

Decentralized Identity Management Using Blockchain: Cube Framework for Secure Usage of IS Resources

Ashish Singla, Management Development Institute, Gurgaon, India*

 <https://orcid.org/0000-0001-6590-0761>

Nakul Gupta, Management Development Institute, Gurgaon, India

 <https://orcid.org/0000-0002-8781-3287>

Prageet Aeron, Management Development Institute, Gurgaon, India

 <https://orcid.org/0000-0003-3957-5912>

Anshul Jain, Management Development Institute, Gurgaon, India

 <https://orcid.org/0000-0002-4007-5512>

Divya Sharma, Management Development Institute, Gurgaon, India

 <https://orcid.org/0000-0002-5273-9654>

Sangeeta Shah Bhargava, Management Development Institute, Gurgaon, India

 <https://orcid.org/0000-0001-7955-4660>

ABSTRACT

This article explores the usage of decentralised identity (DID) management using blockchain in global organisations to support secure usage of information resources. Blockchain as technology was initially introduced as a cryptocurrency and there have been challenges in its adoption for enterprise applications such as identity management. DID is emerging as one of the strong blockchain adoption use cases. Industry pioneers and users across domains have started exploring DID use cases, which help better protect their personal data and application access control as compared to traditional, central, or federated identity management models. In this exploratory work, the authors employ qualitative secondary case-based study research methodology to understand the challenges of the current digital identity management landscape and explore the possible benefits of DID as an emerging identity management paradigm. They propose a conceptual cube framework for analysing and studying various DID platforms thereby contributing to both the theory and practice of digitally secure identity.

KEYWORDS

Blockchain, Decentralised Identity Management, Distributed Ledger Technology, Identity Management, Information Security, Interoperability

DOI: 10.4018/JGIM.315283

*Corresponding Author

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

INTRODUCTION

Proving one's digital identity has become crucial when accessing government and commercial services or participating in the digital and mobile economy (Rannenbergh, 2009; Wang et al., 2020). The criticality of establishing digital identity varies by context. For example, minimal verification is needed when establishing identity for an e-commerce transaction than a passport or social benefits by a government agency. Still, authentication of digital identity is necessary for initiating most digital transactions (Madon & Schoemaker, 2021).

In the current paradigm of the Internet, digital identity services are provided to users by organizations that capture and store personal and confidential information in central databases supported by either inhouse or third-party data protection mechanisms. Examples of digital identity issuers include government entities (for example, Aadhar in India) and non-government entities (for example, Google Id or OAuth). These entities capture users' personal sensitive information like date of birth, gender, address, mobile number, and biometric information (i.e., eye retina scan, thumb and finger scan, or face scan).

Research has shown that securing centralized databases is a costly and challenging task for most organizations (Ngwenyama et al., 2021; Wang, 2021). Due to paucity of appropriate security mechanisms, it is common for personal information stored in central databases to get compromised through security breaches. Such incidents cause financial and reputational loss for organizations (Bose & Leung, 2019; Juma'h & Alnsour, 2021; Sen & Borle, 2015). A breach can also have adverse consequences for individual users (Karwatzki et al., 2017; McKnight et al., 2002). In 2014, hackers ransacked the population identification (ID) codes of almost 20 million South Koreans, including the country's president (Thomson, 2014). In March 2017, personally identifying data of hundreds of millions of people, including 147 million names and dates of birth, 145 million social security numbers, and 209,000 credit and debit card numbers and expiration dates (Fair, 2019), were stolen from Equifax, a credit reporting agency that assesses the financial health of nearly every person in the United States (Fair, 2019). These are only a few examples of the large number of ID security breaches across the globe.

The phenomenon of identity theft has also become embedded in popular culture. The popular Netflix show, "Jamtara – Sabka Number Aeyga" (Padhi, 2020), showcases how miscreants run phishing operations that target those who are digitally illiterate or less tech-savvy.

Research has shown that a limited understanding of digital systems that are used to offer digital services is likely to make large populations, including old, young, and illiterate, vulnerable to cybercrime (Cruz-Jesus et al., 2018; Lee, 1999; Niehaves & Plattfaut, 2014; Reaves, 2017). This situation has also drawn the attention of regulatory agencies. In May 2018, the European Union (EU) enforced the new General Data Protection Regulation (GDPR), which aims to protect users by giving them greater control over their personal online data (Voigt & Von dem Bussche, 2017). Similar regulatory attempts are also being undertaken elsewhere, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 in the U.S. (Annas, 2003) and the Personal Data Protection Bill (PDPB) of 2018 in India (Prasad & Menon, 2020).

Despite regulatory efforts, the proliferation and ubiquity of digital services calls for the provision of reliable frameworks for managing the digital identity of individuals in digital ecosystems (Höller et al., 2022). Cameron's (2005) seminal work on digital identity proposed the "laws of identity" for successful management of digital identity. However, most centrally managed digital identity infrastructures (for example, Aadhar, Google Id, etc.) are not compatible with these laws. Cameron (2005) recommended that digital identity be coupled with its human user, allowing the human user to control their digital identity and associated personal data. It is also suggested that the digital identity be managed through a system that allows scaling across identity providers and service providers, while revealing minimal information to ensure security. Most digital identity systems, however, neither allow the users to control their digital identity information nor scale across services. This, in

turn, leads to balkanization of digital identity as users create multiple digital identities for different digital contexts (Allen, 2016).

