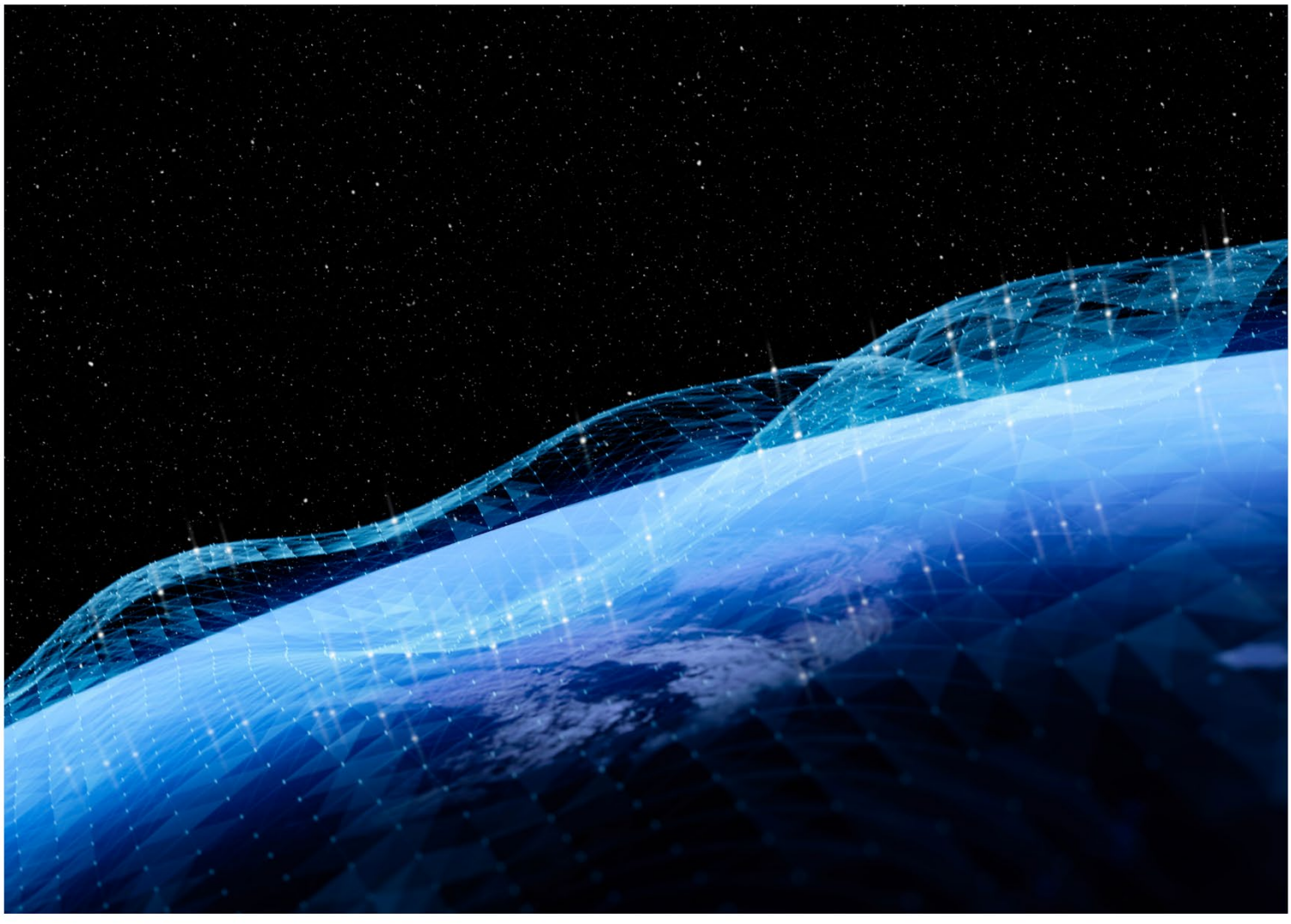
GBBC
Global Blockchain Business Council

INSIGHT REPORT

GLOBAL STANDARDS MAPPING INITIATIVE (GSMI) 2.0
STANDALONE REPORT

DIGITAL IDENTITY

November 2021



The GBBC would like to thank our many partners, members, and supporters who worked tirelessly and enthusiastically over the past months to produce this standalone report as a part of GSMI 2021, version 2.0.

Contributors

Tangem	James Loperfido (co-chair)
SITA	Arnaud Brolly (co-chair)
University of Dundee	Mya McCalmont (GSMI fellow)
Affinidi	Sandeep Bajjuri
Blok Solutions	Alex Tai
Cloud Compass Computing	Stephen Curran
Continuum Loop	Darrell O'Donnell
Government of Bermuda, FinTech Business Unit (FBU)	Marcus Wade
HHS	Darryl Burton
Hyland	Natalie Smolenski
Indicio.tech	Sumiran Agarwal
Lumedic	Jim St. Clair
MetaMe	Dele Atanda
OpenID Foundation	Don Thibeau
Sky Republic	Chris Fabre

Executive Summary

"The only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others." - John Stuart Mill from “On Liberty”

The rapid deployment of global decentralized networks has created large gaps with respect to data disclosure, financial transactions, and privacy related to digital assets. Digital assets come in many forms, but the COVID-19 pandemic and rapid development of Web 3.0 decentralized networks has incited a need for a foundational, global, interoperable framework for modern “digital identity” and its correlates. The inability to prove COVID test and vaccine credentials has quickly become a prime example of the need for global standard harmonization to issue, maintain, share, and verify credentials in critical situations. These pieces of personal data also carry value, which can be protected and exchanged on decentralized ledger technologies (DLT) with the individual in control. Beyond that goal, decentralized exchanges (which are often autonomous with no central governing body), and non-custodial wallets make it difficult for regulatory and enforcement agencies to prevent illicit activity with current know your customer/anti-money launder (KYC/AML) protocols.

Decentralized identity solutions, sometimes referred to as “self-sovereign identity” (SSI) frameworks, have been recommended for many use cases, align well with the United Nation’s Sustainable Development Goals (SDGs), especially SDG 16,[1] and can serve as a foundation for Web 3.0 and beyond. Applications include globally interoperable frameworks for government, healthcare, finance, and even physical interactions. In combination with biometrics, digital asset wallets, and other technologies, SSI may serve as a foundation to enhance KYC and AML integrity while enabling financial access for the unbanked and underbanked. It can help remedy archaic administrative costs in different verticals like healthcare and financial services. A decentralized approach to identity can also offer vulnerable populations some form of documentation by which they can verify their identity for issuance of first aid, food, water, and other essentials in times of crisis. Reports suggest over a billion people lack proper identification.[2]

In a growingly complex global internet and financial system, black swan events can pose greater economic risk. The right to owner-centric control becomes a prerequisite to digital identity and its corollaries constitute basic human rights. To ensure personal identity and related data are protected, the individual should have the option to take complete ownership and

custody of her data. Shifting of trust to the edges of communication networks also has the potential to reduce complexity and increase security.

As of this writing, many tools, businesses, and pilots are being deployed; standards for verifiable credentials (VCs), DID (decentralized identifier) methods, and other technical issues are being developed in tandem. Beyond solving for the aforementioned problems, SSI and DLT solutions can create automated transactions with triple entry accounting, a careful balance of transparency and privacy, and a more robust and efficient global economy.

