# MECHANISMS FOR DIGITAL TRANSFORMATION IN THE EDUCATION AND HEALTHCARE SECTORS UTILIZING DECENTRALIZED SELF-SOVEREIGN IDENTITY

Gregory H. Jackson[1] and Karaitiana Taiuru[2]

[1]The University of Buckingham, U.K. and Adayge Inc., Utah, U.S.A
[2]University of Auckland, Faculty of Engineering, Department of Electrical, Computer and Software Engineering, Auckland New Zealand and Taiuru & Associates Limited, Christchurch, New Zealand

## *ABSTRACT*

*This paper argues for the consideration of a decentralized, open, interoperable identity framework as a secure, scalable, user-centered meta-platform capable of leveraging many aggregate network advantages and delivery options for education and healthcare providers. An overview of the shortfalls and vulnerabilities of the current Internet and systems for identity management is first explained, followed by a summary of the status of development and primary proponents of decentralized, blockchain-enabled, self-sovereign identification (SSI). An examination of the Key Event Receipt Infrastructure (KERI) open-source decentralized key management infrastructure (DKMI) and its primary root-of-trust in self-certifying identifiers (SCID) is evaluated. This paper recommends KERI for consideration as a potential meta-platform overlay and solution for both the education and health industries as a means of attaining their primary goal of being more user versus institution-centric in their core interactions and processes. Finally, some pathways for future research are recommended.*

## *KEYWORDS*

*Distributed Ledger Technology, Digital Transformation, Self-Sovereign Identity, Education, Healthcare*

## 1. INTRODUCTION

In a technology-driven, digital world, many of today's largest and most influential businesses operate as open and inclusive 'platforms.' [1] Most are familiar with the leading platform-based software systems and companies prevailing. In the consumer context, we speak of Alphabet (Google) for searching, Amazon for purchasing goods, Facebook (now Meta), or Twitter for social media exchanges. In an enterprise or commercial context, the platforms are different, e.g., Salesforce for CRM, TradeLens, for logistics, and Amazon AWS or Microsoft Azure for cloud-based services. Such firms leverage cloud-based networked technologies to facilitate economic exchange, transfer information and connect people. These entities derive their primary value from their roles as intermediaries. [2]

The rise of Distributed Ledger Technology (DLT) has paved the way for the development of self-sovereign identity (SSI) — a new class of user-controlled resilient identity management systems securely enabled by DLT. This paper will examine how a blockchain-based decentralized identity management system can draw on the SSI framework to provide high-level security and transparency for all involved parties in public and private education and healthcare ecosystems.

DOI: 10.5121/ijnsa.2023.15201 

Furthermore, it further explores the potential utilization of a recently developed open-source, self-executing, DLT technology to establish a decentralized identity meta-platform overlaying the Internet. Such a meta-platform has significant potential to facilitate more cost-effective digital transformation and propel secure cooperation among educational and healthcare providers spanning different operators and end-users in multiple countries.

## 1.1. Network Effects – Centralization vs. Aggregated Cooperation

The principles and laws of network effects are at the heart of these extremely valuable companies built over the last 20 years. In general, it could be stated that the incremental progressive reduction that these platforms offer in transaction costs is what drives their expansion and market value. Some of these transaction costs include various aspects involving transfer, triangulation as well *the critical element of trust*. [3] Thus, the lower-per-transaction overhead accrues not only to the benefit of the platform provider's profitability but, via Metcalfe's law of network effects, to the aggregated value of the platform itself. [4]

Unfortunately, network effects are so powerful that they motivate network owners toward monopolistic objectives. In other words, as the network expands, both the value of participating and the cost of switching are sufficiently high that the entire group of potential participants consolidates around a single platform or network. The downsides start to occur when these powerful network effects are owned by centralized private companies. As network effects push industries towards monopoly, the owner of the network can assert, what MIT Cryptoeconomics Lab economist Cathy Barrera calls, "Market Power."

Market power arises when users or customers have few comparable alternative options for sources of the good or service being provided. This gives the seller the ability to raise prices, or in the case of some internet giants to charge transaction fees, and compile and sell user data, all as a condition for giving users access to the platform. [5]

Insidiously, the company's responsibility to shareholders means it will always look to maximize profits. To maximize this network-driven value formula, these platform companies have often adopted a type of "winner takes all" philosophy as the only way to achieve growth and their ongoing survival. Consequently, the net result is that the true winners are few and powerful, and typically highly centralized. Some suggest that we are living in the age of the platform economy and that all firms---not just technology firms—should consider operating as a platform. [6] In contrast, numerous others have become wary of the centralized dominance of these platform systems and their value proposition---i.e., the monetization of user data through data mining and advertisement-based revenue models. As a result, in recent years, *trust has diminished* in these would-be platforms owing to their respective maneuvers to achieve market dominance.

In 2019, Shoshana Zuboff, illuminated the dark side associated with these platform giants in a scathing analysis—coining the terms "surveillance capitalism," and "extraction imperative" as their fundamental business model. [7] Zuboff used these terms to describe a new economic order and logic that claims human experience and behavior as free raw material for commercial practices of extraction, prediction, and sales. Surveillance capitalism claims human experience as raw material for translation into behavioral data. That data is partially used to improve digital products or services, but most importantly, it is declared "proprietary behavioral surplus," fed into "machine intelligence" manufacturing processes producing predictive meta-data and user profiles. These "behavioral prediction products" are then sold in a new type of market: the "behavioral futures market." [7] Zuboff argues that in the battle for market domination and profit maximization, surveillance capitalists are on an endless quest to acquire ever-more predictive sources of behavioral surplus.

According to Zuboff, the first economic imperative of surveillance capitalism is *the extraction imperative*, meaning "raw material supplies must be produced at an ever-expanding scale." [7] Surveillance capitalists are thus bound to strive to obtain every detail about their human subjects as viable information for extraction. Thus, every society, every social relation, and transaction is now a "fresh terrain for rendition, calculation, modification, and prediction." [7]

In his essay, "*Why Decentralization Matters*," [8] Chris Dixon of Andreessen Horowitz captures the results of the Extraction Imperative with the following S-Curves:

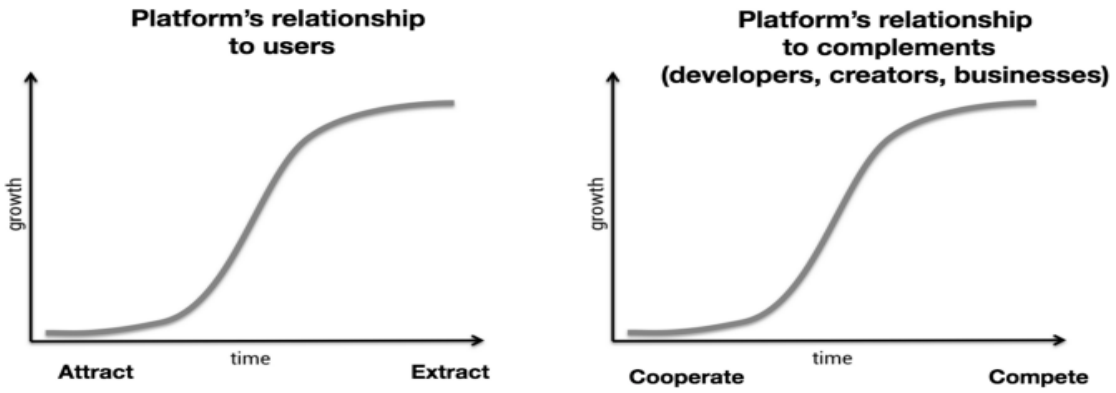


Figure 1. The Impact of the Extraction Imperative on Platform Company Relationships
Source: https://onezero.medium.com/why-decentralization-matters-5e3f79f7638e [8]

In short, when a platform-based provider reaches the top of the S-curve, their relationships with both users and network participants change from positive-sum to zero-sum. Thereafter, the easiest way to continue growing lies in extracting data from users and competition with prior partnerships for audiences and profits.