Nonetheless, with the development and commercialization of distributed and decentralized information infrastructures like blockchain, alternatives to a centrally issued and controlled digital identity have emerged in the form of decentralized identity (DID) or self-sovereign identity (SSI) (Mühle, 2018). SSI relies on the user to maintain and manage their digital identity in a secure data store and present it for verification when prompted by a verifier (Chango, 2022). In this way, SSI enables full control of the digital identity to the holder of the identity (Allen, 2016). SSI is managed and maintained in a decentralized manner over a blockchain that reduces the possibility of catastrophic cybercrime, such as a data breach, identity theft, or misuse by mitigating the risk of a single central database being exposed to miscreants (Soltani, 2021). For instance, eIDAS (Cuijpers, 2014) enables access to basic services for individuals in countries they do not normally live in. Such systems of digital identity are valuable for individuals and beneficial to perspective of service providers because they can easily ascertain the validity of identifying information to initiate a transaction without having to act as a custodian of the sensitive information. Important implications of reduced data custody are lower costs for infrastructure, security, and regulatory compliance and the reduced privacy burden for business activities (Lesavre, 2019).

It is expected that DID will ease the provision of a range of private and public sector services that rely on accurately linking individuals with personal information (Barnard, 2022). It is also purported to enable users to monetize their identity (Harvey et al., 2018) rather than having a third-party like Facebook monetize their identity (Andrews, 2012). Given the emerging importance of establishing and securing digital identity, many frameworks and protocols claiming to address this pursuit are being developed under the broader umbrella of Web 3.0 (Davis, 2020). However, the extent to which these frameworks establish a robust, scalable, trustworthy, and secure digital identity remains an underexplored question (Rudman & Bruwer, 2016). Hence, this study is motivated to understand the facets that are critical and resonant with the “goal of establishing digital identity” and robust, scalable, trustworthy, and secure information system(s). The following research questions (RQ) are explored to pursue the overarching research objective:

RQ1: How does a decentralized identity framework differ from centralized and distributed identity frameworks? How do stakeholders interact in decentralized identity management?

RQ2: What are the essential characteristics of existing DID platform architectures?

RQ3: How can the various DID platforms be classified according to the identified essential characteristics?

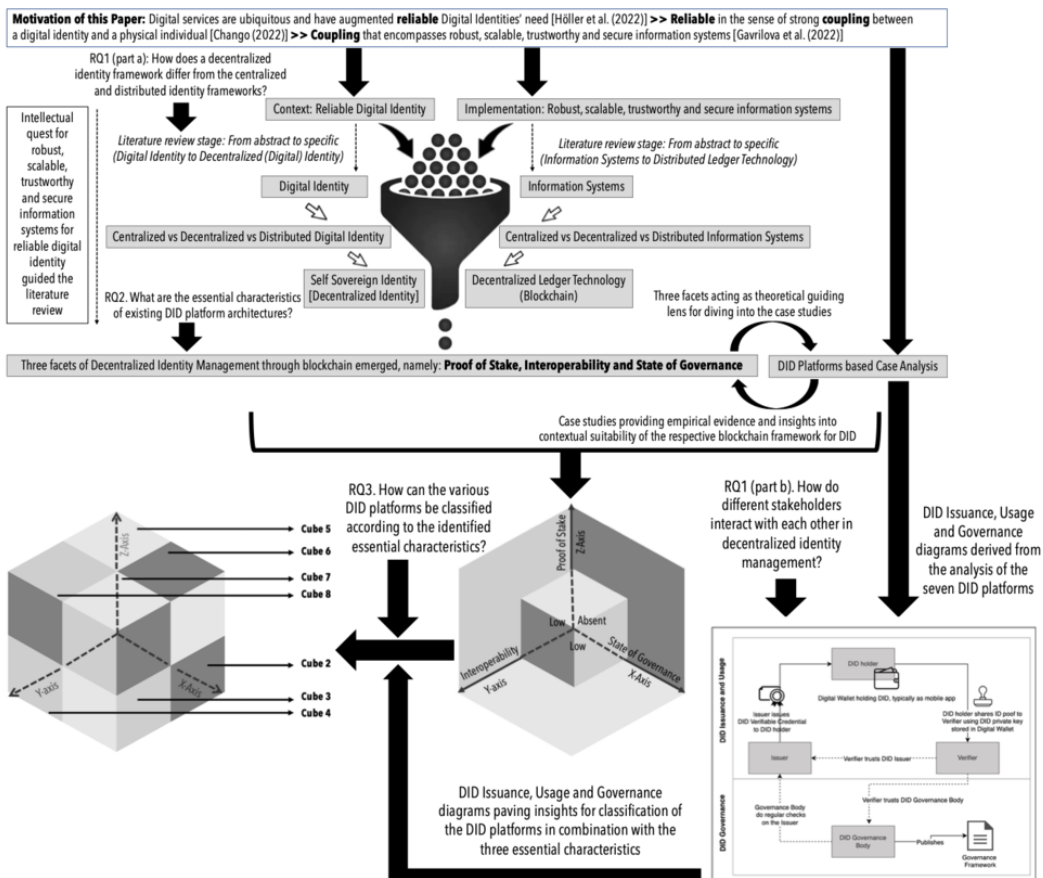
This study’s approach to addressing these research questions is summarized in Figure 1. Research motivation guides the overarching methodology. It has already been mentioned that digital services are ubiquitous in contemporary times; efficient consumption and delivery of the same require constant verification of digital identities (Höller & Mayrhofer, 2022). Digital identities must be reliable in terms of strong coupling between the digital identity and physical individual (Chango, 2022). For stakeholders to trust the digital identity, the establishment of digital identity must be driven by robust, scalable, trustworthy, and secure information systems (Gavrilova, 2022; Seltsikas & O’Keefe, 2010).