Potential Digital ID Applications

- Security Breaches
    - Based on the FYEO Breach Database, the average internet user has been exposed more than three times.
    - Whether users say they care, most do not use any solutions designed to this point - either password managers or two-factor authentication (2FA) - without mandates.
    - Cybercrime is estimated to be a $1.1 trillion burden on the global economy (1.3% of global GDP), forecast to rise by 2023 to $2.7 trillion (2.8% of global GDP).
    - Cyber risk insurance coverage is only $1.0 trillion as underwriting standards tighten so enterprises need better Identity & Access Management (IAM) solutions.
    - The average “Value At Risk” (VAR) for Global 2000 corporates from cyberattack is 3% of market capitalization, an average of $4.9 billion.
    - 2021 FYEO Report on Identity
- Denial of basic human rights
    - More than 1.5 billion people are excluded from accessing basic services due to their inability to prove their identity. A large majority of these people are in Asia and Africa, in areas that lack the proper infrastructure to register births and other life events. According to the UNHCR, there are currently over 70 million forcibly

displaced people as a result of conflict or persecution, 25 million of which are refugees — mostly from Syria, Afghanistan, and South Sudan. There are also approximately four million stateless people, who have been denied a nationality, and therefore have been prevented from access to basic services and rights.

- Immigration standards and recognition of foreign credentials
- Loss of fidelity in healthcare records when patients switch doctors, hospitals, insurance plans, or states of residency due to data siloing and separate registries
- Incompatible cross-state registries for vaccines and other essentials
- Centralized storage creates “treasure trove” incentivizing hackers to focus on one vector

Key Definitions:

Government Issued/attested primary credentials and identifiers	National IDs like Social Security Number, Passport, Driver's License, and birth certificates
Attestation	Acknowledged evidence or confirmation of the existence of something, whether by an individual or organization.
Credential	A qualification, trait, achievement, or authority assigned to a person or entity which can be issued in physical or digital form
Digital Identity	Identity issued by an organization that is considered to be either "Siloed" or "Federated."[3]
Federated Identity	The means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems. Federated identity is related to single sign-on (SSO), in which a user's single authentication ticket, or token, is trusted across multiple IT systems or even organizations. SSO is a subset of federated identity management, as it relates only to authentication and is understood on the level of technical interoperability and it would not be possible without some sort of federation.[4]
Decentralized Identifier (DID):	A globally unique identifier developed specifically for decentralized systems as defined by the W3C DID specification. DIDs enable interoperable decentralized Self-Sovereign Identity management: A DID is associated with exactly one DID Document.[5]
Decentralized Identity	A portable set of identity credentials (which may be issued or attested to by third parties) controlled by the individual owner in a digital wallet underpinned by a DLT platform.[6]
Self-Sovereign Identity	An identity system architecture based on the core principle that identity owners have the right to permanently control one or more identifiers together with the usage of the associated identity data[7]
Verifiable Credential	A specific digital form of credential that can represent all of the same information a physical credential represents. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts. Holders of verifiable credentials can generate verifiable presentations and then share these verifiable presentations with verifiers to prove they possess verifiable credentials with certain characteristics.[8]
Zero-Knowledge Proof	A Proof that uses special cryptography and a Link Secret to support Selective Disclosure of information about a set of Claims from a set of Credentials. A Zero Knowledge Proof provides cryptographic proof about some or all of the data in a set of Credentials without revealing the actual data or any additional information, including the Identity of the Prover.[9]

Principles and Solutions

Numerous institutions and individuals have proposed principles of identity, as shown in the table below. This working group has identified five essential principles for digital ID.

Table 3: Various "Principles of Identity"

Kim Cameron [125] (2005)	Chris Allen [126] (2016)	World Bank [127] (2017)	ID 2020 [128] (2017)	WEF [129] (2018)	Access Now [130] (2018)
	Existence	Universal Coverage	Universal Coverage	Existence	
User Control and Consent	Control	User Privacy and Control	Control	Control	Control
Human Integration	Access	Remove Barriers to Access and Usage	Access	Access	Access
	Transparency	Open Standards	Open Standards	Transparency	Transparency
	Persistence	Sustainability	Persistence	Persistence	Persistence
Consistent Experience Across Contexts	Portability	Independent Oversight	Portable	Transportable	
Pluralism of Operators and Technology	Interoperability	Interoperable and User-Responsive	Interoperability	Interoperability	
Justifiable Parties	Consent	Legal and Regulatory Framework	Permissioned	Consent	Consent / Accountability
Minimal Disclosure for a Constrained Use	Minimalization	Mandates and Accountability	Private	Minimization	Minimization
Directed Identity	Protection	Unique, Secure, Accurate Identity	Secure [131]	Protection	Protection [132]

Source: -https://www.newamerica.org/future-land-housing/reports/nail-finds-hammer/the-principles-of-self-sovereign-identity/

1. **Privacy**
2. **User Focus**
3. **Security**
4. **Inclusion**
5. **Decentralization**

Privacy

Any digital ID solution should enable entities to control the privacy of their information, including minimal, selective, and progressive disclosure of attributes or other data. The sheer volume of data and value in aggregate makes centralized systems less resilient. Giving the user control enhances privacy, which becomes especially valuable in the healthcare and financial services

verticals. Where there is potential for value, there is potential for fraud or theft. In this sense, privacy is a civil right that needs to be established in the physical and digital realms.

Inclusion

Inclusion for all is the first step toward a brighter shared future. SSI technologies and principles align with the UN Sustainable Development Goals in their unique purpose to provide irrevocable agency to any human regardless of place of birth, bank account, or social status.

Security

Cybersecurity infrastructure is an absolute prerequisite for safe creation, issuance, storage, and transfer of all digital data for purposes of commerce or verification. Those credentials or claim sets relatable to an individual person typically carry value and are broadly disseminated and traded. Unfortunately, data breaches have become the norm, putting identity fraud and identity-related crimes at the forefront of international economic and social threat. The need for privacy-protecting infrastructure embedded in global data transfer networks grows each day.

Global Interoperability and Economic Efficiencies

An individual can move from one jurisdiction to another, and they should be able to carry their identifiers with them. Additionally, increasing globalization calls for frictionless trade of physical and economic resources, cross-border transactions, and valued data exchange. Sound digital identity infrastructure and governance aligns well, and should be integrated with, Web 3.0 architecture for this reason alone. The global pandemic highlights both the opportunity and importance of implementing interoperable verification protocols at the consumer level. Paper credentials and segregated data pools with centralized storage systems have prevented efficiencies in data exchange and created costly inefficiencies. Fragmentation of standards, technologies, jurisdictions, and redundant implementations have not allowed for the immediate solutions required to achieve convenient, privacy-enhanced public necessities such as a global interoperable vaccine credential in a secure, interoperable, and portable format.

As cited by the United Nations:[10]

> Globalization has impacted people and communities across the globe and has significantly influenced sustainable development. Fueled by fast-paced changes in technology and the increased mobility of goods, services, capital and labour,

globalization has greatly changed economies, societies and the natural environment and has made our world more interconnected than ever before.

These trends have presented a wealth of opportunities. Globalization and increased economic interdependence have accompanied — and facilitated — rapid economic growth in many countries and regions, helping world GDP grow from around 50 trillion USD in 2000 to 75 trillion USD in 2016. Yet, globalization has also presented significant challenges, including an uneven distribution of its benefits and costs.