## 2. DISTRIBUTED LEDGER TECHNOLOGIES – THE REDUCTION OF CENTRALIZED PLATFORM INEFFICIENCIES AND THE INCREASE OF DECENTRALIZED NETWORK COOPERATION

Economists frequently view technology adoption through the lens of reducing or eliminating inefficiencies i.e., improving outcomes at both the micro and aggregate levels.

One of the inefficiencies that blockchain or distributed ledger technology may help mitigate is what Catalini and Gans call the cost of networking--where inefficiencies have arisen due to the market power of Internet platform giants. Their premise is that reducing the cost of networking significantly alters the trend toward monopolization because it disentangles the benefits of network effects from the detrimental impact of market power. [9] Catalini and Gans further build on this theory to discuss how blockchain technology can shape innovation and competition in digital platforms. They identify two key costs affected by the technology: (1) *the cost of* verification and (2) *the cost of networking*. The cost of verification relates to the ability to cheaply verify the state, including information about past transactions and their attributes, and the current owners or identity holders of digital assets. Blockchains can reduce the cost of networking owing to their ability to bootstrap and operate a marketplace without assigning control to a centralized intermediary. This is achieved by combining the ability to cheaply verify transitions that are particularly valuable from a network perspective, such as the contribution of the resources needed to operate, scale, and secure a decentralized network. [9]

The resultant decentralized digital marketplaces created using blockchain-based systems incentivize cooperation as they allow participants to *make joint investments in shared infrastructure and digital public utilities without assigning market power to a platform operator*. These new decentralized marketplaces are characterized by both increased competition and cooperation, in conjunction with lower barriers to entry and a reduction in privacy risk. On the other hand, because of their decentralized nature, they also introduce new types of inefficiencies and governance challenges. [9]

Whereas the utopian view has argued that distributed ledger technologies (DLTs) have the potential to transform every digital service by removing the need for intermediaries, Catalini and Gans convincingly argue that it is more likely that they can change the nature of intermediation by reducing the market power of intermediaries by progressively redefining how they add value to transactions.[9] Catalini and Gans have thus contributed to the current literature on DLTs by providing an underlying framework for understanding how the technology changes the types of transactions and networks that can be sustained, especially in a decentralized economy. Erikson similarly argues that the network effects of tomorrow will often be built around decentralized tokenized ecosystems in which there is no distinction between network participants and network owners. She further states:

> This transformation will occur because tokenized ecosystems can capture the value of the network for participants without the economic rent extraction (fees and data) that is characteristic of centralized network effect platforms — resulting in better outcomes for everyone. The combination of reduced costs, higher value capture by participants, and the powerful growth incentives that well-designed tokenized networks provide create the conditions necessary to supplant some of today's most powerful companies.in the 4IR (*4th Industrial Revolution-- definition added*) [10]

While we have come to expect that the fees and data demanded are simply the cost we must pay for the benefits that large platforms offer, decentralized blockchain-based networks provide a viable alternative. In this alternative, the owners are the market participants themselves and the use of tokenization not only keeps incentives aligned but adds a new level of impetus to network growth. Together, these factors suggest that many successful enterprises in the future could be organized not as centralized for-profit corporations driven by the extraction imperative, but rather as decentralized token-based economies with strong trust and incentive alignment between network owners and participants.

## 3. CYBERSECURITY AND TRENDS IN IDENTITY MANAGEMENT

The proliferation of digital services has placed digital identity at the forefront. As the use of online services has increased in recent years, institutions and end-users have faced an exacerbation in the growth of a complex, inconsistent, tangled, and insecure web of digital identity practices. Increased awareness of the implications associated with the existing digital management approaches and their deficiencies has come about because of this complexity. Moreover, as a direct result of these trends, the field of identity management has been ripe for change and disruption due to recurring incidents of data breaches that have led to personal information leaks and identity theft.

An inherent vulnerability exists in verifying and managing identities online because the Internet operates through protocols that identify *only technological endpoints* (e.g., IP addresses) *and not people, organizations, or other entities.*

Most online identities are currently centralized, which means that a single service provider controls them—such as the ubiquitous online platform services mentioned previously. This model results in identity data being siloed and fragmented across disparate cloud-based services and applications. In addition, under this centralized model, a user does not own his or her identity and exercises little or no control over how the identity is used or with whom the data is shared. The lack of control over one's identity and private data is a prime factor in the acceleration of mistrust and numerous other privacy issues.

Furthermore, there has been an increasing public concern about inadequate privacy laws and protection because data repositories are subject in many cases to a government's arbitrary access to identity data and extrajudicial surveillance without the prior consent of the user. In short, when users share their identity data with an organization, they lose visibility and control over how their data is stored or accessed. Depending on an organization's jurisdiction of operation and data storage location, they may also be subject to government legislation that will require them to provide access to their customer data, without the consent of the customer. This concern led the Court of Justice of the European Union (EU) in July 2021 to determine in the case of *Data Protection Commission v. Facebook Ireland Ltd. and Maximillian Schrems* that the *EU-U.S. Privacy Shield Framework* for data transfers is not adequate. The court found that the U.S. surveillance programs allowing the government access to personal data are not limited to what is strictly necessary and proportional as requested by EU law. [11]

Nowhere is this more problematic than in education and healthcare because of these industries' statutory obligation to protect all of their stakeholder's private data (e.g., involving minors and intellectual content as well as student profiles, certifications, degree transcripts in education or healthcare patient histories, financial and other records).

## 4. INTERNET IDENTITY – THE SSI PARADIGM SHIFT

Kim Cameron, Microsoft's Chief Architect for Identity from 2004 to 2019, made the following revealing statement-- **"**The Internet was built without an identity layer." [12] Cameron provided the answer of why the Internet excluded an identity layer in his series of essays called *The Laws of Identity*, published on his blog in 2004 and 2005. Cameron was prescient in his prediction and statement when he exclaimed further:

The Internet was built without a way to know who and what you are connecting to. This limits what we can do with it and exposes us to growing dangers. If we do nothing, we will face rapidly proliferating episodes of theft and deception that will cumulatively erode public trust in the Internet. [12]

When the Internet was initially developed in the 1960s and 1970s by the U.S. military (sponsored by *The Defense Advanced Research Projects Agency* (DARPA)), the problem it was designed to solve was *how* to *interconnect machines to share information and resources across multiple networks*. The solution developed at that time was a packet-based data exchange utilizing what we now term the TCP/IP protocol. It was proclaimed as a brilliant concept that finally enabled a true "network of networks." However, the severe limitation of the current Internet's TCP/IP protocol is that one only knows the address of the machine that you are connecting to -- it provides no information about the person, organization, or thing responsible for that machine with which you are communicating. [13]

Despite numerous efforts to solve the Internet identity problem, the lack of a breakthrough solution has proved Cameron's prognosis true many times over. Failure to solve the Internet ID problem has perhaps now reached the breaking point. A few examples may serve to illustrate the magnitude of the current problem.

- By 2017, the average business user had to keep track of 191 passwords [14] and surveys to verify their ID online. The result is that username/password management has become the most hated consumer experience on the Internet. [14]
- IBM President and CEO Ginni Rometty described cybercrime as "the greatest threat to every profession, every industry, every company in the world." [15]
- According to estimates from *Statista's Cybersecurity Outlook*, the global cost of cybercrime is expected to surge, from $8.44 trillion in 2022 to $23.84 trillion by 2027. [16]
- Over 90% of American consumers believe they have lost control of how their personal information is collected and used by all kinds of entities. [17]
- In 2016, 3 billion Yahoo accounts were hacked in one of the biggest breaches. [18]
- Sixty-three percent of network intrusions are the result of compromised user passwords. [19]
- According to the Identity Theft Resource Center (ITRC), data breaches were up over 14% in the first quarter of 2022 alone which comes on the heels of 2021's 68 percent increase in breaches over 2020, which beat the previous record, set in 2017, by 23 percent. [20]

## 4.1. Basic Models Currently Used for Establishing Digital Identity

Historically, three models for digital identity have been used. These are briefly described in the following sub-sections.

