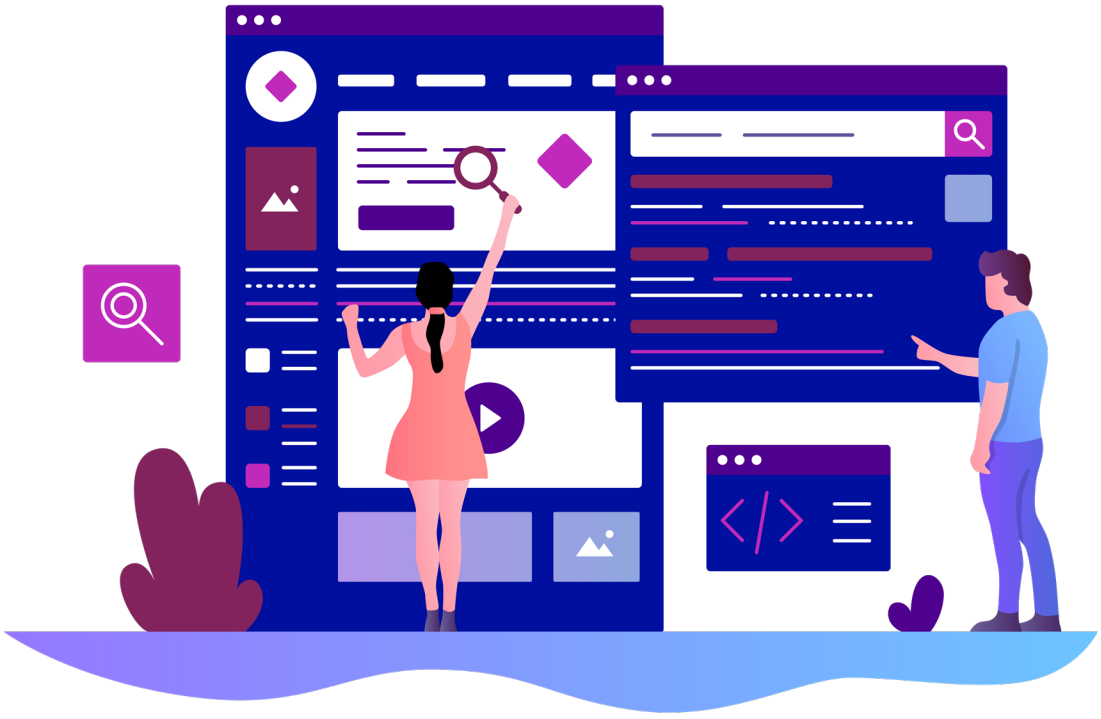
An Overview of Digital Identity Management

What are the ways by which digital identities are created and managed? This paper will delve into the market positioning and perception of centralized and decentralized identity schemes, focusing on SSI, federated identity, SecureKey Technologies' Verified.Me hybrid decentralized identity verification network and their respective strengths and weaknesses. Lastly, this paper will offer a potential path forward for a trusted digital ecosystem crafted by robust partnership and collaboration.

The Status Quo: Centralized Digital Identity

Digital identity arises from the use of personal information on the internet, as well as the data and behaviors generated through online actions. Currently, digital identity management is predominantly conducted through centralized identity schemes used by organizations to create discrete identities within their individual online properties, allowing for access and use of their platforms, services and software. The challenge when users have a fragmented identity experience on the internet as a whole is frustration, an increased attack surface, and higher risk identity proofing outcomes for business.

Centralized identity systems come in many forms, from enterprise identity and access management systems, to social media accounts, to government identity issuance. Individual industries demand robust IT infrastructures that are customized to the nuances of their day-to-day operations. Organizations rely on Identity-as-a-Service and identity and access management solutions that allow individuals to use a single set of credentials across their network of resources and may allow identities, such as a user's social identity from a social network, to be imported and used to access resources. These solutions are differentiated from federated identity by their lack of external applications beyond the organization's network. They also typically feature one set of credentials, generally a username and password combination, that allows for access to one organization's network or platform. In addition, they often involve identity verification (document scanning, knowledge confirmation) during the initial onboarding process (in fact, it is mandatory for regulated industries such as financial services) and additional authentication (such as facial biometrics or multi-factor authentication) upon log-in attempts.