Given the emergent nature of information systems and the available technological frameworks of DID, this work is an exploratory study encompassing theoretical logic established through extant literature and empirical logic through secondary cases analyzed using multiple case study methods (Eisenhardt & Graebner, 2007). The literature review helped establish the scope and boundary of the key concept central to this article, namely digital identity information systems (for establishing the digital identity). This part of the literature review encompassed discussion and intellectual debate from an abstract level to the respective specific level (Van Fenema & Keers, 2018). Literature from academia and industry was explored to understand the nuances of centralized, decentralized, and

distributed identities and information systems. This helped in addressing RQ1. A literature review also spotlighted three key facets of decentralized identity management through blockchain-based information systems, namely: (1) proof of stake; (2) interoperability; and (3) state of governance.

Using purposive sampling and expert advice, seven leading platforms that offer DID services were identified. Their features were studied to understand their characteristics and use cases, considering theoretical grounding that was established in terms of proof of stake, interoperability; and state of governance. These three facets acted as axes in space, wherein each axis has two possible states of existence (values) to consider. Two possible values for each of the axes meant the study could imagine the space as an ensemble of 2^3 (equal to 8) small cubes. The proof of stake values were absent or present, the values for interoperability were low or high, and the values for state of governance were low or high. This paved the way for cross case analysis, wherein each of the seven DID platforms acted as a case. Through cross case analysis (Yin, 2014) and discussions with experts, the research meaningfully distilled and formulated characteristics of each of the eight cubes. This analysis process was enriched by studying the DID issuance, usage, and governance user diagrams for the DID platforms. The eight cubes that emerged, resultant of this activity, form an operational DID taxonomy that helps to classify and arrange the seven platforms. At the same time, it leaves room for work-in-progress DID platforms. These cubes and associated characteristics were then linked with a use case to enable practitioners and future scholars in seeing the utility and possibilities of extension of the proposed cube framework.

Figure 1. Overarching Approach of the Research Article and Evolution of Cube Framework by Intertwining of Theoretical and Evidence-Based Methods



The current study contributes to both theory and practice. From a theoretical perspective, it brings together disparate threads of identity management, secure identity, and distributed logic to offer a holistic picture of contemporary DID. It also documents a process overview and stakeholder interaction for digital identity management to clarify the utilization of contemporary architecture. Further, the study brings together DID use cases to identify three key facets of DID architecture and establish an operating taxonomy for studying DID. Finally, the research utilizes a taxonomy to establish mapping between DID facets and possible industry use cases. To the best of the researchers' knowledge, none of the above activities have been brought together in the form of a cube framework. This work offers scholars in the field an interesting pivot to explore the evolving domain of DID. It also offers a working guide for practitioners in making technology choices for identity management.

The article's remaining sections are structured as follows. The next section presents the related literature on digital identity, drawing out the essential aspects of decentralized digital identity. Thereafter, the study presents a brief overview of the technology infrastructure used to manage digital and, specifically, decentralized digital identity. This is followed by an explanation of decentralized identity management. Then, the study specifies the research methodology, presenting the current state of art of decentralized identity management with an overview of seven prominent platforms that offer DID services. Through cross-case comparison, the researchers arrive at the essential characteristics of DID platforms. These are used to create a DID typology that classifies DID platforms according to their architecture. The article concludes with a discussion on the findings, scope for future work, and limitations of the study.

IDENTITY

Identity literature has developed not only as a philosophical topic (for example, exploring questions like "Who am I?"), but also as a psychological, sociological, and economic construct (Akerlof & Kranton, 2000; Hammack, 2008; Lawler, 2015; Quine, 1950). In common parlance, identity implies the essential and/or distinguishing characteristics of an individual. Identity is used to refer to an individual's traits, beliefs, and personality attributes, as well as race, ethnicity, gender, religion, etc. Even in a literary sense, "identity" as a construct has taken different contextual meanings (Brubaker & Cooper, 2000), ranging from identity as the foundation of social or political action to implying sameness among members of a group, a core condition of "selfhood," and the product of social or political action.

Identity can broadly be understood along the two dimensions of "sameness" and "selfhood" (Ricoeur, 1992). Sameness relates to characteristics that are persistent; selfhood relates to characteristics that ascribe uniqueness. Over time, identity has also come to be understood in a post-modernist and post-structuralist sense as the fluctuating, multiple, and fragmented nature of "self" (Brubaker & Cooper, 2000).

Information systems research has built on the traditional notions of identity to propound the notions of digital identity and information technology (IT) identity. While digital identity deals with the unique representation of an entity in a digital context (Allison et al., 2005; Camp, 2004; Soltani et al., 2021), IT identity signifies "the extent to which an individual views use of an IT as integral to her sense of self" (Carter & Grover, 2015, p. X). This research draws on the former notion of digital identity, which establishes a digital object as being the object it purports to be (Allison et al., 2005).