### 4.1.1. The Centralized Identity Model

The original centralized form of Internet identity and the one that in many cases is still in use today. Identification is established by registering an account (typically a username and password) with a website, service, or application. For this reason, it is also called "account-based identity." Examples include, but are not limited to, government ID numbers, passports, identity cards, driving licenses, invoices, Facebook logins, Twitter handles, and so on. All of these are issued by centralized governments or service providers like banks or telecom companies. The primary shortcomings of this type of digital ID system are that the onus of remembering and managing all the usernames and passwords (and in some cases other multi-factor authentication tools such as one-time codes) falls entirely upon the individual and none of the identity data is portable or reusable elsewhere.

### 4.1.2. The Federated Identity Model

To alleviate some of the issues associated with the centralized model the identity industry has developed the federated identity model. The basic idea is simple: insert a service provider, called an identity provider or IDP, in the middle. Using this model, users have one identity account with the IDP and can log in and share some basic identity data with any site, service, or app that uses the same IDP. Three generations of federated identity protocols have been developed since 2005—SAML, OAuth, and OpenID Connect. Using these protocols, SSO (Single Sign-On) is now a standard feature of most corporate intranets and extranets. Federated identity also started to catch on in the "consumer Internet," where it began to be called user-centric identity. Using protocols like OpenID Connect, social login buttons from Facebook, Google, Twitter, LinkedIn,

etc. are now a standard feature on many consumer-facing websites. Despite all the work that has gone into federated identity, it still has done nothing to solve the Internet's underlying missing identity layer problem.

#### 4.1.3. The Decentralized Identity Model

This new model inspired by blockchain technology that first surfaced in 2015 has accelerated rapidly, assimilating new developments in cryptography and decentralized systems. It has spawned new decentralized identity standards such as Verifiable Credentials (VCs) and Decentralized Identifiers (DIDs). The most important difference in this model is that it is no longer account-based. Instead, it works like identity in the real world, i.e., it is based on a direct relationship between peers, where neither "controls" the relationship with the other. This is true whether the other party is a person, an organization, or a thing.

#### 4.1.4. Self-Sovereign Identity (SSI)

Self-sovereign identity (SSI) represents a *new decentralized alternative* for digital identity on the Internet capable of validating "who" we are interacting with on websites, services, and apps, where trusted relationships are mandatory to access or protect classified information. Driven by innovative technologies and standards in cryptography, distributed networks, cloud computing, and smartphones, SSI is a paradigm shift for digital identity like other technology paradigms, (e.g., the shift from keyboard-driven user interfaces such as MS-DOS to graphical user interfaces like Windows or Apple iOS). It is critical to point out that the SSI paradigm shift represents not just a technology shift, *but a fundamental transition in the underlying infrastructure and power dynamics of the Internet itself*. Because there are now billions of people and multiple billions of devices on the Internet, and almost everyone is a stranger, the implications and complexity of this type of change in infrastructure are exceedingly complex. What is required, is an elegant, simple but near-universal solution.

The figure on the next page illustrates the differences between the centralized and federated models and the decentralized self-sovereign model. The latter puts the individual at the center. To fundamentally find a solution to the Internet's missing identity layer, industry pundits are now in agreement that a shift in control from the center of the network to the edges of the network, where all Internet users function and interact as peers are required. Global markets today are highly focused on business efficiency and customer experience, security, cost savings, and convenience. These trends represent the primary market demand driving SSI in its early stages. SSI is primarily a disruption to the existing Identity and Access Management (IAM) marketplace, and, like most disruptive technologies, it will give rise to new companies, new business models, and new subsegments within the IAM market.

### 4.2. Self-Sovereign Identity Platforms

There exists a rapidly growing number of SSI platforms, industry players, and technical groups committed to developing and improving the SSI and decentralized identity framework. Much of what is happening in the development of SSI is being made possible through the work of various technical groups that help design the requirements, specification standards, and processes for SSI. Some of the most prominent are summarized in the subsections below.

#### 4.2.1. World Wide Web Consortium (W3C)

The W3C is an international community that creates open standards for the web. [21] Its W3C Verifiable Credential Working Group [22] is actively working on the verifiable credential data

model and Security and Communication Networks use cases while the W3C Decentralized Identifier Working Group [23] is focused on developing the decentralized identifier specification, including its method registries and use cases.

#### 4.2.2. Rebooting of the Web of Trust (RWoT)

The RWoT group facilitates discussions on identity-related topics with a particular focus on decentralized trust-based identity systems. Various initiatives such as Decentralized Identifiers (DID), Decentralized Public Key Infrastructure (DPKI), and JavaScript Object Notation for Linked (JSON-LD) are among the initiatives currently being examined in RWoT. [24]

#### 4.2.3. Hyperledger Identity Group

This group promotes discussions, research, and collaboration on the management of digital identity data on decentralized platforms and in particular solutions related to Hyperledger. [25]

#### 4.2.4. Decentralized Identity Foundation (DIF) [26]

The DHF is a technical organization focused on developing foundational elements required for an open ecosystem for decentralized identity The DIF provides technical specifications and reference implementations and assists in coordinating the industry leaders. Identity hubs and universal resolvers are among the many projects incubated by DIF.

#### 4.2.5. The Digital ID and Authentication Council (DIACC) [27]

This council in Canada is a union of public and private sector players working together to create a trusted digital identity experience for Canadians.

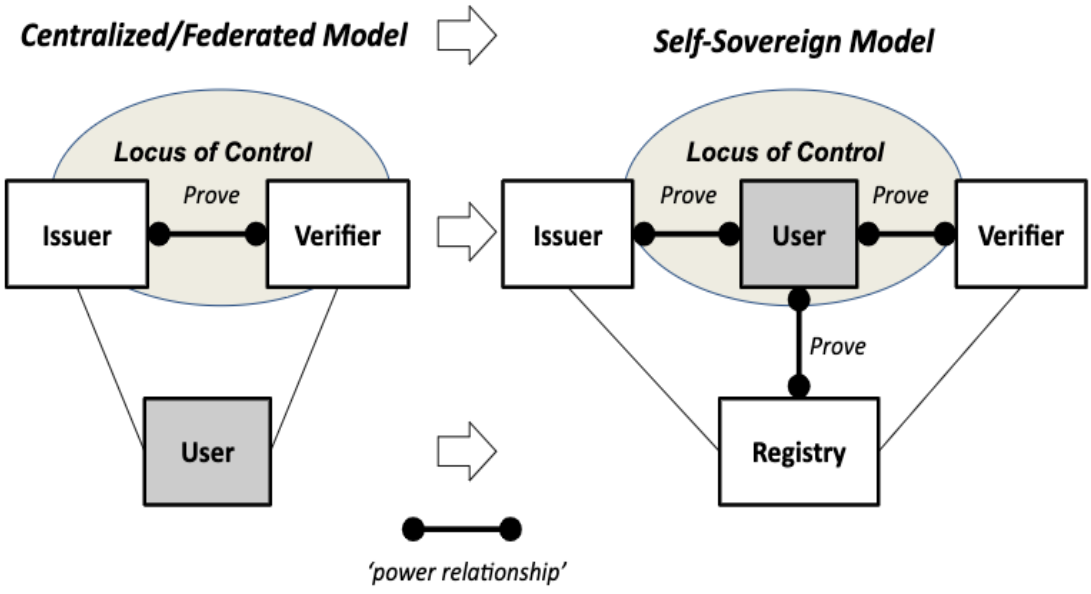


Figure 2. The Centralized/Federated Model vs. the Self-Sovereign Model
Source: https://livebook.manning.com/book/self-sovereign-identity/chapter-2

# 5. DIGITAL TRANSFORMATION (DX) – REDESIGN OF THE DELIVERY MODEL IN THE EDUCATION AND HEALTHCARE SECTORS

## 5.1. Education Sector

Verifying, securing, and managing identities, academic credentials, and the protection of intellectual property rights have always been critical to the education sector. Challenges in doing so have been exacerbated in recent years as more and more digital content has been created together with students' accelerated movement and participation online. Moreover, the COVID-19 pandemic has caused the largest disruption of education in history, having already had a near-universal impact on learners and teachers around the world, across schools, institutions, universities, and skills development establishments. [28] Students are now more than ever learning online--expanding their digital learning in real-time outside of the classroom.