While centralized identity systems are the most widely accepted method of identity management to date, they have several crucial flaws. Fundamentally, centralized identity systems store sensitive personal data, resulting in honeypots of valuable information likely to be targeted in data breaches. This proves to be a significant risk, as data breaches have increased significantly in recent years in

frequency as well as cost to businesses.[1] [2] Consequently, organizations can never really know if the data they are being given is being presented by the person it belongs to, because it can neither be verified against the source nor correlated with the person presenting it.

Furthermore, centralized identity systems offer limited to no interoperability between platforms and organizations – many of whom are unwilling to share proprietary data points collected from their users, both from an economical and legal standpoint. This limited data sharing allows for the formation of "walled gardens", where one carrier and/or service provider controls its applications, content and data, preventing both individuals from taking control of their identities, as well as competitors from gleaning proprietary knowledge. Beyond these pain points, however, lies the impending hurdle of future technological trends that have the potential to disrupt our current paradigm, namely quantum computing. All systems as we know them that rely on modern digital encryption will be disrupted with the advent of enterprise quantum computing, which possesses the potential to break existing cryptography in a matter of minutes.[3] Widespread adoption of quantum computing in the upcoming decades will fundamentally change the ways by which all privacy and cybersecurity protocols are designed, implemented and enforced.[4]

As the workforce becomes increasingly remote both organically and as a result of extenuating circumstances,[5] [6] organizations are looking into new solutions that can better accommodate a flexible working environment, with personal devices and distributed networks.[7] Simultaneously, after high-profile data breaches and data abuses, users are becoming more aware of the lack of control and privacy they possess over their data and digital identities. The COVID-19 pandemic highlighted the value and desirability of having a 'touch-free' document presentation and user onboarding, but it also emphasized how there must be high-trust to be viable. Digital ink over wet ink for document signing is also required for touch-free and online transactions – but we need to know who signed the documents. In today's socioeconomic environment, decentralized identity is coming into the spotlight as an extremely viable alternative to existing centralized systems.

The Change-makers: Decentralized Identity

In this whitepaper, we will segment decentralized identity into three categories: SSI, federated identity and hybrid decentralized identity (a combination of centralized identity, SSI principles and federated identity frameworks).

Self-Sovereign Identity

SSI is a philosophical perspective on an approach to digital identity. SSI is an emerging market based on the concept of placing ownership and control of all digital identity attributes into the hands of the user, such that individuals retain management of their digital identity (i.e., the user is "sovereign" over the digital identity of their own self). SSI is often distinguished from current methods/practices by the use of a secure distributed ledger technology and shifting more power and decision authority to the user.

The philosophy has many different implementations, but all are rooted on ten principles defined by Christopher Allen:[8]

Existence: Users must have an independent existence. Note: This sometimes presumes that everything must be documented to exist. We disavow that notion and respect that there is an inherent quality to existence and a right to remain unknown in certain contexts.

Control: Users must control their identities. Note: The focus is specifically on control and not ownership (e.g. you don't own your passport, the State does, but you want the right to control the use of it).

Access: Users must have access to their own data.

Transparency: Systems and algorithms must be transparent. Note: To this end, the foundation of all technology solutions to enable SSI must be open source.

Persistence: Identities must be long-lived.

Portability: Information and services about identity must be transportable.

Interoperability: Identities should be as widely usable as possible.

Consent: Users must agree to the use of their identity.

