The technology category now widely known as “decentralized identity” and more narrowly as “self-sovereign identity” didn’t even exist four years ago. At that time, the cutting edge of digital identity technology consisted of Internet-scale federated identity protocols such as OpenID Connect and user-centric data sharing protocols such as User-Managed Access (UMA) [1].

Then along came Bitcoin and a surge of interest in blockchain and distributed ledger technology (DLT) [2]. Although the initial uses of this technology focused primarily on cryptocurrency, it didn’t take long for the digital identity community to begin applying it to digital identity scenarios. In October 2016, several sessions on “blockchain identity” were held at the 23rd Internet Identity Workshop in Mountain View, California [3]. Soon afterward, the U.S. Department of Homeland Security Science & Technology division (DHS) published a Small Business Innovation Research (SBIR) grant topic, “The Applicability of Blockchain Technology to Privacy Respecting Identity Management” [4].

DHS awarded four research grants on this topic; one of them produced the first draft of the Decentralized Identifier (DID) specification [5]. Within a year, this specification was contributed to the World Wide Web Consortium (W3C) Credentials Community Group [6] for further development. At the same time, W3C approved its first working group on another foundational component of decentralized identity: the Verifiable Credentials Data Model 1.0 specification (which became a full W3C Recommendation in November 2019 [7]).

Why has interest in decentralized identity grown so quickly? Why has it become a topic track at almost every major digital identity conference? Christopher Allen provided an evolutionary perspective on this question in his April 2016 article, “The Path to Self-Sovereign Identity” [8].

The models for online identity have advanced through four broad stages since the advent of the Internet: centralized identity, federated identity, user-centric identity, and self-sovereign identity.

Centralized identity is the easiest identity model to understand: a centralized authority (government, corporation, university, service provider) that provisions and administers identity accounts (“logins”) for all the users of its systems. This works fine as long as users only need to deal with a small number of centralized systems. But once the Internet took off, users were faced with dozens, then hundreds of accounts, all demanding their own usernames, passwords, security and privacy policies, and account maintenance.

Industry responded with a solution: let users reuse an identity account they established with one provider with other sites and services. Thus was born the new model of federated identity and the new role of identity provider. Several generations of federated identity protocol standards followed: the Security Assertion Markup Language (SAML) [1], OpenID and OpenID 2.0 (URL-based identity) [1], and OpenID Connect (based on the OAuth authorization framework) [1].

The initial development of OpenID more than a decade ago was part of a movement toward user-centric identity — seeking to give end users greater control over the sharing of their identity data, particularly in social networking and social media contexts during the rise of Facebook, Google, Twitter, and LinkedIn. Another major new thrust in user-centric digital identity during that same era was moving from physical credentials in physical wallets to digital credentials in digital wallets. Called Information Cards, it was led by Kim Cameron [9] and the identity team at Microsoft. They helped establish the vendor-neutral Information Card Foundation and provided a set of open standards for digital credential generation, exchange, and verification at OASIS [9].
While OpenID still lives on in some fashion in the social sign-in deployments built on OpenID Connect, the overall Information Card model did not succeed in the marketplace. A likely key factor is that verification of this new form of digital credential required cryptographic libraries and cryptographic engineering skills that were neither familiar nor easy to master for the majority of developers.

User-centric identity was a distinct improvement, but the fundamental limitation of all federated identity solutions is that the identity provider(s) is at the center. There is no federation that can serve everyone everywhere, and every federation is constrained by the security and privacy policies its identity provider(s) can support. For example, Facebook identity users cannot use their credentials to log into their bank account. Furthermore, identities are not portable outside of the federation, so there is a degree of user lock-in to a federation that stands in stark contrast to the natural portability of the identity credentials we carry in our wallets to prove our identity every day in the real world.

Fast forward 10 years. Blockchain and distributed ledger technology (DLT) exploded on the scene, powered entirely by cryptographic algorithms and distributed computing. Quickly it became clear that ordinary developers and applications could take advantage of the same cryptographic libraries needed for blockchain transactions to issue and verify digital credentials. More importantly, since every transaction on a blockchain was digitally signed and verified by the blockchain itself, it also became clear that distributed ledgers could be used as a highly decentralized but potentially very secure mechanism for publishing and verifying the public keys needed to secure transactions off-chain.