A recent *VMware Future of Education Survey* highlights the changes that have made education student-centered and how higher education institutions are coping with this change and the demands for more digital transformation (DX). According to this same survey, 71% of the higher education institutions surveyed are looking to invest in DX and the integration of new technologies and virtual learning modalities.[29] Nonetheless, education leaders face considerable obstacles hindering their digital transformation and generally trail the commercial business sector in adapting to the systemic changes posed by DX. Most notable among those are: (1) Resistance to change on the part of key stakeholders such as teaching staff; (2) Unclear development paths and difficulty to execute process transformation necessary to complement technological change; and (3) Lack of clarity on the direct benefits for the learning outcomes from DX initiatives.

In a 2020 special report analyzing the top ten information technology issues and challenges that higher education institutions face, EDUCAUSE researchers ranked the following as having the highest priority:

#1. Information Security Strategy: Developing a risk-based security strategy that effectively detects, responds to, and prevents security threats and challenges.[30}
#2 Privacy: Safeguarding institutional constituents' privacy rights and maintaining accountability for protecting all types of restricted data.[30]
#3 *Sustainable Funding*: Developing funding models that can maintain quality and accommodate new needs and the growing use of IT services in an era of increasing budget constraints.[30]
#4. *Digital Integrations*: Ensuring system interoperability, scalability, and extensibility, as well as data integrity, security, standards, and governance, across multiple applications and platforms. [30]
#5. Student-Centric Higher Education: Creating a student-services ecosystem to support the entire student life cycle, from prospecting to enrollment, learning, job placement, alumni engagement, and continuing education. [30]

Given the stated priorities of higher education institutions in the U.S. listed above, it is significant that all of the highest priorities, except for sustainable funding, hold technological imperatives tied to the safe, secure management of data, transactional integrity, and private identity. As EDUCAUSE states, it is important to indicate, however, *that digital transformation is not fundamentally about technology in education, it is about culture*. EDUCAUSE defined this systemic imperative as "a series of deep and coordinated culture, workforce, and technology

shifts that enable new educational and operating models and transform an institution's strategic operations and value proposition." [30]

## 5.2. Healthcare Sector

*Practice Fusion*, the largest cloud-based electronic health record (EHR) provider in the United States, provided the following statistic about EHR adoption in 2014:

Less than a decade ago, nine out of ten doctors in the U.S. updated their patient's records by hand and stored them in color-coded files. By the end of 2017, approximately 90% of office-based physicians nationwide will be using electronic health records (EHRs). [31]

Today, by contrast, *Healthcare IT News* provides a graphical representation of the state of EHR interoperability showing the reality of how difficult it remains to move an EHR from one doctor to another in the United States. [32] Figure 3 shows how many different electronic medical records (EMRs) vendors are in use in affiliated medical practices in the United States, thus highlighting the difficulty of establishing any real interoperability.

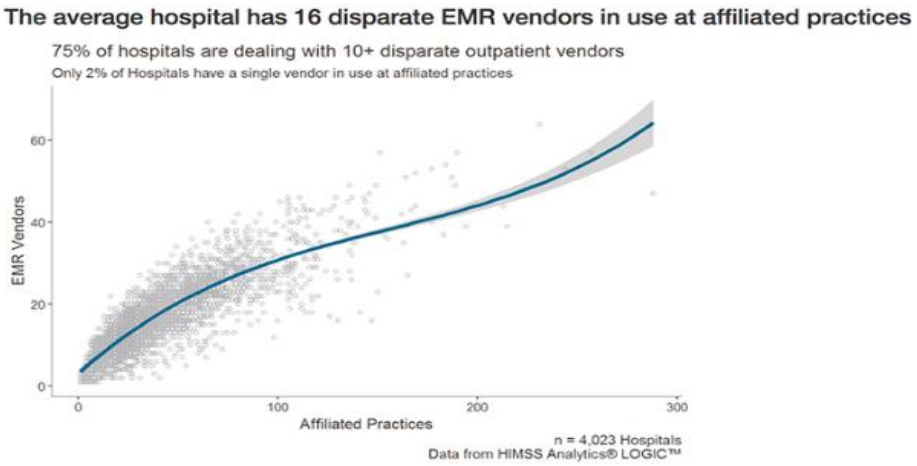


Figure 3.
https://www.healthcareitnews.com/news/why-ehr-data-interoperability-such-mess-3-charts

Sixteen distinct electronic health records platforms, according to statistics HIMSS Analytics pulled from its Logic database looking at 571,045 providers affiliated with 4,023 hospitals.
*Healthcare IT News* summed up this major issue in a recent publication this way:

The thorny matter of interoperability in healthcare, as it is or has historically been in other industries, is almost all-consuming among technology vendors and their clients. Indeed, a big part of the problem is exactly how many EHR companies are out there and more specifically, the average number of platforms hospitals are running today. [32]

What is the solution? *Healthcare IT News* is noticeably clear about what is required-- HIMSS Analytics Chief Revenue Officer Mitchell Icenhower states:

Achieving interoperability among different EHR platforms is so difficult, that the Centers for Medicare and Medicaid Services working with the Office of the National Coordinator for Health IT, the federal agency charged with leading public and private healthcare organizations toward interoperability essentially retooled the meaningful use of an EHR incentive program to focus on

enabling a more unified view of patient data. Health IT shops across America, meet to promote interoperability…There were three steps originally. Get as many hospitals as possible and medical groups to purchase a viable EHR, then meaningfully use that EHR, and the direction for the third step was to focus on qualitative value and quality measures… Icenhower added. Now they're saying instead of that 'we skipped the step where the patient is the center of the universe, and their dattea is spread across different systems,' so ONC shifted to focusing on the patient." [33]

Keep in mind, all of this is in the context of healthcare IT systems for doctors, hospitals, and medical institutions. It doesn't even contemplate yet *how the patient could participate in being "the center of the universe" of their healthcare data* [33]. How much easier would the whole EHR portability problem be if SSI were employed for patients? As *Healthcare IT News* states, patients would be able to:

(1) Instantly obtain copies (either on their phone or securely stored in a private cloud) of their EHR records immediately after any medical procedure. [33]
(2) Securely and privately share their EHR in seconds others of their choosing. [33]
(3) Provide secure, legally valid, auditable consent for medical procedures for themselves, family members, dependents, etc., directly from their smartphone or another networked device. [33]
(4) Have a lifetime history of vaccinations, allergies, immunities, etc. available in a verifiable electronic record to share in seconds—in person or remotely with schools, employers, doctors, nurses, or anyone who needs to verify it. [33]

This list does also not even mention how personal EHR might be accessed by apps on digital devices in neither one's healthcare management nor the impact of being able to share medical data securely and anonymously with universities and medical researchers who can use it to advance the state of public health for multiple stakeholders.