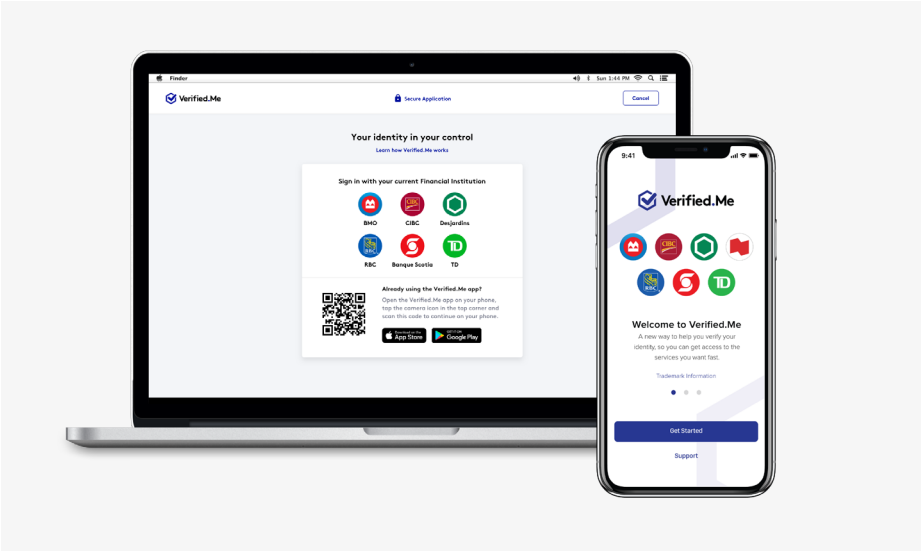
Minimization: Disclosure of claims must be minimized.

Protection: The rights of users must be protected.

The concept of SSI itself is still being debated and while SSI has received significant attention in the past few years, the product type is still nascent.

Federated Identity

Federated identity management is the reliance on one system or organization to manage user authentication for a group of organizations. This allows users to use the same identification data and credentials to access the applications, programs and networks of all members of the group. Federation differs from single sign-on through its extension beyond a single organization, allowing for single-point access to multiple systems across different software. Successful identity federation hinges on trust in one organization to conduct IDV for the group.



Federated identity systems that consumers may recognize include social logins such as Sign In With Facebook and Sign In with Gmail. Eighty-eight per cent of U.S. consumers have used social logins, relying on Facebook or Google to conduct any necessary authentication through an existing user account.[9] Other federated identity systems include the U.S. government's Login.gov, a shared authentication platform that enables access to services from numerous government agencies that do not otherwise share a network or platform, as well as SecureKey Concierge, a widely adopted federated authentication system in Canada that leverages financial institution credentials without providing PII.[10]

Verified.Me: A Hybrid Solution – SSI+

Verified.Me by SecureKey Technologies Inc., is a decentralized network solution for digital identity verification. The service involves multiple participants working together within an ecosystem to securely and privately help verify the identities of eligible individuals wishing to engage with a variety of online services in Canada.

The Verified.Me service's underlying network is managed and facilitated by the network owner, SecureKey Technologies Inc., in order to ensure the service is as safe, private and useful as possible. The service is also supported by a variety of other parties called network participants. This group includes identity & data providers and relying parties. [11]

Financial institution identity & data providers include seven of Canada's major financial institutions, which are responsible for helping to verify end-users wishing to use the Verified.Me service and for hosting the core components of the network. Relying parties, also known as service providers, are eligible organizations in Canada that participate in Verified.Me and ask users to provide certain information through the service to facilitate desired transactions. One example of these transactions includes helping verify identities and/or eligibility for product or service offerings. While Verified.Me continues to expand in scope, existing and anticipated service providers include but are not limited to financial institutions, insurance companies, telecommunications providers, online merchants and

healthcare solutions.

Verified.Me and the network owner, SecureKey Technologies, also advocates for many of the SSI principles, placing emphasis on control, privacy, minimization and consent. Verified.Me's progress contributes to the overall development of decentralized identity standards, such as with the Decentralized Identity Foundation by core support for the Decentralized Identifiers (DID) specification, and SecureKey Technologies plans to register Verified.Me as a DID method. In addition, SecureKey Technologies is a founding member and active contributor to the Digital Identity and Authentication Council of Canada (DIACC), as well as the World Wide Web Consortium (W3C), 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.

However, rather than emphasizing "sovereignty" or possession, Verified.Me prioritizes exclusive user control over data. For example, Verified.Me coordinates with relying parties to accommodate account recovery protocols to satisfy the requirements of both parties, allowing for a more user-friendly account recovery process and lowering the likelihood of the permanent loss of keys and credentials. In this way, Verified.Me combines the advantages of federated identity and SSI to create a service that is interoperable, secure and user-friendly.

Verified.Me is neither a service nor a technology. Verified.Me is SSI+.

Existing Challenges

While opportunities are available for decentralized identity, there are still a number of hurdles that stand in the way of widespread adoption. The regulatory landscape is uncertain and likely to garner attention and witness compelling changes as awareness and adoption increase. Furthermore, decentralized identity providers must consider ease of implementation for other identity providers and relying parties, end-user adoption challenges and interoperability not only between organizations, but also between different decentralized identity systems.