Digital Identity

According to the National Institute of Standards and Technology (NIST), digital identity refers to the "unique representation of a subject engaged in an online transaction" (Grassi et al., 2020, p. X). Here, digital identity pertains to the online persona of a subject or a partial identity. It consists of a subset of identity attributes of an entity (Soltani, 2021). A digital identity is a machine-readable form of

human identity that uniquely identifies an individual in the context of a focal digital service, enables authenticated access to the service, and authorizes certain actions by the individual (Nyst et al., 2016).

Digital identity models have advanced from centralized to distributed and decentralized identity.

Centralized Identity

Centralized identity is issued and authenticated by a centralized authority or third-party service provider like Amazon for a specific purpose (Allen, 2016; Stockburger et al., 2021). Centralized identity ascribes more power to the issuing authority than the individuals associated with the identity. The central authority can deny the individual's identity or confirm a false identity. Furthermore, centralized identity entails the balkanization of identity as users are forced to create separate identities for different websites and online services. Centralized identity proliferates the current Internet. It has resulted in users having to maintain multiple digital identities without having complete control.

Federated Identity

Federated identity is a centralized identity that enables users to use the same credentials to access multiple digital services within a federation via single sign-on services. For example, Google account credentials can be used to log in to other services like YouTube, Gmail, and Google Docs. Federated identity reduces the problem of balkanization of identity; however, control over identity persists with the federation and not the individual.

User-Centric Identity

Another type of centralized identity, user-centric identity, delegates greater control over digital identity to individual users. User-centric identity is issued by a digital identity service, such as OpenID or OAuth. It allows users to independently manage and maintain their identity. Users can authorize these services to verify their identity to other third parties without disclosing users' confidential information. User-centric identity enables greater portability. Still, it does not provide full control to the user because the ownership and control of the user's digital identity remains with the centralized digital identity service provider.

Distributed Identity

Distributed identity refers to digital identity that is managed through a network of peers (Kruk et al., 2006). In this case, identification, authorization, and access rights are delegated through a community of individuals or nodes (for example, a social network or a federation of organizations). The participants in a distributed identity system are considered equal, with any of them acting as the issuer of digital identity that may be used to access services offered by other participants (Koshutanski et al., 2007). Furthermore, verification is local (between two nodes). A third party cannot track the use of the digital identity (Höller et al., 2022).

Decentralized Identity

Decentralized identity give the user full control over their digital identity. It is fully autonomous and decoupled from any centralized digital identity issuing or managing authority. A centralized authority is often responsible for exposing users to the risk of data breaches, identity misuse, and identity theft. Without this, users can gain sovereignty over their digital identity (Stockburger et al., 2021).

Self-Sovereign Identity

Decentralized identity over a blockchain is referred to as a self-sovereign identity or SSI (Kubach et al., 2020). The SSI uses decentralized, distributed identity management systems to enable the user to exist independent of a service (Mühle, 2018). Here, decentralization refers to the removal of a central identity management authority. Distribution refers to redundancy or the utilization of the exact copy

of the user's identity across all components of the identity management system (Mulaji & Roodt, 2021). In this case, the user holds their digital identity in a secure data store, such as a digital wallet or vault. It is used to prove an identity to legitimate verifiers (Chango, 2022).

Allen's (2016) prescribed guiding principles for SSI can be categorized along the dimensions of security, controllability, and portability (Stockburger et al., 2021). The security dimension requires that the SSI management system enables a persistent digital identity for the user as it minimizes data exposure and protects the rights of the user. The control dimension grants full control over digital identity to a user who must exist independently of the digital identity. Any data of this user must be shared with their consent. The portability dimension implies that the digital identity must be transportable to another system. This ensures that the user retains access and control over their identity and data. In addition, the system must operate and manage identities in a fully transparent manner.

Identity Management

With the proliferation of digital services, digital identity has become the backbone for the provision of most commercial and government services. This includes universal health and education services, targeted social security nets for the vulnerable, and emergency services for those impacted by a natural or man-made calamity (Masiero & Bailur, 2021). Digital identity, especially that managed by a central agency, is prone to leakage and theft.¹ This creates problems in digital identity for service providers and beneficiaries. As a result, organizations and governments should manage the digital identity of their customers and beneficiaries.

Identity management deals with the oversight of all aspects related to digital identity, including creating, using, and destroying records associated with a specific identity (Windley, 2005). Many organizations use identity management to protect data, control authentication, and manage access to digital applications and other resources (see Figure 2). Identity management provides dynamic authorization to grant or restrict access to an organization's resources, share specific pieces of data, authorize sensitive actions, and manage access privileges (i.e., assigning,

Figure 2. Identity Management Services (Digital Identity, 2020)



removing, or suspending user privileges). Hence, security and access management are essential aspects of identity management (Windley, 2005).

Digital identity management occurs through information systems. The following section discusses specific characteristics of information systems that manage a digital identity.