## 6. THE CONCEPT OF A META-PLATFORM

According to Smith et. al, a meta-platform is a platform that "*enables and fosters participant-controlled value transfer across and among other platforms and participants.*" [34] Because platforms in education and health always involve some type of network, the potential use of a meta-platform by and between entities in these industries has the potential to create for the cooperating institutions a network-of-networks effect. In this context, *cooperation vs. competition among educational platforms may be more advantageous and preferable in comparison to a centralized proprietary network approach*.

This paper argues for the consideration of a decentralized, open, interoperable identity framework as a secure, scalable, user-centered meta-platform capable of leveraging many aggregate network advantages in today's digital world. An investigation will be conducted in the following sections describing how a blockchain-enabled SSI might provide the connective pathway (in software terms, the "protocol") to free up the benefits of data-flow decentralization. Such an attempt could provide a more effective foundation for the creation of a meta-platform overlay for educational delivery while also affording its participants with a new level of control and portability. By making their participation portable to other platforms structured around the same protocol, these platforms empower the individual actors (e.g., education and healthcare providers and learners or clients) vis-a-vis the platform.

Recent years have seen significant momentum behind the establishment of a universal decentralized identity system based on open standards. These include, but are not limited to, the

W3C-supported decentralized identifier (DID) [35] and verifiable credential (VC) standards. [36] Various associations and industry groups promoting this open standard include the Decentralized Identity Foundation (DIF) [26], the Sovrin Foundation [37], and the HyperLedger Foundation projects (Indy [38], Aries [39], and Ursa [40].

Not only do macro-level advantages emerge for the cooperating education platforms themselves, but it is also hard to overstate the micro-level impact that decentralization of identity infrastructure might have on certain target populations such as Gen Z youth and young adults who see technology as an extension of themselves and are anxious to take back control. A decentralized SSI-validated control means that participants may form customized virtual platforms of their choosing which could also aggregate or amplify their identity's value, and manage their educational certifications, degrees, and profiles across multiple platforms. In addition, SSI participant control better balances the interests of participants and platform operators by decreasing the data protection liability of providers due to increased cooperation and the resultant network effects available via tokenization of identity. [41]

In today's platform economics, the major upfront cost of connecting to a platform is not the Internet connection itself, but the onboarding cost of creating an account with login credentials and provisioning electronic payment, with identity verification. This requires the participation of many companies and market-wide mechanisms--from insurance to credit cards to underwriters to regulatory bodies and infrastructure providers--all of whose costs are incorporated into our current networks of global commerce and educational delivery.

One of the limitations and problems with decentralized blockchain technology is that it still has a way to go before it can compete with the simple and convenient user experience offered by popular platform systems. In terms of onboarding, in comparison to the user of a new platform or network, many peer-to-peer digital networks or blockchain systems have comparatively high onboarding costs. As a result, in the case of peer-to-peer technologies, there can be a very steep learning curve relative to the increasingly convenient and intuitive commercial software. In the case of blockchain and cryptocurrency networks, participants have to contend with difficulty in managing keys, increased regulatory friction, and a higher level of complexity by contemporary standards. Today's plethora of competing and largely non-cooperative blockchain platforms only heighten this inefficiency and confusion.

On the other hand, a decentralized identity meta-platform overlaying the Internet allows those onboarding costs to be amortized across every platform a participant chooses to join. This potentially lowers the critical platform size and also the break-even point for the participant on each of the sub-platforms. It further offers the opportunity to be customized, scalable, and transacted via any device. All of this could readily accelerate network-of-network effects and overcome some of the inefficiencies created by competition while at the same time propelling increased cooperation between students' educational providers.

## 7. IoT Addressability and the 4th Industrial Revolution

We have been discussing about a power of networks effects in positive terms, but from the perspective of communications, the leverage of the network effect also involves a huge escalation in the number of digital devices, which in turn exacerbates the technical difficulty to link to and identify them. *Of critical concern then is central the issue of addressability.*

Today, the Internet is best described as a network comprised of all interconnected objects, of which the lion's share were traditionally human users and computers. When you add in the so-called Internet of Things (IoT), the number of addressable elements has already exceeded 100

billion, with analysts predicting a tenfold increase within a decade. [42] The resulting matchmaking complexity of possible connections between any given subgroup is an impossibly large number. Yet in today's user journeys or business environments, agents (whether human, machine, or software) increasingly need to access, control, or transact with a diverse group of these interconnected objects to achieve their goals in both the digital and physical worlds. *Needed is a universal standard and straightforward method to address, verify, and connect these objects.*

At some point, this enormous network-of-networks complexity will be equally pertinent in all business verticals, but today it is most keenly felt in businesses dependent on supply-chain management because of the large number of actors and multi-vendor components likely to be involved there.

Education and healthcare providers, except for research functions, frequently have analogous logistical barriers because of the preponderance of legacy-based IT infrastructure, intellectual property policies, and regulatory burden satisfying user-profiles and government regulatory mandates (at least in the U.S. context).

Human or object identities are stored in multiple centralized or federated systems such as a government, ERP or in manufacturing systems. From the standpoint of cryptography-based systems of trust and/or verification, each of these centralized authorities serves as its own root of trust, tightly controlling all identities' access to one another's credentials and trust information. An object trailing along a given value chain is interacting with multiple systems and platforms. Consequently, a new actor in any given value chain has no method to independently validate the credentials of a human or attributes of an object, except through the locally-governed central authority. Even then, the audit trail they can access rarely extends back much further than the jurisdiction of that authority unless data has been forwarded along in parallel to the human or object's trajectory. Ideally, a trust verification system and associated interoperable meta-platform protocol, built on some kind of universal addressing system should be utilized to help solve this huge verification complexity.

To be a truly global solution, easy-to-use and still safe from hacking, censorship, and other sovereign interference, such a meta-platform scheme must be independent of any vendor-defined naming API or otherwise centralized namespace, yet they usually need to be one-to-one mappable onto such APIs and namespaces.

*A participant-controlled meta-platform based on decentralized identity solves the problem of addressability and trust verification across participants involved in each value chain transaction*. The potential of enabling these devices to interact across a network of networks is inconceivably broad in scope. It may well prove to be many orders of magnitude broader than Facebook as an aggregator for human interactions and an enabler of new connections and networks.

Such a platform will be of particular value for the Fourth Industrial Revolution (4IR), i.e., the fusion of technology bridging the biological, physical, and digital spheres across industrial domains and societies. 4IR is moving our world into one big convoluted cyber-physical system in which everything is connected with everything else. In this digital fabric, there is ubiquitous network connectivity among IoT devices and digital agents establishing dynamically defined cooperation across interlinked digital value chains. We purport that an identity meta-platform is a prerequisite to establishing trust and cyber-physical security for dynamically defined cooperation.

## 8. KEY EVENT RECEIPT INFRASTRUCTURE (KERI)

Samuel M. Smith and his research associates at have developed a unique open-source meta-platform design capable of providing an identity system-based secure overlay for the Internet called *Key Event Receipt Infrastructure* (KERI). [43] Smith describes KERI as "a decentralized key management infrastructure (DKMI) based on key change events that support attestable key events and consensus-based verification of key events." [44]

As Smith indicates, an important differentiation to note with KERI, compared with other SSI constructs, is that security becomes a function of a given participant's infrastructure and not another entity's "trusted" internet infrastructure. Therefore, each controller of an identifier gets to pick their infrastructure, and each validator gets to pick their infrastructure. The key advantage here is that this approach does away with the vulnerabilities evident in the use of "trusted entities" and the Internet's current IP/DNS-based security protocols. In short, as Smith maintains that "*it is easier to secure personal keys than to ensure the security of all other external internet computing infrastructures."* [45]

The KERI solution includes a primary root-of-trust in self-certifying identifiers (SCID), and a formalism for Autonomic Identifiers (AIDs), which are part of an Autonomic Identity System (AIS) underlying KERI. This AIS utilizes what Smith describes as "minimally sufficient means" as the basic design principle to provide a trust-spanning layer for the Internet. The theory underlying the KERI model provides truly decentralized trust derived from the cryptographic root of trust of a given AID. Each AID is based on a self-certifying identifier (SCID) prefix. Associated with this system is a decentralized key management infrastructure (DKMI). [46]