Undefined Liability

Currently, North America lacks specific regulatory restrictions on SSI and decentralized identity. However, private organizations must comply with data privacy regulations, as well as industry specific requirements. Decentralized identity is especially impacted by data privacy regulations such as Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR; applies to all organizations conducting business in the European Union), which limit data portability and require user consent prior to data collection and usage.

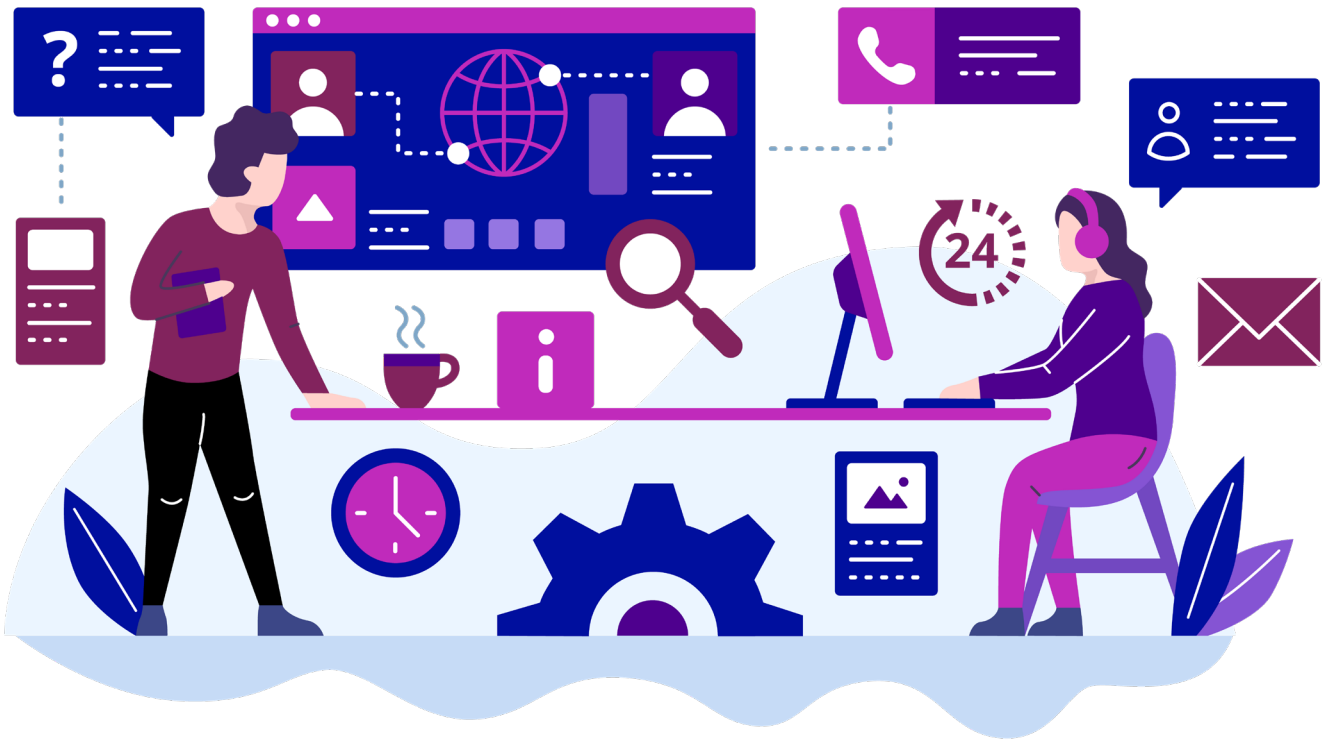
SSI solutions have gained support among governments and private sector players, however, there is a lack of governance frameworks (i.e. agreements between identity providers and service providers), resulting in limited liability assurance. Consequently, many organizations have been hesitant to embrace decentralization due to lack of defined liability structure. For example, financial institutions are required to conduct customer due diligence to prevent money laundering and other fraudulent actions. If a bad actor is permitted into a network due to an error in verification or authentication conducted by another party, it is unclear who would be held accountable. Subsequently, due diligence

processes, such as know your customer (KYC), cannot purely rely on SSI until further frameworks are developed and adopted. In order for decentralized identity schemes to be more widely adopted by both private and public entities, the regulatory requirements and frameworks must be further developed.