INFORMATION SYSTEMS

Information systems have many exemplary definitions. From the technology standpoint, the system utilizes computer hardware and software, a database, manual procedures, and models for analysis, planning, control, and decision making (Symons, 1991). From a socio-technical view, the information systems field examines more than just the technological system or social system. It investigates the phenomena that emerge when the two interact (Land, 1985). Process view defines it as a work system whose activities are devoted to processing data by capturing, transmitting, storing, retrieving, manipulating, and displaying information (Alter, 2008). They are further divided into centralized, decentralized, and distributed information systems. Centralized systems handle all external requests. Decentralized systems manage the decisive power, which is divided among many. The information systems ecosystem is owned by many (Peng et al., 2021). A distributed system refers to the location and components of the ecosystem (i.e., database, servers). These are also found at different locations (Lehmann, 2003).

Decentralized Ledger Technology

Nakamoto (2008), the mysterious person behind Bitcoin, described blockchain (or distributed/decentralized ledger technology [DLT]) as a distributed network that could be used for maintaining the order of transactions, trust, and transparency. Profound changes were introduced to traditional business processes. Business applications that needed trusted third parties or central solution architecture for verification could now operate in a decentralized manner and with the same level of certainty. In essence, it is a distributed transactional database shared among multiple parties that support decentralization. Advantages of blockchain include:

1. **Decentralized Management:** Data is stored in multiple nodes (computers), improving control of user data. Each node maintains a replicated copy of the same data. The nodes may not know the identity of the other nodes. Nodes are controlled by many entities, some of which may be anonymous (Buthelezi et al., 2021).
2. **Immutable Audit Trail:** Data can be updated but not deleted. Hence, data audit trails are easy to verify. Transactions on a blockchain ledger are immutable; therefore, every party can be confident they are dealing with the same data. One version of the truth is transparent to all parties. Therefore, there are no reconciliations. This enables faster settlement times and lower transaction costs (Raddatz et al., 2021).
3. **Data Provenance:** Data is signed by the source party while updating to the blockchain. This promotes the legitimacy of the records. This meta-data describes where the data of interest originated, who owns the data, and what transformations were done to the data. Data provenance facilitates the integration of data from diverse sources, as well as provides verifiability of the sources (Lacity & Van, 2021).
4. **Robustness/Availability:** Data is stored on a decentralized network. Thus, there is no single institution to rob or hack. Blockchain ensures that all stakeholders have the availability of tamper-proof data from each stage of production (Hossain et al., 2022).
5. **Security/Privacy:** Data is encrypted within the blockchain. It can only be decrypted with the user's private key. There is no practical way to read user data even if the network is infiltrated by a malicious party. The security and privacy of blockchain technology can protect private information and prevent its loss (He et al., 2022).

A blockchain presents various ways to build consensus as it addresses finality for the group of transactions and adds to the next block. These include proof of work (PoW) and proof of stake (PoS). In a PoW, miners in the blockchain network compete by solving mathematical problems computationally. PoS uses network participant stakes in the blockchain to define the next valid block (Pedersen et al., 2019). Emerging areas in blockchain include interoperability (the ability to see and access data across multiple blockchain systems) and scalability (Buthelezi et al., 2021; Lacity & Van, 2021).

DID Management

DID management involves the issue, verification, and use of user-generated, self-owned, globally unique identifiers rooted in decentralized systems. They possess unique characteristics like greater assurance of immutability, censorship resistance, and tamper evasiveness. These attributes, which are critical for any ID system, are intended to provide self-ownership and user control (Microsoft, 2022). Prominent use cases of DID management systems are Zug digital identity (Young & Verhulst, 2018), Credit Union (CU) ledger (Hyperledger Foundation, 2015), British Columbia OrgBook (Columbia, 2019), Traveler Digital Id (KTDI, 2018), NHS Health ID (Alamango, 2021), European Blockchain Services Infrastructure (EBSI), and digital credential on blockchain (BC Diploma, 2018).

We are in the early stages of adopting DID management systems through proof of concepts and pilots within organizations. DID management systems foster user control over digital identity and minimize the quantum of information collected and stored by service providers. This, in turn, reduces the monetization of personal data by companies and data breaches by hackers. By enabling people to own their identity as a sovereign identity, DID management systems can achieve the goal of the United Nations to “provide [by 2030] legal identity for all, including birth registration” (United Nations, 2015).

Building Blocks of Decentralized ID (DID)

1. **Verifiable Credentials:** These digital or paper-based methods provide user identity via birth certificate, educational degree, passport, driving or pilot license, utility bill issued to customer, and power of attorney. The public key, a cryptographically generated key, helps in DID public validation. It is stored on blockchain. The private key is also a cryptographically generated key used to verify the DID of the user. It is specific to the user and stored in the user’s wallet via a mobile application (Vescent, 2019).
2. **DID Trust Parties:** Trust parties in DID include the issuer of the identity, holder of the identity, and verifier of the identities (see Figure 4).
3. **Digital Wallets:** These mobile-based apps store digital identity credentials like the private key of DID. It helps in the identity verification for the users.
4. **Decentralized Identifiers:** This is the address of a public key on a blockchain or decentralized network. It helps locate an agent for the DID (the entity identified by the DID) using W3C DID Working Group recommendations (W3C, 2021). For example, did:example:3k6dg356wdcj5gf2k9.
5. **Blockchain:** Blockchains is a globally distributed database that serves as a source of truth for DID public keys. It is not subject to single points of failure or attacks for decentralized identity management.
6. **Governance Framework:** Standards and unequivocal definition of regulations for varied roles and functions are encompassed in the overarching DID platform framework (W3C, 2021). See Figure 3.