The primary root of trust within the KERI design according to Smith are SCIDs that are bound at issuance to a cryptographic signing (public, private) key pair which may be transferred to a new key pair. Under the KERI system, the root-of-trust for each SCID is inherently decentralizable, giving the SCID three especially important properties: (1) a self-contained secure cryptographic root-of-trust, (2) Decentralized control via private key management, and (3) Universally unique identifiers. Smith further suggests that an SCID that does not support rotation of the underlying key pairs is not sustainable as a persistently secure identifier because eventually through exposure due to use, the key pairs may become weakened. [45]

In such an event, a chained key-event log of signed transfer statements provides verifiable control provenance. These event logs may be served up by any infrastructure enabling verification by anyone, anywhere, at any time. The primary key management operation is key rotation (transference) via a novel key pre-rotation scheme. [47] Because KERI is event streamed it enables the establishment of decentralized key management infrastructure (DKMI) that can operate in sync with data streaming applications such as web 3.0, IoT, and others where performance and scalability are more important. Smith indicates that core KERI engine is identifier independent, making it a good candidate for a universal portable DKMI. [48] [56] Outlined below is a brief list of the benefits of the KERI design and how it might satisfy various data management and ID challenges found in the education and healthcare sectors.

1. Self-certifying identifiers - A self-certifying identifier (SCID) is an identifier that can be proven to be the one-and-only identifier tied to a public key using cryptography alone--No blockchain needed. *An individual can prove the control of a KERI identifier without needing to rely on anyone else outside of his/her control*. [45]

Figure 4 below compares and differentiates the KERI identity system security overlay (meta-platform approach) and how it captures, generates, derives, verifies, and strengthens the binding between key pairs and digital identifiers (DID) through SCID issuance.

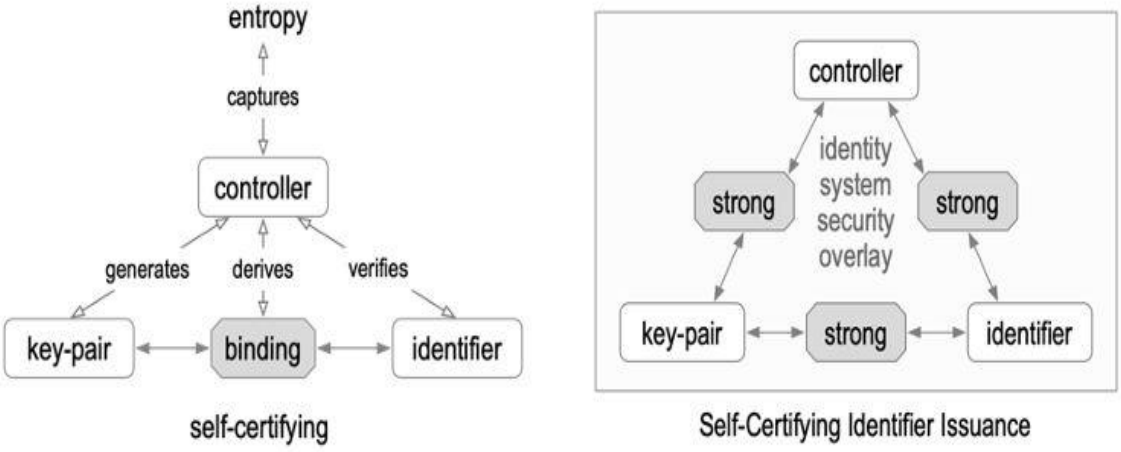


Figure 4. The KERI Self-Certifying Identifier Issuance and Binding
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf, page 9 [46]

2. Self-certifying Key Events - Each time an individual or entity changes ("rotates") their public/private key pair, KERI writes a new digitally signed message to a log file to prove and digitally verify that the same person made the change. This also proves control without needing to rely on anyone or an outside entity (even a blockchain). [46]

3. Witnesses and Key Event Logs – Each user of KERI keeps their copy of the KERI key event log, and can also, if they select, have other witnesses keep and digitally sign copies as witnesses. Although witnesses are not required, their use may provide additional evidence concerning the control of current holders of the public key(s) are not cheating. [46]

4. Pre-rotation as simple, safe, scalable protection against key compromise—While KERI cannot prevent the theft or loss of a person's private key— it incorporates an ingenious solution for hiding one's next private key that makes it nearly impossible to steal. One can safely "lock away" the next private key so it can't be stolen from a digital device thereby protecting that against the compromise of private keys. [46]

5. System-independent validation -- Because KERI identifiers and event logs are self-certifying, they can be witnessed by any system anywhere that can store and return data. As a result, these systems all can be used as witnesses if necessary. In addition, KERI identifiers and keys are not "ledger-locked," making them fully portable and capable of being validated using any ledger, distributed database, or another verifiable data registry. [46]

6. Delegated self-certifying identifiers enable enterprise-class key management – KERI identifiers can be "delegated", meaning one identifier can create another one that can prove its relationship with its parent—so you can create any hierarchy of identifiers & keys. Thus, with the KERI identifier and key delegation, enterprises can scale and manage delegation hierarchies of any size and complexity. [46]

7. Compatibility with the European Union General Data Protection Regulations (EU-GDPR) including the "right to be forgotten" – When a decentralized identifier for a person is written to

an immutable ledger, it can create a privacy issue because it cannot be erased. But KERI identifiers can use witnesses that permit erasure. The KERI infrastructure is therefore GDPR-compliant because it does not require the use of immutable ledgers and KERI event logs can be deleted without compromising security. [46]

## 9. POTENTIAL BENEFITS OF USING KERI FOR EDUCATION AND HEALTHCARE SYSTEMS

The primary takeaways for educators and healthcare providers to consider the deployment of the KERI infrastructure centers on the highly customizable features of the KERI methodology as discussed above. We list those features as stated by Smith, and while by no means all-inclusive, connect a few of the potential benefits for the use of KERI in education below.

(1) *Data management and security become largely a function of a given participant's infrastructure and not another entity's "trusted" Internet infrastructure.* [43]

Benefit: This KERI feature helps to satisfy the stated goal of educators' top priority to develop a risk-based security strategy that effectively detects, responds to, and prevents security threats and challenges. (Refer to #1 section 5.1)

(2) *Every controller of an identifier gets to pick their own infrastructure and each validator gets to pick their infrastructure.* [43]

Benefit: This KERI feature appears to help satisfy another high priority – the protection of data privacy and the safeguarding of institutional constituents' privacy rights and maintaining accountability for protecting all types of restricted data. (Refer #2 Section 5.1)

(3) *With KERI, identifier, and key delegation, enterprises can scale and manage delegation hierarchies of any size and complexity and self-certifying identifiers enable enterprise-class key management.* [43]

Benefit: This feature aligns with educators' digital integration objectives and helps to ensure overall system interoperability, scalability, and extensibility, as well as data integrity, security, standards, and governance, across multiple applications and platforms. The scalability and flexibility of the DKMI system could also help protect and validate the intellectual property rights, content/curricula, and research produced by professors and teachers (see section 5.1, #4).

(4) *System-independent validation and witnesses and key event logs – the KERI self-certifying feature allows for flexible validation or witnessing by any system anywhere that can store and return data and since identifiers and keys are not "ledger-locked," they are fully portable.* [43]

Benefit to both educational institution and students: Aids the ability of the education entity's need to verify and secure on a per-student basis the proctoring of tests and examinations. Moreover, it helps to offer accredited academic credentials safely and securely, certifications, grading, or degrees for all students that can be held in the students' portable portfolios themselves. This could also have a significant impact on reducing costs for storing, processing and transferring, and validating this data and documentation.