“To ensure that globalization can be leveraged to support inclusive economic growth and sustainable development, it is essential to analyze the current system as well as emerging trends to devise policy solutions addressing them,” said Liu Zhenmin, UN DESA’s Under-Secretary-General, as he introduced the Secretary-General’s new report “Fulfilling the promise of globalization: advancing sustainable development in an interconnected world.”

Decentralization

Decentralization enables new economic models that incentivize “good” behavior and reduces or eliminates existing compromises between individual privacy and institutional transparency. DLT infrastructure allows for security, decentralized custody, peer-to-peer transactions, a programmable spectrum of privacy, and automation of modern financial and identity data transactions. Layers of technology, governance, economics, privacy management and moral guard rails are developing through co-opetition, member groups, and standards organizations. However, enabling technologies provide an increasingly clear path to harmonization and deployment of novel solutions viable for public entities, enterprises, and perhaps most interestingly, individuals.

User Focus

In a sense, anyone who uses the internet already has a digital identity. Email addresses, social logins, and national IDs all serve as public identifiers and gatekeepers related to personal Identity. An individual’s digital identity has basic principles and credentials, as well as derivatives from transactions and sharing of personal data. That personal data is currently monetized in commercial settings, as well as social media and advertising channels.

In many instances, third party attestation by a verifying party is necessary to have trust in credentials. For example, birth “credentials” are issued by a central authority or government body. In most cases, names are given by parents or guardians; individuals do not choose their place of birth, name, and other critical credentials. Thus, architecture with respect to attestations — how they are maintained, managed, and verified — requires careful consideration. Because of the ever-present tension between hacking and cybersecurity, individual ownership of identity in a decentralized framework may allow for the greatest security of personal data. Those preparing for Web 3.0 and decentralized technology should consider a transparent and viable governance framework capable of achieving the virtues invoked by Self-Sovereign Identity principles.

Standards and Interoperability

There are no **unified and overall standards to define precisely how digital ID mechanisms — from issuance to verification — would or should work**. Technology firms have their own way to implement standards specifications, which limit interoperability. The (limited) list of below standards, consortiums, and foundations are working on various technology stack layers used in a digital ID solution.

- *World Wide Web Consortium (W3C)* is an organization that has been working on building web standards since the early 2000s. They have primarily focused on the development of the browser and have been instrumental in making browser interoperability possible. They are specifically involved in a working group to specify architecture, data model and representation of DIDs that enable verifiable, decentralized digital identity.

- *JavaScript Object Notation (JSON)* is an open standard file format, and data interchange format, that uses human-readable text to store and transmit data objects. JSON is used for passenger QR code presentation. It is important to note that though JSON is a standard, the schemas required for interoperability have not been standardized.

- *Decentralized Identity Foundation (DIF)* is an engineering-driven organization acting as the center for development, discussion, and management of all activities required to create and maintain an interoperable & open ecosystem for the decentralized identity stack. DIF has the capability to set up intellectual property rights-protected working groups, deliver specs and standards, and offer infrastructure for the community.

- *Trust over IP Foundation* is an organization hosted at the Linux Foundation that is defining a complete architecture for Internet-scale digital trust that combines both cryptographic trust at the machine layer and human trust at the business, legal, and social layers.

- *Hyperledger Foundation* is an organization hosted at the Linux Foundation which promotes collaboration from a variety of industry stakeholders building implementations in open-source communities for a variety of use cases around decentralized ledgers and blockchains (Aries, Ursa, Indy).

- *The DID Communications Working Group (DIDComm)* was spun out of the Hyperledger Aries community and is now hosted at the Decentralized Identity Foundation (DIF). This group develops and contributes to the standards and technology for authentication protocols. It's working to enhance and standardize protocols over the next year, with an emphasis on interoperability

- *The Sovrin Foundation* is a 501(c)(4) non-profit entity that provides the business, legal, and technical support for the Sovrin Network, an open-source project. Using Decentralized Identifiers (DIDs) technology, the Sovrin Network allows for digital credentials to be privately issued, controlled, managed, and shared. The growth of the Sovrin Network partly depends on contributions from an active and supportive open-source development community.

- The Kantara Initiative - As one of the three brands comprising the global Kantara stable, the Kantara Initiative, Inc is an international, ethics-based, non-profit industry commons. Kantara's Mission is to grow and fulfill the market for trustworthy use of identity and personal data in pursuit of its vision to see equitable and transparent exchange of identity and personal data for mutual value.

Currently, numerous organizations — ranging from governments (national and sub-national), financial institutions, technology companies — are taking a "working code first" approach. Current stakeholders recognize that the standards are not ready for broad adoption and are thus building out ecosystems using code that meets their needs while they participate in shaping the standards and specifications that will be required for full interoperability. One key trend is the adoption of a consistent technology stack of Hyperledger Aries and Hyperledger

Indy and establishment of ecosystems around the globe (Canada, Finland, Germany, and more). These projects are driving several things forward:

- Interoperability Testing: The Hyperledger Aries Interoperability Test is being used to drive multiple areas of alignment, which is particularly crucial for governments. This approach is being used to drive other specifications such as the Wallet and Credential Interaction (WACI) effort hosted at DIF.

- Trust Over IP 4-Layer Model: The Aries and Indy codebases align well with the Trust Over IP 4-layer model. Aries operates at Layers 2 and 3, while Indy provides the Layer 1 utility. Each project that is operating provides the Layer 4 ecosystem.

- Machine Readable Governance (MRG): MRG is a way of orchestrating governance rules and the functions of a conventional trust registry in a semantically rich way at the agent software level. MRG was developed by Indicio.tech and SITA for the Cardea Project, a complete ecosystem based on Indy and Aries, designed for sharing digital health credentials and data in a privacy-preserving way. After a successful pilot with the Aruban government and health authorities, it was donated to Linux Foundation Public Health for use by public health agencies around the world. The key advantages of MRG are flexibility (everyone can publish their rules and these can be incorporated and updated according to hierarchy and need), speed (there is no transaction delay required by the need to contact a Trust Registry), and the ability to cache governance rules so that the system can work offline. MRG also obviates the challenges presented by commercial interests controlling both the flow and the participants in a trust registry-based system — along with the need for registries of registries to manage expanding global interoperability. Critically, Indicio and SITA found that MRG was the most effective way for the Aruban government to exercise its sovereignty over the process of COVID testing, meet its needs, and thereby feel confident in using the system.

Vertical Focus #1: Healthcare & Travel Applications

Current State of Practical DID Applications for Cross-Border Travel and Health Passes

- ***The Commons Project Foundation and the World Economic Forum*** have launched the **Common Trust Network** in collaboration with a broad voluntary network of public and private stakeholders. **CommonPass** is the traveler app which will store and display

COVID-19 test results and eventually vaccination records. **Five airlines** are part of this initiative as well as **Airport Council International**, representing 2000 airports.

- ***IATA Travel Pass*** is a mobile application (available in March 2021) allowing travelers to store and manage certifications for COVID-19 tests or vaccines. The information provided through the IATA Travel Pass can be used by governments requiring testing or vaccination proofs as a condition of international travel during and after the COVID-19 pandemic. **Emirates Airlines** is one of the first airlines to partner with IATA for the adoption of Travelpass

- ***World Health Organization (WHO):*** Initiated the development of a digitally enhanced **International Certificate of Vaccination**, a 'smart yellow card'. WHO also set out the **Smart Vaccination Certificate Consortium**. The consortium is intended to bring together experts to focus on defining specifications and standards for a digital vaccination certificate

- ***International Chamber of Commerce (ICC)*** has partnered with International SOS to launch the new ICC **AOKpass** mobile app, to provide trusted recognition of individuals' COVID-19 compliance status. Singapore Airlines has trialed the AOKpass service for inbound travelers from Malaysia and Indonesia.