This approach could not only solve the problem of how to decentralize conventional public key infrastructure (PKI), but how to keep the issuance and verification of verifiable digital credentials private by exchanging them entirely off-chain, and only using public blockchains for discovery and public key verification.

Recently, a new identity model known as decentralized identity — popularly called “self-sovereign identity” (SSI) — has emerged. It is important to note that the definition of self-sovereign identity (SSI) is still a work in progress in the industry. In principle, SSI enables individuals to “control” their identities (note that the topic of “data ownership” is still highly contentious). SSI provides the means for users to control personal information flow during digital interactions. In effect, SSI adds security controls to enable entities to agree on the nature and context of shared information for an online interaction. In this regard, SSI strives toward enabling user control over their identities and related information.

This objective is best achieved through the use of decentralized identity infrastructure such as DLT. In this model, individuals (or other entities including organizations and things) can utilize DLT-based identifiers to present claims relating to those identifiers without the need for a centralized identity provider. The SSI model enables the identity holder to be “sovereign” over their own digital wallet and digital credentials even though the identity holder is still required to obtain any except “self-issued” credentials from third-party issuers who have the trust of relying parties.

**Examples of Early POCs/Pilots**

Decentralized identity efforts have matured beyond architectures and early standards — we are now seeing advanced proof of concept projects spanning many public agencies and private industries. As one might expect, these are appearing in areas where centralized and federated identity approaches are not meeting the needs of the participants, particularly in use cases requiring improved agency and greater mobility of individuals, more efficient and secure onboarding (KYC) of under-served populations, and business process automation challenges in the reach of conventional federations.

In this section we provide a small sample of SSI-based projects in the marketplace. It is not intended to be comprehensive or complete, merely exemplary of the market activity that is developing.

**ID2020**

This initiative was formed in 2017 to address the digital identity needs of the 1.1 billion people in the world without legally recognized identities. It has received a grant fund, advisory services, and certification programs for ethical approaches to digital identity. One of its first efforts, undertaken in partnership with iRespond and the International Rescue Committee, is offering a decentralized identity platform to the approximately 35,000 externally displaced residents of the Mae La Camp in Thailand. Through their digital identities, participants will be able to not only access improved healthcare services but also securely store educational and professional credentials.

**uPort**

uPort [11] is a self-sovereign identity solution that is built on top of the Ethereum blockchain. The uPort solution is composed of the following components: a) smart contracts, b) developer libraries, and c) a mobile application. In this solution, users’ private keys are held in the mobile application. Smart contracts are used to support core identity services including cryptographic key and credential recovery in the event the user wallet is lost. Third-party developers use uPort libraries to integrate with the system. Several relying parties including the city of Zug in Switzerland accept uPort identity services to digitally sign and verify the authenticity of a claim.

**Sovrin Foundation**

Founded in September 2016, the Sovrin Foundation is a non-profit governance authority for a global public ledger for SSI based on open standards and open-source technology. The code for the Sovrin ledger is available through the Hyperledger Indy Project [12] and licensed under Apache 2.0. As a public
permissioned ledger, the Sovrin Network is operated by over 70 steward organizations around the world and governed by a community-developed governance framework. [13]

CULedger

CULedger is a global consortium created by the credit union industry to harness blockchain technology for the benefit of credit union members worldwide. [4] Its initial focus is the development of a verifiable credential that can be issued by any credit union or financial cooperative worldwide to any member who qualifies for credit union membership by fulfilling the necessary KYC requirements. This credential is currently in early production by several credit unions in the United States, and distribution is expected to scale steadily throughout the next several years.

Decentralized Identity Challenges

While interest in decentralized identity has exploded over the last few years, the path it needs to trod has been shaped by decades of lessons learned. Significant work lies ahead to make decentralized identity a reality.

The first and most obvious focus area is standards. The fundamental elements of this emerging technology stack are already coming into place: The Verifiable Credentials Data Model 1.0 specification [7] was released as a W3C Recommendation in November 2019, while the Decentralized Identifier Data Model [5] is in draft phase. Additional standards and protocols to ensure interoperability and portability throughout the stack are being incubated in the W3C Credentials Community Group, the Decentralized Identity Foundation, the Hyperledger project, the Rebooting the Web of Trust conference [15], and other communities.