(5) *Delegated self-certifying identifiers enable enterprise-class key management – KERI identifiers can be "delegated", meaning one identifier can create another one that can prove its relationship with its parent—so you can create any hierarchy of identifiers.* [43]

Benefit: IF properly structured and key management is safe and controlled, this KERI feature is capable of establishing data interconnections between educational entities along a student's entire educational pathway (vertically) as well as facilitating increased sharing and collaboration with other institutions (horizontally). This would go a long way toward meeting the goal of a more student-centric educational approach and a student-services ecosystem to support the entire student life cycle, from prospecting to enrollment, learning, job placement, alumni engagement, and continuing education (refer to section 5.1, #5).

At present, as far as the writers can ascertain, there seems to be no other comparably simple technological ID system that offers a solution to the Internet's underlying security layer risks while also providing the above-mentioned customizable flexibility and simplicity of implementation.

In the healthcare sector, many of the same data protection, privacy safeguards, and transfer mechanisms articulated for education are also applicable. If the stated goal of healthcare providers in the United States is true, that being to establish an analogous ecosystem that is more patient-centric, then KERI might be deployed to move in that direction. The sheer number of EHR providers and the lack of interoperability even within one hospital's data management systems alone merits some consideration of the application of the KERI infrastructure. Also, if a fundamental problem is that healthcare administrators and IT managers "skipped the step where the patient is the center of the universe and their data is spread across different systems" [33] – likely due to the focus on machine vs. person architecture of today's Internet – then the scalable, delegable and independent enterprise-class key management features of KERI could help mitigate and simplify the interoperability of the overabundance of EHR systems now working at cross purposes in the American healthcare environment.

## 10. SUMMARY AND RECOMMENDATIONS FOR FUTURE RESEARCH

The field of Self-Sovereign Identity (SSI) is growing rapidly but still evolving. On one hand, rapid growth in the commercialization of SSI ecosystems has taken place, but there is still a growing awareness concerning the need for more research on cryptographic protocols empowering users' privacy and allaying trust concerns.

This paper has been limited its analysis and examined only in a summary fashion the current state of SSI along with its potential application to solve some major challenges faced by the education and healthcare sectors for data security and privacy increasingly demanded by their major stakeholders and end-users. A key barrier that must eventually be overcome is the inherent vulnerabilities of the current Internet's security layer protocols which are machine vs. human-centered. Observing the current state of SSI, this paper suggests consideration of the Key Event Receipt Infrastructure (KERI) as a possible viable alternative *because of its unique open-source meta-platform design capable of providing an identity system-based secure overlay for the Internet*. This being suggested, there exist many issues that must be analyzed and addressed before education or healthcare can implement KERI quickly and effectively. The following are suggested as some future directions for analysis and research:

(1) Key Management-- If leading educators and healthcare providers are sincere in their stated intent of making their student or patient experience the focus of their respective digital transformations, then the user experience must be a major avenue for research and testing. However, although the collective understanding of user experience has improved in the security space, only a small share of that change currently relates to key management. Losing a private key or password can lead to major vulnerabilities and economic costs. Proper key management in the context of SSI will be a major factor in its mass adoption rate.

(2) Data Sharing Approaches and Incentives -- In addition to key management, there are open research questions around the acceptable approaches by which users should be informed about, and consent to, sharing their data with other parties. In addition, as with any new business transition or initiative, the incentives and the return on investment on deployment, operation, and participation in an SSI network must be thoroughly articulated and analyzed.

(3) Interoperability - Moreover, institutions will need to understand how to design interoperable and consistent policies and specifications for SSI. One of the apparent advantages of the KERI ecosystem is that it provides a set of simplified standards to generate, bind, exchange, and validate identity credentials successfully under a framework that is interoperable with almost every existing database or data management system.

(4) Scope of Decentralization - One of the other research pathways and important considerations will be how to realize and articulate in each use case, the correct degree of decentralization that can support the vision and requirements of a user-centric identity model. More research must be done to better design critical identity operations such as identity issuance, user authentication, identity lookup, and secure data storage, as these actions may rely on some degree of centralization. At one end of the spectrum, solutions relying solely on smart contracts to facilitate decentralized governance have suffered from various vulnerabilities. At the other end, models that have required every member to engage and abide by onerous terms and conditions before joining may encounter the risk of unexpected or creeping centralization.

(5) Addressability and Entanglement with Underlying Systems--Lastly, the expected growth and future success of many of the currently available SSI systems are still entangled with the key problem of addressability. It will be important to carefully evaluate the scalability, operational cost, and performance of the underlying distributed ledger technology system.

## 11. CONCLUSIONS

The purpose of this paper has not been to provide a comprehensive overview of all SSI models. Highlighted, however, have been the significant shortfalls of the current infrastructure of the Internet and its growing inability to ensure the security, privacy, and trustworthiness of data exchanges to project all participants against the risk of loss or fraud. Identity is a central pillar of trust, and identity and access management are a multidisciplinary and growing field that will require devoted attention and much more research, experimentation, and collaboration. This being said, SSI should never be considered the total solution, however, in the age of surveillance capitalism, SSI represents, at present, the only realistic and user-centric identity model. This paper suggests the potential consideration by education and healthcare institutions of the KERI model that could be deployed by these industries as a more secure systemic component of their digital transformations.

## REFERENCES

[1] Parker, G., & Van Alstyne, M. W. (2017) “Innovation, Openness, and Platform Control,” Management Science. https://www.researchgate.net/publication/319074337_Innovation_Openness_and_Platform_Control

[2] Hagiu, A. & Wright, J. (2015) “Multi-sided platforms”, Harvard Business School Working Paper, No.15-037. https://www.hbs.edu/ris/Publication%20Files/15-037_cb5afe51-6150-4be9-ace2-39c6a8ace6d4.pdf

[3] Munger, M.C. (2018) Tomorrow 3.0: Transaction costs and the Sharing Economy, United Kingdom: Cambridge University Press. https://assets.cambridge.org/97811084/47348/frontmatter/9781108447348_frontmatter.pdf

[4] Metcalfe, B. (2013) "Metcalfe's law after 40 years of Ethernet", Computer, vol. 46, no. 12, pp.26–31. https://www.semanticscholar.org/paper/Metcalfe's-Law-after-40-Years-of-Ethernet-Metcalfe/14024f7e61706829fd07672cf03da2fd6c7a08da

[5] Berrera, C. (2018) "The Blockchain Effect: Network Effects without Market Power Costs", MIT Cryptoeconomics Lab, https://medium.com/mit-cryptoeconomics-lab/the-blockchain-effect-86bd01006ec2

[6] Altman, E. J., & Tushman, M. L. (2017) "Platforms, Open/User Innovation, and Ecosystems: A Strategic Leadership Perspective", Harvard Business School Organizational Behavior Unit Working Paper, No. 17-076 https://www.hbs.edu/ris/Publication%20Files/17-076_89f9f387-6692-41ca-a744-3528dc569c23.pdf

[7] Zuboff, Shoshana (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, Public Affairs, ISBN-13: 9781610395694, pp.8, 87, 399 https://www.publicaffairsbooks.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/

[8] Dixon, C. (2018) "Why Decentralization Matters", https://onezero.medium.com/why-decentralization-matters-5e3f79f7638e

[9] Catalini, C. & Gans, J.S. (2019) "Some Simple Economics of the Blockchain", Rotman School of Management Working Paper, No.2874598, MIT Sloan Research Paper, No. 5191-16, https://ssrn.com/abstract=2874598 or http://dx.doi.org/10.2139/ssrn.2874598

[10] Erickson, K. J. (2018) "The Future Of Network Effects: Tokenization and the End of Extraction", https://medium.com/public-market/the-future-of-network-effects-tokenization-and-the-end-of-extraction-a0f895639ffb

[11] Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems (2020), Case C-311/18, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=%20CELEX%3A62018CJ0311&qid=1616638710605

[12] Cameron, K. "The Laws of Identity", Kim Cameron's Identity Weblog, http://www.identityblog.com/?p=352

[13] "MAC Spoofing - Note: Hackers have demonstrated how to change a computer's hardware (MAC) or IP address before they are sent to remote network devices. This makes it nearly impossible to rely on, or trust, current network-level identifiers" (accessed 2022), Wikipedia.org, https://en.wikipedia.org/wiki/MAC_spoofing

[14] "Average Business User Has 191 Passwords" (2017) Cybersecurity | Security Newswire | Cybersecurity News, https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords

[15] Morgan, S. (2018) "IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'", Forbes, http://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/

[16] Fleck, A. (2022) "Cybercrime Expected to Skyrocket in Coming Years", Statista Cybercrime, https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/#:~:text=According%20to%20estimates%20from%20Statista's,to%20%2423.84%20trillion%20by%202027 .