- ***Vaccine Credential Initiative (VCI)*** is working to enable individuals vaccinated for COVID-19 to access their vaccination records in a secure, verifiable, and privacy-preserving way. The coalition (*CARIN Alliance, Cerner, Change Healthcare, The Commons Project Foundation, Epic, Evernorth, Mayo Clinic, Microsoft, MITRE, Oracle, Safe Health, and Salesforce*) is developing a standard model for organizations administering COVID-19 vaccines to make digital credentials available.

- ***Good Health Pass Collaborative*** - a cross-industry group was established in 2020, in response to COVID-19 shutting down international travel, to provide guidance on travel pass creation and use. The resulting Interoperability Blueprint makes recommendations for adoption that include the early standards and specifications from Trust Over IP, DIF, and W3C.

The adoption of Digital Health Credentials will take off if interoperability allows a traveler who received their COVID-19 test result credential from a health information exchange in one country to present that credential to immigration officials in another country. It is unlikely that there will be a single, shared ledger where credentials are anchored. Many ledgers will likely be involved in exchanging verifiable credentials, often referred to as a "network of networks." The governance and technical architecture of these networks must be carefully designed for interoperability and governed by principles that are consistent with privacy, security, and individual data ownership.

Vertical Focus #2: Government and International Interoperability

Various governments have started initiatives (some of them are listed below) in decentralized ID, with user privacy as a key focus. Importantly, trending privacy legislation in Europe, Canada, the U.S. and other global leaders focuses on data transparency in commercial settings and the right for individuals to have full control of their personal data and how it is used.

This is a current interactive map covering SSI projects around the world created by Northern Block.

- **Canada**
  - **Province of Ontario's Digital ID Plan**
  - **The Pan Canadian Trust Framework**
  - **Public Sector Profile of the Pan-Canadian Trust Framework**
  - **CIO Strategy Council** - an official standards development organization
- **Estonia**
  - **Estonia Global ID Solution**
- **EU**
  - **Video Highlights of the European Commission Proposal**
  - **Proposal for New EU ID**
  - **News on Proposal for EU Digital Identity**
- **Great Britain**

    - Framework Solution
- **India**
    - India's Digital Identity Program - Aadhar
    - Digital IDs to Land
    - Family Digital ID
- **Lack of government issued/sponsored credentials**
    - **Greatest Opportunity**
- **Adoption of VC standards and/or "progressive" or potentially Decentralized or Self-Sovereign Identity**
    - ISO/IEC 29794 Series
    - ISO/IEC 29109 Series
    - ISO/IEC 24745
    - ISO/IEC 24761
    - ISO/IEC 19784-1:2018
    - ISO/IEC 24709-1:2017
    - ISO/IEC TR 29194:2015
    - ISO/IEC TR 29196:2015
    - ISO/IEC TR 30125:2016
    - ISO 19792:2015
    - ISO 24714:2015
    - ISO/IEC 29100
    - Privacy ISO/IEC 27018
    - Privacy ISO/IEC 29190
    - Privacy ISO/ IEC 29184
    - Management ISO/IEC 24760 Series

Vertical Focus #3: Financial Services and Taxation

In addition to the rapidly growing decentralized finance (DeFi) space, which, at the time of writing (at the time of this paper's writing), holds over $250 billion USD in total value locked, issuance of retail CBDCs has begun in major economies. All DeFi platforms are built upon DLT infrastructure and many retail CBDC deployments are expected to leverage DLT. A universal, user-centric access point to global financial infrastructure would create efficiencies alongside the development of these transaction networks. The Institute of International Finance published a detailed framework in the Global Assured Identity Network White Paper which also details use cases. Additionally, the U.S. Financial Crimes Enforcement Network (FinCEN) is pursuing solutions via collaboration and innovation platforms to explore the efficacy of SSI implementations for financial services.[11]

Beyond creating an interoperable global financial network which allows rapid value exchange without an expensive intermediary, privacy engineering made possible by Decentralized Public Key Infrastructure (DPKI) would allow for efficient compliance tools to be developed; capital markets participants could protect the anonymity of holdings while still being properly identified. This transparency can root out bad actors by process of elimination and create further safeguards to prevent illicit activity.

The Travel Rule

Combating money laundering is a key focus of financial regulation around the globe. Know-Your-Customer (KYC) regulations in most jurisdictions require that regulated financial services companies collect and store identifying information on their customers, whether individuals or businesses. In June 2019, the Financial Action Task Force (FATF), a global financial regulatory standards body, recommended that the "travel rule" be applied to institutions that handle cryptocurrencies.[12]

The travel rule requires that regulated institutions include identifying information with a transfer of funds to another regulated institution. In doing so, institutions (and potentially regulators or law enforcement) can monitor for money laundering or terrorist financing. Numerous jurisdictions are experimenting with or deploying blockchain-based KYC systems, including the United Arab Emirates[13] and Sri Lanka.[14]

Taxation

Perhaps the most valuable application of decentralized ID in the long run will be the automation and standardization of tax laws. Currently, there is great political impetus to reduce tax avoidance and evasion, as shown by the new Global Minimum Tax proposal.[15] A more complete description of Taxation, standards, and applications can be found in the Global Tax section of the GSMI 2.0 Report.

Gaps and Challenges

As excerpted from Hindawi Survey on SSI:

The self-sovereign identity model is considered as the latest evolution of IAM models. It attempts to address a number of shortcomings found in the existing digital identity space. However, it also begets a unique set of challenges that warrant adequate research, exploration, and discussion. The following paragraphs discuss these challenges:

Standards for Data Management and Wallets. Standard protocols, practices, and policies around user experience, data management, and data exchange should be carefully defined and implemented. While SSI supports an open ecosystem, there is value in consistent yet flexible user interactions, data management policies, and data presentation standards.

Key Management. In traditional identity management models, the identity providers are primarily responsible for the management of identity data and secret keys and therefore must address the liabilities, risks, and technical requirements associated with that task. Conversely, in the SSI model, this responsibility and its associated risks are placed on the shoulders of the users. There have been numerous instances of users losing their cryptographic keys, resulting in the loss of valuable information and unrecoverable funds. Addressing the key management requirements in the SSI architecture is a fundamental step towards the mass adoption of SSI. Reliance on decentralized key custodians is one form of addressing the key management challenge.

Consent. As stated by Article 4 of General Data Protection Regulation (GDPR), the consent given by the user must be meaningful, well-formed, unambiguous, specific, and freely given, specifying clear decisions. This process is not easy to implement and hard to verify in the current identity models. Moreover, requesting users to provide consent to many privacy policies and data sharing practices has led to what is known as *consent fatigue*, where the user is

bombarded with privacy notifications. Ideas such as automated decision-making and response by digital wallets or agents representing the user, based on prior user decisions, should be entertained. Moreover, research around consent management, presentation, and enforcement is valuable.