To overcome this liability uncertainty, Verified.Me enters into comprehensive agreements with each network participant in the Verified.Me service mandating certain performance levels, security requirements and compliance with privacy and other laws. In addition, agreements between SecureKey and service providers prohibit the use of subject information for purposes other than the approved sharing transaction. These arrangements ensure that Verified.Me provides a safe and secure environment for users sharing their data. The service itself holds no personal information. The primary recourse that individuals have is via the Verified.Me service terms and privacy notice, any existing agreements between individuals and data providers and agreements between individuals and service providers they choose to share information with.

Furthermore, Verified.Me enables service providers to select or request only the attributes needed for business purposes. This improves their ability to meet regulatory requirements for data minimization. Data protection is at the core of the design of Verified.Me. The service embraces the "privacy by design" approach and is intended to exceed data protection requirements – both federal and provincial. Data providers and service providers are also required to meet all relevant data protection requirements. The agreements with data providers and service providers place specific requirements on them, to ensure the protection of personal information across the serviceand to define clear boundaries of responsibility.

Industry Ease of Implementation



Federated identity is likely to be the most technically straightforward to implement, as a designated federated identity provider would be responsible for all ongoing and future verification, authentication and authorization. There is already significant pressure on organizations to implement social login, with 86 per cent of users feeling hindered by new account creation processes.[12] However, many organizations are unlikely to place such a sensitive responsibility (not to mention foregoing valuable data sources) in the hands of third-parties, especially heavily regulated industries such as financial services. This makes the widespread adoption of any one provider challenging.

Verified.Me's consortium model of trust chooses which identity providers are trustworthy. For organizations who highly value privacy or have strict privacy mandates, the concept of outsourcing trust to a group of institutions may be difficult to accept. The ecosystem approach requires that all players agree to changes – a thorough approach that requires significant time commitment. However, this method ensures that all parties involved are thoroughly vetted and reliable, each providing secure and thorough identity management processes and reliable data. Furthermore, Verified.Me uses a Triple Blind™ model that ensures data privacy between the user, network owner and network participants. The underlying blockchain foundation follows strong security protocols to prevent personal information from being identified, accessed, or misused.

Consumer Adoption / Friction

Interaction friction refers to required actions a user experiences when interacting with a product's interface and covers all aspects of the UI that may be hindering users from accomplishing their goal. For the most part, federated social login solutions offer consumers minimal friction for accounts that have already been created. Federated identity in the form of social login benefits from widespread end-user adoption and awareness, with more than 88 per cent of U.S. consumers having used social logins. As the world becomes increasingly digital, consumers are developing increasing password fatigue and expecting more seamless digital experiences. In fact, consumers' top reasons for using social logins are to avoid filling out yet another form and to avoid remembering yet another set of credentials. As such, adoption of social login reduces the cognitive friction required when onboarding onto another platform.

However, despite widespread adoption, social login and federated identity as a whole must overcome emotional friction. Consumers are becoming more aware of data privacy issues and are increasingly hesitant to allow social media companies with unfettered access and ownership of their identity data.[13] Consumers are similarly concerned about the misuse of their data collected in accordance with organizations' security practices. Consumers have been given good reason to believe that reliance on social login may be disastrous if the account is breached by a cyberattack, leaving a multitude of platforms and networks open for exploitation.

SSI, on the other hand, faces significant amounts of both interaction and cognitive friction. As a bottom-up approach to identity that requires every user to control their own identities, SSI faces a steep user learning curve to understand its purpose. This is partially as a result of both the movement's focus technical standards over user experience and its requirement that users handle their own security.[14] More importantly, many SSI solutions provide ineffective recourse if credentials are lost. SSI solutions have traditionally struggled to create user-friendly solutions that provide recourse should a user lose access to their wallet or be hacked, while still adhering to principles of digital privacy and user-centricity. In many cases, recovery is very challenging, leaving users hesitant to adopt a new,

technically challenging product that may result in permanent loss of sensitive, high-value data and resources.