DID Creation

Parties involved in DID creation include blockchain service provider, issuer, users, and blockchain on which public keys are stored (see Figure 4). The service provider selects the blockchain and provides an identity issuer with an application to support creation-related functionalities. In addition,

Figure 3. DID issuance, usage, and governance

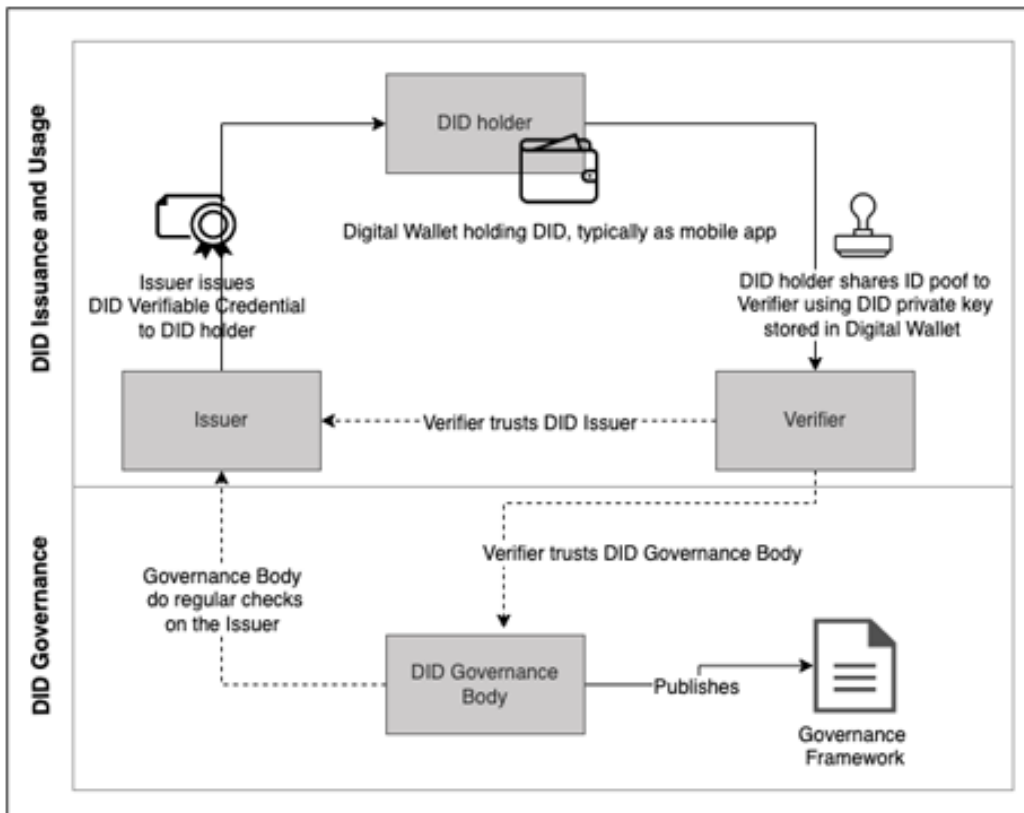
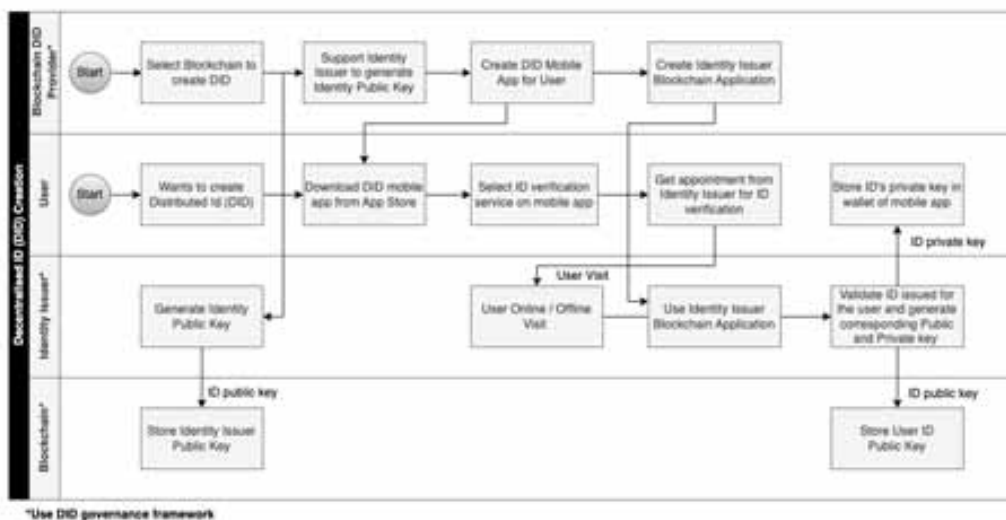


Figure 4. Decentralized Identity Creation Process



it generates their public key to store on the blockchain for validations. They provide mobile apps to users with a digital wallet to store private keys of their identity. Identity issuers store their public key on the blockchain for their identity verification, generate private and public key for the users, support storing identity public key on the blockchain for the users, and support storing their private key to user's mobile app-based wallet. Users install identity mobile apps from the app store and visit identity issuers online/offline for their identity verification. Based on the identity verification, the verifier issues them a public and private key for their identity document. A private key is stored in the user's wallet; a public key is stored on the blockchain (Preukschat & Reed, 2021).