Access. The backbone of many SSI systems is DLT. The concept of DLT and blockchain will be explained in the next sections. Certain DLT systems are public, allowing any entity to read or write to the ledger, while others are permissioned and allow only a selection of authorized entities to read or write new records into the ledger. If not carefully designed, the permissioned approach possesses the risk of forming centralized architecture similar to an oligopoly among the few authorized entities. On the other hand, the permissionless and public model may be vulnerable to attacks common in various open DLT architectures.

Accountability and Governance. It is important to articulate the policies and procedures around identifying and addressing malicious behavior and dishonest entities. It is also important to realize and articulate the correct degree of decentralization needed to support the vision and the requirements of SSI. Certain identity management operations such as identity claim issuance, identity lookup, and secure storage of data may rely on some degree of centralization and dependence on trusted intermediaries. Some implementations of SSI place significant power in the hands of a select few trusted entities that must comply with a common contractually binding trust framework, potentially making these entities the weakest point of the network. While other implementations of SSI aim for a more decentralized, programmable, and machine-readable governance framework. The latter form of governance too has shown to suffer from various flaws in the past. Therefore, efforts to determine the correct balance between centralization and decentralization is an important topic.

Trust in Data. While there may be trust in the underlying SSI network as a secure, robust, and decentralized platform, the methods to form trust among the entities, and the trust in data including the verifiable credentials exchanged must be carefully designed. The authentication and data validation may need to be done through a trusted authority and outside of the blockchain network.

New Technology Adoption. As a new identity model, SSI requires various modifications to the existing system architectures. An important step towards the success of SSI is the discussions around the suitable technology stacks, deployment practices, and operational procedures.

Particular attention must be given to the user experience, including the user interactions from the operator's perspective. Proper design steps must be taken to avoid the fate experienced by many other good innovations such as Pretty Good Privacy (PGP), which while is a useful technology it has not met the expected broad use.

Investment and Commercialization. As a relatively new venture with a growing ecosystem but with limited knowledge on the revenue model, unknown user acceptance, and utilization and unknown risks, any entity intending to adopt SSI must design a strategic plan that supports the investment and risk involved in the deployment and operation of such a system. The SSI economic model may lead to the chicken and egg problem where user adoption depends on the support of the service providers and vice versa.

Recommendations

1. Governments are gradually adopting some version of the SSI framework, and we expect this to be a trend rather than an anomaly. The first solutions will not be perfect, but experimentation will prove valuable. The beauty of Web 3.0 is the open-source nature of documentation, projects, pilots, and case studies made available to all who can contribute.

2. Open standards and technologies will pave the way for wider adoption of decentralized identity standards. Stakeholders should up to date with open-source community developments. The Hyperledger Foundation and other open-source consortiums frequently publish vast research repositories and case studies.

3. Basic identifiers like national IDs, passports, etc. will always be issued by the founding authority, but within an SSI framework, the user will control their sacred identifiers and give consent to share them. Most developed nations are providing a legislative template for the rest of the world to follow.

4. Interoperability and inclusion will be the crucial features in decentralized identity solutions going forward.

Conclusion

Leveraging decentralized public key infrastructure as the basis for SSI frameworks is a frontier development. Standards for DID methods, protocols, verifiable credential formats, and other technical ambiguities are being explored through trial and error. Although the end goal involves

direct interaction with the individual, enterprise and government adoption are critical for rapid iteration and proliferation. Institutions which adopt SSI frameworks will create economic efficiencies and rebuild eroding public trust. The open-source nature of early implementations will help create a robust and interoperable framework which laggards will benefit from; early adopters will pave the way. The more intangible benefits of SSI will be portrayed in human form. By providing agency, basic digital identification, the ability to prove ownership of digital property, and banking services, each human being will have greater potential to self-actualize.

Data exchange networks envisioned today will allow for the “self-sovereign individual” to monetize their own data with control, autonomy, and privacy without sacrificing convenience. Travel across borders will be seamless. Electronic healthcare records will be accessible by the user regardless of location or insurance provider. Financial services will be accessible to many more people simply because they can prove their identity with multiple sources of attestation without recurring registration or creation of another set of siloed credentials made liable to data breaches.

The combination of public communication networks and privacy-preserving identity management tools will allow frictionless flow of data and value with automated accounting trails and transactions. The economic efficiency of free-flowing resources in an increasingly connected world cannot be measured, but decentralized systems have already proven that the world agrees.

Digital ID Report Appendices

Appendix A: Companies and Projects in Commercial Action

Figure 1. Positive Blockchain Updated Catalogue of DLT Based Projects - Identity Related Projects In Action (https://www.g2.com/categories/decentralized-identity)

Appendix B: Digital Identity Lexicon/Glossary/Statistics

Sovrin V3 Glossary

W3C Terminology Index

Digital Trust Statistics

65% of people responded, in a survey recently administered by Accenture, that they would want control over their personal data.

Passwords

- As of 2020, phishing is by far the most common attack performed by cyber-criminals, with the U.S. FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime. (FBI Internet Crime Complaint Centre, 2021)
- Google has registered 2,145,013 phishing sites as of Jan 17, 2021. This is up from 1,690,000 on Jan 19, 2020 (up 27% over 12 months). (Tessian, 2021)
- Ransomware attacks have been experienced by 1 in 5 Americans. (Anomali and The Harris Poll, 2019)

Phishing

- As of 2020, phishing is by far the most common attack performed by cyber-criminals, with the U.S. FBI's Internet Crime Complaint Centre recording over twice as many incidents of phishing than any other type of computer crime. (FBI Internet Crime Complaint Centre, 2021)
- Google has registered 2,145,013 phishing sites as of Jan 17, 2021. This is up from 1,690,000 on Jan 19, 2020 (up 27% over 12 months). (Tessian, 2021)
- Ransomware attacks have been experienced by 1 in 5 Americans. (Anomali and The Harris Poll, 2019)

Data Breaches

- There were 1,767 publicly reported data breaches in the first six months of 2021, which exposed a total of 18.8 billion records. (Risk Based Security, 2021)
- Over 90% of all healthcare organizations reported at least one security breach in the last three years. 61% acknowledged they don't have effective mechanisms to maintain proper cybersecurity. (Frost Radar, 2020)
- In 2020 the average cost of a corporate data breach was $3.86 million. (Dice.com, 2020)

Privacy Erosion and Surveillance Capitalism

- 82% of web traffic contains Google third-party scripts and almost half of them are tracking users. (WhoTracks.Me, 2019)
- 74% of Internet users feel they have no control over the personal information collected on them. (Ponemon Institute, 2020)
- 72% of Americans report feeling that all, almost all, or most of what they do online or while using their cellphone is being tracked by advertisers, technology firms or other companies. (Pew Research Center, 2019)

Misinformation and Unverified Sources

- In 2020, only 29% of US adults said they mostly trust the news media. (Statista, 2020)
- In Q3 of 2020, there were 1.8 billion fake news engagements on Facebook. (German Marshall Fund, 2020)
- 56% of Facebook users can't recognize fake news when it aligns with their beliefs. (SSRN, 2018)

Artificial Intelligence (AI)

- 62% of the companies adopting AI are extremely concerned that it will increase their cybersecurity vulnerabilities; 57% are concerned about the consequences of their AI systems using personal data without consent. (Deloitte, State of AI in the Enterprise, 2020)
- 93% of automation technologists feel unprepared or only partially prepared to tackle the challenges associated with smart machine technologies. (Forrester, 2016)
- Only 36% of AI adopters are establishing policies or a board to guide AI ethics. (Harvard Kennedy School, 2019)