[17] Rainie, L. (2018) "Americans' complicated feelings about social media in an era of privacy concerns", Pew Research Center, http://www.pewresearch.org/fact-tank/2018/03/27/americans-complicated-feelings-about-social-media-in-an-era-of-privacy-concerns/

[18] "Yahoo Provides Notice to Additional Users Affected By Previously Disclosed 2013 Data Theft" (2017), Business Wire, https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/

[19] "63% of Data Breaches Result From Week or Stolen Passwords" (2017), ID Agent, https://www.idagent.com/blog/2017-06-16-63-data-breaches-result-weak-stolen-passwords/

[20] Sveinsson, R.L. "Top 10 Data Breaches So Far in 2022", ERM Protect Cybersecurity Solutions, https://ermprotect.com/blog/top-10-data-breaches-so-far-in-2022/

[21] World Wide Web Consortium (W3C) (2021), https://www.w3.org/

[22] Verifiable Credentials Working Group, W3C (2021), https://www.w3.org/2017/vc/WG/

[23] DID Working Group, W3C (2021), https://www.w3.org/2019/did-wg/.

[24] "Welcome to the Web of Trust", Rebooting the Web of Trust, https://www.weboftrust.info/

[25] Identity Working Group, Hyperledger Confluence (2021), https://wiki.hyperledger.org/display/IWG/Identity+%20Working+Group.

[26] DIF-Decentralized Identity Foundation (2021), https://identity.foundation/.
[27] Digital ID for Canadians (2021), DIACC CCIAN, https://diacc.ca
[28] Bureau, B.O. (2021) "71% Higher Education Institutions Are Adopting Digital Pedagogies For Post-Covid19 World | Survey", BW Education, http://bweducation.businessworld.in/article/71-Higher-Education-Institutions-Are-Adopting-Digital-Pedagogies-For-Post-Covid19-World-Survey/26-08-2021-401930
[29] "Digital Transformation and Integration of New Technologies: A Priority for Higher Education Institutions – VMware Education Research Reveals" (2021), VMware, https://news.vmware.com/in/releases/digital_transformation_and_integration_of_new_technologies_a_priority_for_higher_education_institutions
[30] Grajek, S. & the 2019–2020 EDUCAUSE IT Issues Panel (2020) "Top 10 IT Issues, 2020: The Drive to Digital Transformation Begins", EDUCAUSE Review, p.7 https://er.educause.edu/articles/2020/1/top-10-it-issues-2020-the-drive-to-digital-transformation-begins
[31] Vestal, C. (2014) "Some states lag in using electronic health records", USA Today, http://www.usatoday.com/story/news/nation/2014/03/19/stateline-electronic-health-records/6600377/
[32] Sullivan, T. (2018) "Why EHR data interoperability is such a mess in 3 charts", HIMSS, https://www.healthcareitnews.com/news/why-ehr-data-interoperability-such-mess-3-charts
[33] Smith, S.M. (2019) "Meta-Platforms and Cooperative Network-of-Networks Effects: Why Decentralized Platforms Will Eat Centralized Platforms", SelfRule, https://medium.com/selfrule/meta-platforms-andcooperative-network-of-networks-efects-6e61eb15c586
[34] Smith, S.M., Conway, S., Hughes, A., Ma, M., Poole, J., Riedel, M. & Stöcker, C. (2019) "A DID for Everything: Attribution, Verification, and Provenance for Entities and Data Items," https://github.com/WebOfTrustInfo/rwot7toronto/blob/master/fnaldocuments/A_DID_for_everything.pdf
[35] Sporny, M., Longley, D., Sabadello, M., Reed, D., Steele, O. & Allen, C. (2022) "Decentralized Identifiers (DIDs) v.1.0", W3C Draft Community Report https://rdm.mpdl.mpg.de/2022/11/28/decentralized-identifiers-for-research-data/
[36] Sporny, M., Longley, D. & Chadwick, D. (2022) "Verifiable Credentials Data Model v1.1", W3C https://www.w3.org/TR/did-core /
[37] "Sovrin: A Protocol and Token for Self- Sovereign Identity and Decentralized Trust," (2018), Sovrin.org, https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf
[38] HyperLedger Indy Project, Hyperledger Foundation, https://www.hyperledger.org/projects/hyperledger-indy
[39] HyperLedger Aries Project, Hyperledger Foundation, https://www.hyperledger.org/projects/aries
[40] Hyperledger Ursa Project, Hyperledger Foundation, https://www.hyperledger.org/projects/ursa
[41] Erickson, K. J. (2018) "The Future Of Network Effects: Tokenization and the End of Extraction," Public Market, https://medium.com/public-market/the-future-of-network-effects-tokenization-and-the-end-of-extraction-a0f895639ffb
[42] Morrish, J., Hatton, M. & Arnott, M. (2022) "New report from Transforma Insights predicts ten-fold growth in AI use over the next decade", Transforma Insights, https://transformainsights.com/news/new-report-ten-fold-ai-growth
[43] "Welcome to KERI", Key Event Receipt Infrastructure (KERI), https://keri.one
[44] Smith, S. M (2020) "Universal Identifier Theory", https://raw.githubusercontent.com/SmithSamuelM/Papers/master/whitepapers/IdentifierTheory_web.pdf, p.18
[45] Smith, S. M. (2015) "Open Reputation Framework", https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/open-reputation-low-level-whitepaper.pdf
[46] Smith, S. M., (2021) "Key Event Receipt Infrastructure (KERI) Design v.2.60", https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf

[47] Smith, S. M. & Gupta, V. (2018) "Decentralized Autonomic Data (DAD) and the three R's of Key Management: A White Paper from Rebooting the Web of Trust VI", https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/DecentralizedAutonomicData.pdf

[48] Smith, S. M. (2019) "Key Event Receipt Infrastructure (KERI) Design and Build v.1.6", https://arxiv.org/abs/1907.02143

## AUTHORS

**Dr. Gregory H. Jackson**, Ph.D., MBA retired in 2022 from Utah Valley University. His doctoral thesis at the University of Buckingham examined the utilization of open-source distributed ledger technologies to integrate Anglophone and Indigenous pedagogies as s methodology to propel learning more efficiently and at a lower cost. He currently works as a CFO for Adayge Inc., a company incubating and testing open-source, blockchain-based containerized computing microservices. Dr. Jackson also currently serves on several NGO boards implementing digital systems and educational opportunities for Indigenous individuals worldwide.

**Dr. Karaitiana Taiuru**, Ph.D., is an honorary academic at the University of Auckland, New Zealand where he lectures on Data Sovereignty and researches Māori ethics with robotics. He is a Mātauranga & Kaupapa Māori Authority and conducts an active consultancy practice. His major research interests lie in the areas of traditional Māori ethics with justice, health, data, sovereignty, robotics, and AI. His Ph.D. researched Traditional Māori ethics and Data Sovereignty with DNA.