As a hybrid between federated identity and SSI, Verified.Me reduces interaction and cognitive friction. The service accomplishes this in a number of ways, namely by:

- Enabling streamlined verification and authentication processes and leveraging the due diligence already conducted by trusted identity providers within the service;
- Heavily emphasizing data privacy through its Triple-Blind™ capabilities, easing emotional friction and concerns about data abuse by third parties; and
- Embedding explicit user consent into every step of a transaction within the Verified.Me service.

When using the Verified.Me service, users have control over their data sharing via the need for explicit consent before any data or attributes are shared. Subjects are provided with a clear understanding of what data is being requested by the service provider and the purpose for which the data is being requested. Armed with this information, subjects can make meaningful decisions on whether to share their data.

While users have full control over data sharing, they are not required to take ownership of the security of their personal data. By combining elements of federated identity and SSI schools of thought, Verified.Me allows for the least amount of user friction, allowing users to focus on self-management of credentials and data.

Interoperability

Federated identity provides limited interoperability between organizations – the only data transmitted are between the identity provider and the relying party, with no capacity for relying parties to communicate with each other. However, the same credentials are used for all relying parties and the group members can leverage existing verification and authentication results for their own use.

Both technical standards and governance frameworks are required to uphold trust and foster interoperability in SSI networks. Technical standards are well-established, continue to see active development from developers and are widely adopted across the world. Growing understanding of the importance of governance frameworks will encourage public and private sector adoption, but these frameworks are often siloed into certain groups or networks and remain nascent in development when compared to technical standards.

Verified.Me works with its partners to ensure continued enterprise-grade compliance with regulatory privacy and security mandates. Verified.Me also incorporates in monetary incentives to bring network participants on board. In addition, the network's technology has been successfully applied to interoperability-focused initiatives including with the W3C, DIF, TrustBloc DID and the U.S. Department of Homeland Security's Science & Technology Directorate (DHS S&T) – specifically the Silicon Valley Innovation Program (SVIP). SecureKey Technologies recently completed a project combining elements from W3C and DIF standards in a demonstration with DHS. Further, the Verified.Me network was built by leveraging Hyperledger Fabric v1.2+ and will be interoperable with Hyperledger Indy and Aries projects.

TrustBloc DID is a SecureKey open-source initiative to increase interop for decentralized identity. SecureKey Technologies' open-source initiative to increase interop for decentralized identity. Its aim

is to establish common standards and development frameworks for next generation digital identity networks. The initiative provides a common infrastructure for consortium members to enable data provenance and exchange, while still allowing these consortium networks to differentiate based on their service offerings. TrustBloc is enabling DIDs – decentralized identifiers from any source – to be managed and leveraged from Fabric, and more generically enabling document provenance. The following features are early goals of the initiative:

- Provide out-of-the-box capabilities for document provenance (including DIDs).
- Enhance Hyperledger Fabric private collections to support SideTrees, allowing identifiers and documents to be anchored to a channel without performing individual Hyperledger Fabric transaction for each identifier or document.
- Enable off-chain distributed storage model to support transactions (e.g., transient storage, content-addressable storage).
- Support a storage and query model for data scoped to a particular organization.

Simply put, TrustBloc DID's support of new networks, data sources and data sharing agents will help organizations invest in and roll out interoperable solutions with confidence.

To date, Verified.Me is the only service able to demonstrate full interoperability with other networks.

You can learn more about TrustBloc here: https://trustbloc.readthedocs.io/en/latest or https://github.com/trustbloc/bloc-docs/blob/master/docs/source/index.rst

Benefits of and Opportunities for Decentralized ID

Despite the existing challenges, decentralized identity provides many benefits and has ample opportunity for growth. Federated identity, SSI and hybrid solutions like Verified.Me are able to improve the network and platform security of organizations, place control back into the hands of consumers and interoperate between networks for increased portability and reusability of identity attributes.

Opportunities and Use Cases

To encourage organizational implementation, decentralized identity providers must build up governance frameworks to increase network trustworthiness. Currently, the DIACC is building a governance model called Pan-Canadian Trust Framework (PCTF) for digital identity. This will encourage organizations – often those that were previously skeptical of the assurance levels of decentralized identity–because it sets standards for verification and authentication alleviate organizations' primary concerns.