Cybersecurity

- 95% of cybersecurity breaches are caused by human error. (Cybint)
- The worldwide information security market is forecast to reach $170.4 billion in 2022. (Gartner)
- 88% of organizations worldwide experienced spear phishing attempts in 2019. (Proofpoint)
- 68% of business leaders feel their cybersecurity risks are increasing. (Accenture)
- On average, only 5% of companies' folders are properly protected. (Varonis)
- Data breaches exposed 36 billion records in the first half of 2020. (RiskBased)

- 86% of breaches were financially motivated and 10% were motivated by espionage. (Verizon)
- 45% of breaches featured hacking, 17% involved malware and 22% involved phishing. (Verizon)
- Between January 1, 2005, and May 31, 2020, there have been 11,762 recorded breaches. (ID Theft Resource Center)
- The top malicious email attachment types are .doc and .dot which make up 37%, the next highest is .exe at 19.5%. (Symantec)
- An estimated 300 billion passwords are used by humans and machines worldwide. (Cybersecurity Media)

Appendix C - Use Cases

Snowbridge

- Company Name – Snowbridge, Inc
    - Location: Taipei, Taiwan
    - Founder & CEO: Eric Chou
    - Web site: http://snowbridge.tw

Industry Vertical

- Real Estate
- Personal identity
- Healthcare
- Document Notary
- Blockchain is the technical basis for the above sectors.

After trading land or property, the new owners receive certificates of title on papers to prove their ownership. Every paper certificate is issued and stamped by one of the local branches of the Department of Lands Administration (DoLA), Taiwan. To a landowner, keeping historical paper certificates for decades is not easy; to the owner's counterpart, verifying the paper certificate is also difficult.

The solution adopts Hyperledger Indy as the core technology and issues the certificates of title in the form of a verifiable credential. The agency signs credentials and stores them in the holders' cloud wallets. The holder fetches a QR code representing a chosen credential in his

wallet from a service portal. On the other hand, the verifier scans the QR code to authenticate the credential. The service portal provides an option for the holder to decide whether to mask their private information.

A private blockchain network was established in this solution. In the pilot stage, the DoLA operates 4 nodes centrally. After the solution is in production, select local branches of DoLA would become the node operators and the network will become decentralized.

Stage

- Currently in-flight, commercial pilot in October 2021, real production in 2022

Benefits

The certificate of title is important to the landowner and all the counterparts during trading and mortgage processes. According to government statistics, 30% of the certificates would be lost. The landowner needs to apply for a reissue, which costs time and human effort. Moreover, the ways to authenticate a paper certificate mainly rely on the DoLA branch's stamp and watermarks on the paper. Modern forgery techniques can easily overcome those countermeasures. Fake paper certificates have been seen in many fraud cases, which leads to huge financial damage for real estate buyers, banks, and the government.

Digitalizing the certificate of title in the form of verifiable credential provides the trust within the ecosystem. It is secure and more efficient than using paper certificates. In particular, banks can approve mortgages at a faster speed, and the DoLA staff can waive some legal burden when processing the registration of lands and houses.

In some cases, the landowner may want to prove their ownership without giving out all the personal details. This solution enables the landowners to decide what data to be revealed. The SSI concept in this solution is beneficial to protect the landowner's privacy.

Uniqueness

Although using a mobile app may be more appealing, the solution uses a cloud wallet approach to avoid the "digital divide" among generations. Since the solution would be used by the elders, it must be easy to use with the minimal instruction. The holder's wallet is encrypted and stored in the cloud environment. The holder uses their Citizen Digital Certificate (issued by the government) to log in to the service portal and fetch a time-limited verification code. The verifier uses this code to retrieve the proof of credential.

The replacement cost of the current paper certificate system in a short period of time would be huge. The government wants to run both the traditional and digital solution in parallel for a period of time; the landowner will receive both the paper certificate and the digital credential at the same time. This solution stores the paper certificate file (PDF format) in a decentralized InterPlanetary File System (IPFS). The PDF file's CID (multihash) is inserted in the credential. In this way, the verifier gets not only the certificate data but can also retrieve the image of the paper certificate.

Snapper Future

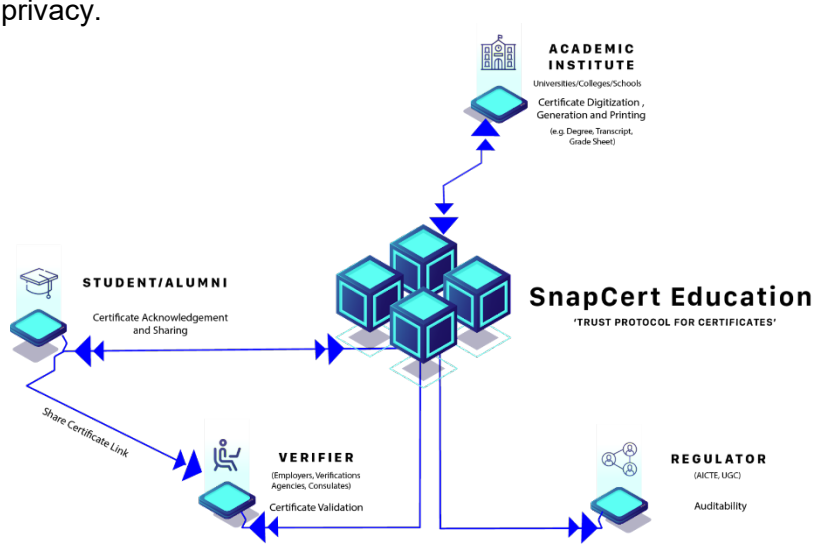
- Company Name – Snapper Future Tech Pvt Ltd
    - HQ Location – Pune, India
    - Founder & CEO name – CEO – Darshana Jain, Cofounders- Naresh Jain, Avnish Gupta, Prashant Surana
    - Website URL – www.snapperfuturetech.com

Industry Vertical

- Education/E-governance

SnapCert is a 'Blockchain Based Credential Issuance and Verification platform where we can digitize, generate, print, distribute, share and verify all kind of academic certificates like degrees, marksheets, transcripts, school leaving certificates or other credentials like employment letters, birth certificates, marriage certificates.

Snapcert is a trusted bridge between Credential Issuers, Record Holders and Verifiers, and creates a connected ecosystem between all stakeholders, where verification can be done within seconds from the primary source without involvement of any personnel while maintaining data protection and privacy.



Stage

- Commercial

Economic Savings/ Benefits

- SnapCert enables Real Time, Primary Source Verification
- Verifier
  - Real Time Certificate Verification
  - Reliability and Trusted
  - Savings in Operational Cost
  - Auditability of Data

Academic Institution

- Efficient Certificate Generation
- Savings in Operational Costs
- Permanent & Secured Data
- Deterrence to fake certificates

Learner

- Online and permanent records
- No risk of losing records
- Easy sharing
- Single account for all records

Uniqueness

SnapCert has a strong architecture and metamodel design to scale up horizontally and vertically to onboard multiple stakeholders and cater multiple industries without changes in the application.

SnapCert gives the flexibility to the users to define their own institution structure like departments, certificate type, programs, batches, etc. They help in the digitization of existing physical records using specialized industrial printers and extracting data to blockchain through DMS.