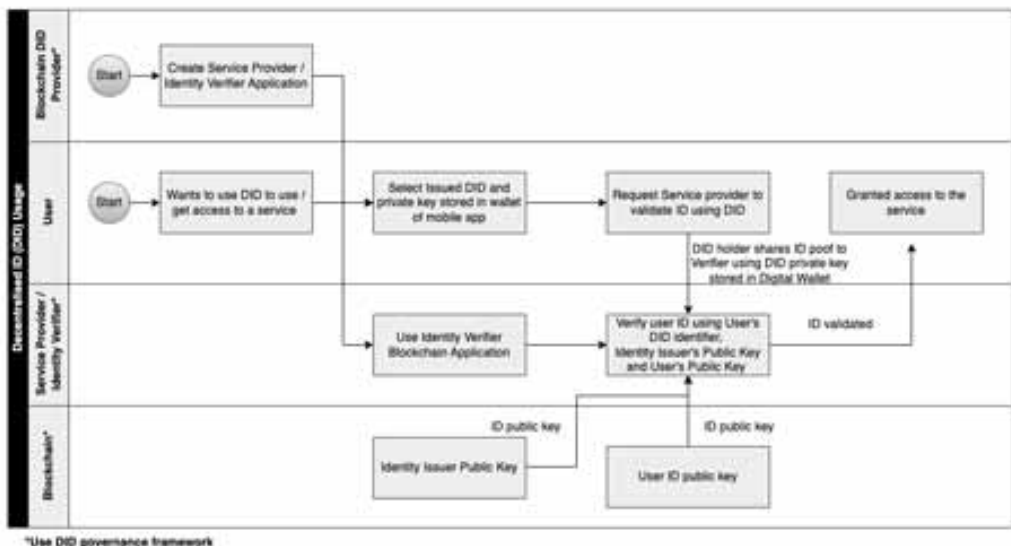
Decentralized Identity (DID) Usage and Associated Benefit

Parties involved in DID usage include: (1) blockchain service providers; (2) users; (3) service providers or verifiers; and (4) the blockchain on which public keys are stored (see Figure 5). Service providers create verification applications via a governance framework. They also provide the same to other service providers or verifiers. Individual users may want access to finance, health, government, or other services using DID-based identity verification.

Consider the example of availing a mortgage loan from a financial institution. In the present scenario, it takes multiple iterations of identity document verifications to prove user identity and credit history. This results in considerable time to release funds to the customer. The primary reason for this high turnaround time is the know your customer (KYC) compliance requirement by financial institutions. Current KYC systems have multiple checks in place and require many manual interventions. Using DID, financial institutions can verify customer identity and KYC requirements via identifiers that share the user's private key (stored in their wallet) and public key (from the blockchain).

The governance framework allows the verifier to trust identity issuers and service providers. The blockchain stores the public keys of identity users and issuers, which can be retrieved by the verifier while ensuring they are not compromised or hacked (Preukschat, 2021). Additionally, DID augments the institution's risk management by ensuring that genuine customers receive loans. This is an important factor in minimizing defaults (Arner, 2019).

Figure 5. Decentralized identity usage process



METHODOLOGY

Research Design

This study uses an exploratory case-based qualitative methodology, guided by Yin (2014) and Eisenhardt (1989). The case study approach is suggested to be appropriate for developing an in-depth understanding of contemporary, real-life phenomena in which limited control can be exerted as the phenomenon is embedded in the context (Yin, 2014). Case study research is also suitable for research in novel areas, especially information systems, where limited research has taken place (Benbasat et al., 1987). Hence, this approach is aligned with the focus of the research, aiming to understand the characteristics and features of the emerging context of DID.

Multiple cases provide a strong foundation to build the theory (Eisenhardt & Graebner, 2007) because they allow generalizability and grounding as compared to a single case study (Davis et al., 2007). Therefore, seven cases were developed with the goal of reaching generalizability. The investigation was guided by thematic analysis, axial coding, and a rigorous process of validation that focused on consensus among fellow researchers. This enabled the current study to achieve precision, reliability, and validity of its findings (Miles & Huberman, 1994).

The case study design followed replication logic. Each case was first individually analyzed. Then, the researchers conducted a cross-case analysis to identify emerging, common theoretical patterns across each case (Yin, 2014). As opposed to pure grounded theory-related work, this research strategy follows Eisenhardt (1989). It does not, therefore, start off with a clean theoretical slate. Instead, it relates the cross-case analysis to existing theoretical constructs when possible and furthers the theoretical linkages by identifying novel relationships between and within the constructs. The back-and-forth feature in the building of the qualitative theory is apparent in the research design.