Furthermore, in an age where data privacy and transparency are key concerns, decentralized identity companies should appeal to consumers' desires to control their personal data, directing the power and profit away from organizations like Big Tech to individuals. In this sense, SSI and hybrid solutions are more likely to succeed, as most federated identity schemes currently rely on organizations who control and manage identity data. Identity providers that offer a seamless user experience, ease of implementation and strong interoperability will likely see the highest adoption from both enterprises looking for identity management solutions as well as end-users looking for straightforward log-in flows without additional friction.

Governance and public safety aside, successful and widespread adoption of decentralized identity would be beneficial for nearly every industry. Financial services providers could conduct KYC due diligence and onboard potential customers more efficiently, without reauthenticating previously screened users and related organizations. Healthcare providers could use decentralized identity to tackle everything from medical file access to immunity proofing–in the case of COVID-19, this concept is already being explored. Public sector agencies could provide more seamless methods of access to cumbersome legacy process flows. By implementing decentralized identity solutions, organizations from all industries can reduce resource inefficiencies and improve their trust and safety frameworks, while easing the burden on end-users.

Indeed, examples of decentralization are emerging globally. Market highlights naturally include Verified.Me, in addition to Shyft Network's partnership with the Bermuda government to provide $10 million in blockchain education and development,[15] and Rabobank's exploration of SSI to replace its existing KYC process and internal credential management system.[16] These examples improve internal employee onboarding, end-user due diligence, public awareness and data portability, highlighting the multitudinous benefits of decentralized identity schemes.

Final Analysis

Each of the showcased decentralized identity solutions have their benefits and drawbacks. Federated identity, with its visibility through social logins, demonstrates a network that is easy to use and implement, but may cause data privacy and ownership concerns. SSI is a pure and philosophical approach to digital identity, demonstrating an ardent perspective of the necessary components to true identity sovereignty, but has a steep technology learning curve and limited productization.

Verified.Me is the bridge between decentralized and centralized identity, merging the seamless flows of federation alongside the principles of SSI and the established requirements of centralized identity management. This combination of strengths results in higher data privacy and empowers users to embrace agency over their digital identity, while streamlining identity flows for organizations and enabling portable identity credentials.

Ultimately, while each decentralized identity provider strives to become a dominant player in the digital identity market, interoperability between solutions is key to successful adoption of decentralized identity. The decentralized identity community is actively working on interoperability standards so that data can be exchanged between their platforms. By working together and pooling their organizational partners and users, players can drive adoption and advance the vision of an internet identity layer, driving access to digital services while maintaining data security and user control.

Decentralized identity solves many of the pitfalls of the centralized identity management tools currently in use. Private and public sector organization should consider the implementation of decentralized identity to tackle the growing problems posed by fraud, inefficiency and efficacy. In today's increasingly digital landscape, data privacy, trust and safety are coming to the forefront of awareness. Decentralized identity providers should work together to address these concerns.

Sources:

1. U.S. Financial Services Companies See Average Cost of Fraud Rise 9.3% from 2017 to 2018, LexisNexis Risk Solutions Survey Finds (link)
2. 2019 Data Breach Hall of Shame (link)
3. Quantum Computing Poses An Existential Security Threat, But Not Today (link)
4. Quantum Computing: How Soon Will It Become a Mainstream Reality? (link)
5. 159% Increase in Remote Work Since 2005: FlexJobs & Global Workplace Analytics Report (link)
6. What COVID-19 Means For the Future of Remote Work (link)
7. The Challenges and Benefits of Identity and Access Management (link)
8. The Path to Self-Sovereign Identity (link)
9. Gigya Survey: 88% Of U.S. Consumers Say They Have Used Social Logins (link)
10. SecureKey Concierge (link)
11. About Verified.Me (link)
12. Social Login and CRO: 9 Things You Should Know (link)
13. How Cambridge Analytica Sparked the Great Privacy Awakening (link)
14. Can LESS be more? (link)
15. Bermuda Starts Development of a Blockchain-Based National ID System (link)
16. Self-Sovereign Identity at Rabobank: Interview with one of Rabobank's Blockchain Specialists, David Lamers. (link)

For more information visit www.verified.me

Verified.Me®

In collaboration with OWI

ONE WORLD IDENTITY