Indicio for Government

- Company Name
    - Indicio
    - Seattle, Wa
- Founder & CEO name
    - Heather Dahl, CEO
    - Ken Ebert, CTO
- Website URL
    - Indicio.tech

Industry Vertical

- Government Services

Indicio for Government is a complete set of technology for a government of any size to integrate Verifiable Credentials and Digital Wallets into their economies with all the technical and business support they may need. Using Indicio for Government, citizens can easily and securely share their data using mobile devices with the agencies and services they require. Governments can reduce errors and fraud, admit visitors, and bring economies back to life. Providing privacy and control for people is the key to establishing public confidence in a system for controlling one's personal data. Indicio for Government makes it possible for a person to present a digital proof of a COVID negative test or vaccination, designed to protect individual privacy. This system enables a government agency to provide digital proof of information to an individual — and involves no one else storing or managing their data. This credential is tamper proof and incapable of being faked. It is easy to download and quick to use at any other agency or participating business. Indicio for Government is based on open source, interoperable technology that allows all agencies and elements of a government to use verifiable digital credentials to safely and securely return to life.

Stage

- Commercial

Economic Savings/ Benefits

Indicio for government is an innovative approach to secure data that makes personal information verification more convenient, secure, and helps eradicate fraud in government

services. Ease of use and interoperability are at the top of the list of benefits for systems that adopt Indicio for Government. Indicio's approach makes it possible for agencies of all types to issue or verify verifiable credentials. This lowers friction for citizens, businesses, and government agencies to safely provide fraud-free services and reduce administrative burden of duplicating data and friction of transferring data between agencies and jurisdictions.

Uniqueness

The COVID-19 pandemic resulted in a massive increase in the number of online citizen identities, credentials and access points. As the pandemic continues, the immense need for digital identity and secure citizens' identities shows no signs of subsiding. According to Gartner, more than 60% of governments will have tripled digital services by 2023, but fewer than 25% will be integrated across organizational silos. This separated approach to citizen identity will lead to major security gaps and a frustrating user experience. Indicio for Government presents the most flexible, interoperable, and secure way for people to access government services and keep their identities safe.

Indicio for Health

Industry Vertical

- Health Care

Public health authorities, governments, organizations, and industries need a way to enable people to maintain their privacy while holding and using an easily verifiable, trustworthy, unalterable proof of a health test or vaccination. Indicio for Healthcare is a complete ecosystem for the exchange of privacy-preserving digital credentials, that provides the necessary technology components, blockchain network, and expert support of highly trained technical and business staff to get up and running quickly. With our complete suite of products and services, including hosting and customization, verifiable health credentials can be easy to use and secure.

Stage

- Commercial

Economic Savings/ Benefits

Indicio for health is an innovative approach to personal health data that makes vaccine verification more convenient and secure. Ease of use and interoperability are at the top of the

list of benefits for systems that adopt Indicio for Health. Indicio's approach makes it possible for all types of organizations to support digital wallets and verify verifiable credentials. This lowers friction for healthcare facilities, testing labs, government agencies, schools, sports arenas, transportation, trade shows, and workplaces to confirm health status and assist efforts to reduce new outbreaks.

Uniqueness

Vaccination rates are on the rise and several countries, including the United States, are relaxing public health restrictions as they steer toward a full reopening. Digital health credentials from Indicio present the most flexible, interoperable, and secure way for people to share private health data to organizations that may require proof of vaccination, including commercial airlines, employers, colleges and universities, and retail establishments. By enabling organizations across all sectors to verify health data, Indicio is offering a solution to help not only reopen a single industry vertical, but reopen the world.

Anonyome Labs

- Company Name - Anonyome Labs Inc.
    - HQ Location
        - Woodside, Californio
    - Founder & CEO name
        - Co-CEOs: JD Mumford and Dr Paul Ashley
    - Website URL
        - https://anonyome.com/

Industry Vertical

- Software: API vendor (Identity, Privacy and Cyber Safety)

Anonyome Labs created the Sudo Platform to provide enterprise software developers with capabilities to add persona (Sudo) based identity, privacy and cyber safety features to their applications. The Sudo Platform provides to these enterprise software developers mobile and web SDKs, sample apps, documentation, and UI Kits to accelerate their application development. A key offering of the Sudo Platform is Decentralized Identity based services. This includes both client (Edge Agent) and server (Cloud Agent) offerings. This allows the enterprise to become a Decentralized Identity Verifiable Credential Issuer and/or Validator. And it allows the enterprise's users to take part in a decentralized identity ecosystem - by giving

them a mobile wallet/agent to manage decentralized identities, connections and verifiable credentials.

Stage (Commercial, Pilot, POC)
Commercial/Pilot: Enterprises have applications in production that leverage the Sudo Platform offerings. The Decentralized Identity offering is at the Pilot stage.

Economic Savings/ Benefits
Enterprise software developers can leverage the Sudo Platform's offerings for decentralized identity allowing them to easily bring these capabilities to market. The Anonyome Labs team has a deep history of working within the decentralized identity standards groups and contributing to decentralized identity open-source software, and enterprises can utilize this expertise in bringing their own decentralized identity offerings to market.

Uniqueness
The Sudo Platform allows enterprise software developers to create decentralized identity applications that support the concept of multiple personas (Sudos). Each of the user's personas have compartmentalized decentralized identities, connections and verifiable credentials making management much simpler for the user.

ID Ramp

- Company Name - ID Ramp
    - HQ Location - Iowa, USA
    - Founder & CEO name - Mike Vesey
    - Website URL - Idramp.com
- Industry Vertical
    - Cross industry enterprise and public sector identity services

<u>Use Case 1</u>

American Electric Power - Developed a Zero Trust third party vendor ecosystem to protect consumers from fraudulent vendors, reduce AEP data liability, and increase consumer confidence by putting customers in control of data request verification. Verifiable credentials and proofs were issued to trusted vendors for real time verification by consumers at point of sale. The solution includes a data verification request process that allows customers to securely audit

and then provision power usage data to only trusted vendors. This process reduces AEP data liability when releasing customer data to third parties. AEP customers are issued a verifiable credential to eliminate passwords and participate in the vendor verification process.

Stage

- Pilot

Economic Savings/ Benefits

- Reduces third party fraud and data liability. Increased customer privacy protection and brand trust.

Uniqueness of the use case

This application combines Oracle blockchain for auditability, with Oracle cloud infrastructure and identity services with a Hyperledger Indy ID network hosted in the Oracle cloud.

Use Case 2

Qiqochat - Empowered Qiqochat customers with password-free privacy-protecting login with verifiable credentials. Deployed API free integration for event ticket credential issuance and verification with Eventbrite, Zapier, and Qiqochat. Verifiable credentials are automatically added to the event registration ticketing and access process. This solution increases security, reduces administration complexity, and simplifies the event participant experience. The solution was first developed for the IIW conferences and is designed to support all future events as a standardized business process.

Stage

- In Production

Economic Savings/ Benefits

- Increased customer privacy protection and brand trust. Reduced integration complexity and user experience for event ticketing and attendance.

Uniqueness

- One of the world's first production deployments for consumer collaboration platform.