There are also other important artifacts to be built as prototype implementations emerge, such as guidance and tools for addressing security and privacy concerns in different deployment types. Another concern is stronger recommendations and best practices to address the full user life cycle, including loss of control over identifiers, keys, or digital wallets. Finally, the use of blockchains in identity solutions introduce the concern of permanence of the data, which could theoretically run afool of privacy requirements such as GDPR’s “the right to be forgotten.” The solutions needed here are not just technical — such as not storing personally identifiable information on-chain — but also legal and regulatory.

Legacy identity architectures have enabled a steady pace of data breaches and corresponding asymmetry of control. The emerging standards and architectures described in this Special Issue propose to shift this balance by placing the user in control of their data. As the authors assert in “Improved Identity Management with Verifiable Credentials and FIDO,” decentralized identity architectures built around verifiable credentials promise to ensure the user is central to exchange of identity data.

Many decentralized identity architectures discussed in this issue rely on blockchains for their decentralized, tamper-evident, “trustless” properties. “Blockchain Research beyond Cryptocurrencies” and “The Trust over IP Stack” demonstrate the role blockchains can play in enabling global, scalable, decentralized identity management schemes. The article “Zero-Knowledge Proofs Do Not Solve the Privacy-Trust Problem of Attribute-Based Credentials: What if Alice Is Evil?” considers the use of zero-knowledge proofs for enhancing security and privacy.

The success of these new architectures requires usable privacy controls. The concern of shifting the burden to users is that it could exacerbate privacy problems or result in unusable systems. Further, the question of “who can I trust?” can become more complicated with decentralized architectures.”

Data Cooperatives: Toward a Foundation for Decentralized Personal Data Management” proposes organizational structures to address some of these concerns, while “Federated Authorization over Access to Personal Data for Decentralized Identity Management” describes how user managed access architecture and protocols can be used to enable scalable and usable access authorization. In addition, the article “Using Biometrics to Fight Credential Fraud” considers methods for increasing trust in used credentials. Lastly, “The Trust over IP Stack” proposes ways to bootstrap existing and new trust frameworks to enable even more secure and broad-reaching trust networks.

Another important theme in this article is that technology alone is not sufficient. The article “Beyond Consent: A Right-to-Use Licensing Agreement for Mutual Agency” takes on the limitations of our current notion of user consent, and proposes a taxonomy that is both more usable and adaptable to legal constructs.

An implicit theme of all the articles is the importance of standards and interoperability. Accordingly, many techniques/solutions described in this issue are complementary elements of improved identity management systems. For example, complete solution could employ FIDO standards for secure, usable authentication along with verifiable credentials and decentralized identifiers for enabling less privilege authorization schemes.

Conclusions

The purpose of this Special Issue has been to engage and explore with the identity community to understand the status, acceptability, and adoption of decentralized identity as it emerges in the marketplace. The community responded; there was a great deal of interest in contributing to our shared understanding of this promising technology. Compounding this interest are the growing requirements of new regulations regarding privacy, data security and data portability — areas where decentralized identity models may have particular advantages. The challenge now is to find appropriate business and integration models for combining this new approach to digital identity with the large installed base of traditional centralized and federated identity systems.

References

Biographies

Oscar Avellaneda is manager of Engineering Planning and Standards in the Canadian Department of Innovation, Science and Economic Development (ISED). His responsibilities with ISED include coordination of standards strategy and policy for Canada’s involvement in ITU-T. He also represents Canada at the Permanent Consultative Committee I (PCCI) of the Inter-American Telecommunication Commission (CITEL) where he chairs the Working Group on Deployment of Technologies and Services. He has also served as head of delegation and principal spokesperson to several ITU international conferences and meetings, such as WTSA, WCIT, PP, and ITU-T Study Group and CITEL meetings. Prior to joining ISED, he held various positions in product development, system engineering, and standards in the ICT industry. He received his M Eng. degree from McGill University, Canada.

Alan Bachmann works for CVS Health in their Office of the CTO department. He specializes in researching and developing impactful innovations for emerging technologies, namely IoT and blockchain (enterprise uses) systems. These technologies bring great possibilities to not only help our company but also our communities.

Abbie BarBir serves as a senior security advisor in the areas of identity management, mobile devices, and authentication at CVS Health Global Information Security. He has extensive experience in identity and access management. He has worked with many standards organizations on developing next generation authentication technologies. Currently he represents CVS Health on the FIDO Board of Directors. He holds a Ph.D. in computer engineering from Louisiana State University. In his more than 25 years in the software and security industry, he has been a professor of computer science, an application developer, a data compression and encryption inventor, systems architect, security architect, engineering manager, consultant, author, and inventor of numerous security algorithms and articles.

Joni Brennan is president of the Digital ID & Authentication Council of Canada (DIACC). Building on 15+ years of experience in identity access management innovation, adoption, and industry standards development, she helps the DIACC to fulfill its vision delivering the resources needed to establish a digital identity ecosystem that accelerates the digital economy, grows Canada’s GDP, and benefits all Canadians. She builds diplomatic and impactful relationships and formalizes strategic partnerships. She has participated in influential committees from organizations including: SCC Data Governance Initiative, OECD ITAC, ISOC, IEEE, OASIS, ISO, and ITU-T. Before joining DIACC, she was Kantara Initiative’s Executive Director driving programs for business, legal, and technology interoperability to connect entities and individuals in a more trustworthy environment. She led Kantara Initiative as the U.S. premier trust framework provider delivering value to multiple industry sectors. She helped to ensure that the Kantara Initiative program is aligned with multiple eGovernment strategies from economic regions including Canada, New Zealand, Sweden, and the United Kingdom.

Pamela Dingle has 15 years of experience in implementation and architecture of identity standards for web access management, provisioning, and federation. As director of Identity Standards at Microsoft, she leads a team of experts dedicated to collaboration within the industry to imagine, author, and drive adoption of identity standards including single sign-on, API security, next generation credentials, authentication, and blockchain.

Kim Hamilton Duffy is architect of the Digital Credentials Consortium — a multi-university effort designing the future of academic credentials — in her role at MIT Open Learning. Her expertise is decentralized educational credentials and infrastructure. Previously, she co-created the successful open-source, open-standard Blockcerts project with the MIT Media Lab. She is a Chair of the W3C Credentials Community Group, where she drives decentralized identity standards and prototype development. She led development of the first open source DID (Decentralized Identifier) method BTCR (Bitcoin Reference), based on the Bitcoin blockchain. Her mission is to expand opportunities to individuals through recognition of learning and skills gained beyond the traditional classroom; and her focus is building the interoperable, privacy-enabling open standards to accomplish this.

Eye Maler is ForgeRock’s Interim CTO. She is a globally recognized strategist, innovator, and communicator on digital identity, security, privacy, and consent, with a focus on fostering successful ecosystems and individual empowerment. She founded and leads the User-Managed Access standards effort and provides expert advice to forums such as Open Banking. Previously, she co-invented the SAML and XML standards. She contributes to the rock ‘n’ roll outfit ZZ Auth and the Love Tokens.

Drummond Reed has spent two decades in Internet identity, security, privacy, and trust frameworks. He joined Evernym as chief trust officer after Evernym acquired his startup, Respect Network. At the Sovrin Foundation he is a Trustee and Co-Chair of the Governance Framework Working Group. He is co-editor of the Decentralized Identifier specification at the W3C and a contributor to the Hyperledger Indy and Hyperledger Aries projects.

Manu Sporny is a serial entrepreneur, social systems hacker, and computer scientist. He has been on the founding team of five startups, two non-profits, and five global standards initiatives related to payments, identity, and blockchain. He spends most of his time driving the creation of open standards and open technology that will integrate privacy-aware identity, payments, and blockchain technologies into the core architecture of the Web. A champion for science and the arts, his life’s work is focused on empowering people to enact global change through the web. He is currently focused on expanding the core infrastructure of the web to include self-sovereign identity, payments for the unbanked and underbanked, and transparent governance systems utilizing blockchain technologies.