Use Case 3

IdRamp enabled North Dakota Department of Education systems to consume student credentials issued by the RANDA Open Credential Publisher system. Students and staff were able to login to North Dakota Department of Education systems without a password by presenting this credential. They assisted RANDA in moving the consumption of these credentials further to the edge, allowing others (like higher education institutions or employers) a simple code-free way of consuming the credentials created as part of the North Dakota project. IdRamp provides code free connections to applications and services, allowing them to consume open standard credentials supporting rapid growth and adoption of student-controlled credential wallet technology.

Stage

- In Production

Economic Savings/ Benefits

- Improved portability of student credentials. Improved security and password elimination.

Uniqueness

- One of the world's first production deployments for portable student credentials.

Dhiway

- Company Name: Dhiway Networks
    - HQ Location: Bengaluru, India
    - Founder & CEO names: Pradeep KP (Co-Founder, CEO); Satish Mohan (Co-Founder, CTO); Sreevidya Satish (Co-Founder); Amar Tumballi (Co-Founder)
    - Website URL: www.dhiway.com

Industry Vertical

- Data governance and data supply chain.

- Use Case Description

Authentic data inputs and immutable data capture are among the key risks being faced across industries. Erroneous data results in compromising audit activities, increasing business risk as well as providing an unsound foundation for business strategies. Compromised data streams have resulted in lowering the confidence in data pipelines and growing mistrust both inside

businesses and within their ecosystems. Provided assurances around trustworthiness of data is the catalyst to a thriving dynamic digital economy and a robust digital trust ecosystem.

Stage

- Commercial Pilot - the Data Fabric utility is available to a curated set of customers in a private ecosystem. Near term plans include enabling a public, permissioned data centric utility network (blockchain) to be generally available.

Economic Savings/ Benefits

- Lower transaction costs compared to alternatives
- Variable transaction costs linked to resource usage (data size)
- Low energy consumption (no mining)
- Public permissioned chain will be governed by a council, which will approve the following to start with
  - Transaction pricing
  - Validators
  - Network expansion
- Lower transaction fee and resilient network will enable:
  - Improved customer experience
  - Lower cost of overall transaction
  - Reduce friction
  - Improve ease of doing business

Uniqueness

Dhiway Data Fabric provides organizations with a way to have authenticated data input sources along with immutable data capture methods. Data Fabric as a Service (DFaaS) is a technology infrastructure built around a set of open standards-based components, immutable storage, distributed ledger. The integrated technology framework enables the creation of immutable, tamper-resistant data structures on a permissioned network.

#MARK, Data Fabric's protocol uses a combination of append-only logs, cryptographic markers, stream update rules, and distributed ledger anchoring to make the programmable data structures (streams) tamper-proof, secure, and verifiable. A stream can be used to build up flexible data structures that can, in turn, be used to represent a wide variety of things such as

identities, specific pieces of data or content, media files, schemas, policies for data access control, verifiable credentials, agreements between multiple parties, etc.

Data Fabric enables information to be composed into higher-order data structures, programmed to behave in any desired manner, and whose resulting state is stored and replicated across the network. The benefit of Data Fabric's permissioned design and unified state layer is that any permissioned application/user can create, discover, query, and build upon verifiable information.

FinClusive

- Company Name: FinClusive
    - HQ Location: Virtual Company (global); HQ address: Guilford, Vt
    - Founder & CEO name: Amit Sharma
    - Website URL: www.finclusive.com

Industry Vertical

- Financial services, payments, financial crimes compliance (FCC); regtech with digital identity compliance credentials

FinClusive provides companies — including fintech companies, virtual asset service providers and other non-bank and decentralized financial services — digital access to accounts and payments (A&P) with an embedded full-stack global-standard based compliance as a service (CaaS) in one integrated platform. CaaS ensures these companies can conduct the full range of anti-money laundering (AML), know your customer/business (KYC/KYB), due diligence, screening, monitoring, and reporting required by regulators. Further, CaaS provides digital identity compliance credentials (FinCIDs) through CDD Check Connect for individuals and entities, ensuring legitimacy of them to financial service providers and enabling a seamless KYC/KYB utility that maintains the protection of underlying personal and entity identifying information (PII/EII). The issuance of unique, compliance-backed digital identity credentials enables seamless onboarding, monitoring and validation of financial service customers across the globe. FinClusive goes further, as a certified issuer/validator of global legal entity identifiers (LEIs) with the Global Legal Entity Identifier Foundation.

Stage

- Commercial with multiple pilots

Uniqueness

This use case enables partners, customers and other node operators to comply with essential KYC/KYB and CDD requirements with the issuance of FinCIDs and LEIs (fully backed by essential compliance checks) that will serve to verify and validate customer/client information with appropriate privacy protocols and access controls. Partners can leverage this CDD Check Connect to obtain comprehensive client due diligence and screening results real-time as a shared utility while enabling clients with a unique compliance credential that can be leveraged by other financial services they seek to access.

Appendix D: Educational Resources and Articles

GBBC DID WG Living Education Resource Repository

Standards for a Trusted Potential Framework as Proposed by ToIP, leading membership consortia group establishing interoperability standards for enterprise and governments alike: https://docs.google.com/document/d/15B3kzBECkasyDZ8CByyGInqVL3gdokPYSRU7KSUP-VQ/edit#heading=h.vns9nhhunwt

Outstanding Paper on Use Cases and Commercial Applications by Affinidi: https://drive.google.com/file/d/1PpVWRCCcBTA7TenkZrBC7eJ4PHcYA5D7/view?usp=sharing

DID and SSI Tenets: For a comprehensive primer on SSI ecosystem, this may serve as a great resource.

Coin center is an example of a research organization contributing educational material and happened to highlight the concerns of this report: https://www.coincenter.org/open-blockchains-and-decentralized-identity-standards/

For further reading:

https://www.edx.org/course/identity-in-hyperledger-aries-indy-and-ursa

https://trustoverip.org/wp-content/uploads/2020/05/toip_introduction_050520.pdf

Example of open-source frameworks and layers of the popular Sovrin "Trust Over IP" stack: https://wiki.hyperledger.org/display/indy

Endnotes

[1] https://www.dgen.org/blockchain-sdgs
[2] https://datacatalog.worldbank.org/search/dataset/0040787
[3] https://www.r3.com/blog/the-evolution-of-digital-identity/
4 https://en.wikipedia.org/wiki/Federated_identity
[5] https://www.w3.org/TR/did-core/#:~:text=Abstract,the%20controller%20of%20the%20DID.
[6] https://www.gsma.com/identity/decentralised-identity
[7] https://sovrin.org/wp-content/uploads/Sovrin-Glossary-V3.pdf
[8] https://www.w3.org/TR/vc-data-model/
[9] https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS173x+1T2020/65cfba99617340f39051f7c6f839bf85/
[10]https://www.un.org/development/desa/en/news/intergovernmental-coordination/new-globalization-report.html
[11] https://www.fincen.gov/news/news-releases/fincen-host-innovation-hours-program-workshop-digital-identity-services-and
[12] https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf
[13] https://gulfnews.com/business/banking/hsbc-joins-dubai-economys-uae-kyc-blockchain-platform-1.1624784197141
[14] https://www.cbsl.gov.lk/en/news/cbsl-successfully-completes-the-process-of-developing-and-testing-a-blockchain-technology-based-shared-kyc-poc
[15] https://www.politico.com/news/2021/11/10/136-countries-agreed-to-a-global-minimum-corporate-tax-rate-what-now-520418