CASE SELECTION AND DATA COLLECTION

The empirical foundation of this research includes seven case studies of leading decentralized identity management platforms that were developed for this research using secondary data sources. The researchers contact experts in the fields of privacy, security, and DID to help in the identification of DID platforms that possessed varied characteristics and were leading the development of DID design. Guided by expert advice, they followed purposive sampling to select cases so they could unravel attributes that were essential to understanding decentralized identity management (Yin, 2014). The researchers knew that the cases must enable them to achieve saturation; therefore, they did not finalize the number of the cases at the beginning of the work. Instead, they were guided by emergent patterns. By the time the researchers documented and analyzed the seventh case, they could sense theoretical saturation in the form of no new insights and a high level of replication. The confidence in the findings allowed the researchers to stop looking for new data points. Finally, they closed with seven polar DID management platforms that possessed diversity in underlying operating rules, attributes, and use cases.

Data collection was challenging. The idea of DID was rather novel; therefore, most applications were experimental or proof of concept (PoC) in nature. Based on the advice of experts, the researchers began searching for documentation related to the projects of importance. They proceeded to dig deeper on projects in which they could seek rich data in the form of white papers, details of experiments, and general testimonials. For seeking triangulation, the researchers regularly sought out newspaper articles and specialized blogs on blockchain technologies to reaffirm the data. The presence of use-case across multiple platforms, blogs, and forums was used as a proxy for veracity of the data.

DATA ANALYSIS

One of the researchers compiled separate descriptive case studies on the seven DID management platforms based on the study's data collection. These were systematically and iteratively analyzed by the first author. The data was continuously compared with emerging categories. The extant literature guided this comparison (Miles & Huberman, 1994). The focus was on identifying patterns of similarity and variance among the cases with respect to the salient characteristics of DID management platforms.

New themes were added as the first researcher iteratively mapped the characteristics observed through case analysis onto prespecified conceptual categories derived from extant literature (Yin, 2014). Some identified lower-level themes were regrouped into more appropriate concepts (Cassell & Symon, 1994). The researchers met every other day to reanalyze and discuss each case as categories emerged. The meetings focused on comparing DID platforms to identify concepts that can explain their salient characteristics. Disagreements with respect to the concepts being derived and categorizations being made were resolved in these meetings. The researchers also met with experts in five meetings to discuss privacy, security, and DID. They vetted and critiqued emergent categories and their relationships. This ensured generalizability and strengthened explanations (Miles & Huberman, 1994).

The next section presents seven caselets for each of the seven DID platforms explored in this research. The caselets are purposefully written to describe the salient characteristics of the DID platforms. They will help in building a conceptual framework for categorizing DID platforms.

LEADING DID PLATFORMS

uPort

uPort is an open source, self-sovereign, distributed identity management system (Naik & Jenkins, 2020). It works on Ethereum as a set of smart contracts (Szabo, 1997; Wood, G., 2014). uPort's process of identity creation and verification is driven by its mobile app. Public DIDs, which are unique and immutable IDs for each user, are stored on a blockchain without confidential data. Personal data is stored in the digital wallet associated with the private key of the user. Users control the identity. They also have the option to share full credentials, partial credentials, and zero-knowledge proofs, as well as a period for which the identity is to be maintained. The recovery of credentials is based on a social recovery method. Friends and family play the role of recovery delegates. The uPort scalability is a function of the underlying Ethereum blockchain.

European Blockchain Services Infrastructure (EBSI)

The European Blockchain Services Infrastructure (EBSI, 2022) is a peer-to-peer network of interconnected nodes. It runs a blockchain-based services infrastructure with the 27 EU countries, Norway, Liechtenstein, and the European Commission, which will run at least one node of the blockchain. The transactions are validated by approved accounts. It aims to put blockchain technology at the service of public administrations to verify information and create trustworthy services. It is an open source blockchain developed through Ethereum and Hyperledger (Hyperledger Foundation, 2015; Wood, 2014). Interfaces of the core services can support business applications. Use cases are available for managing user self-identity and educational diplomas.

Everest

Everest Foundation (<https://everestfoundation.net>) is a non-profit that is governed as a decentralized autonomous organization (DAO). It aims to give every human on the planet a biometric digital identity and wallet. These wallets will be prefunded with an ID token so basic services on the blockchain can be utilized by the users. The system utilizes the Everest blockchain and its protocols to implement DID. The system, which is built with deduplication features, gives users the choice to share zero knowledge proof of their specific information.

Hedera and Earth ID

Hedera is described as a third-generation public ledger (Baird et al., 2019). Unlike other mainstream blockchains, Hedera utilizes a proof-of-stake public network powered by hash graph consensus. It is owned and governed by a global consortium of public and private entities. It claims to be faster and cheaper than alternates. It is also carbon negative. HBAR is its native crypto currency.

EarthID (2018) is a self-sovereign identity and decentralized identity management platform. It utilizes the Hedera blockchain. Biometric information is used in the form of facial recognition. Liveness detection protects against spoofing. It does not use a password. There is an implementation of zero knowledge proof technology. Services provided by Earth ID are compliant with GDPR and PDPB (Prasad & Menon, 2020; Voigt & Von dem Bussche, 2017). They are available across 200 countries.

Hyperledger Indy and Sovrin

The original source code for Hyperledger Indy (Aggarwal & Kumar, 2021) was developed by Evernym (2012), which was donated to Sovrin Foundation (<https://sovrin.org/>). It formed the basis for Hyperledger Indy, which was supported by Linux Foundation (<https://www.linuxfoundation.org/>). The Hyperledger Indy Node project and Hyperledger Indy Agent project form the base for stewards of the Sovrin network and the Sovrin Trust Framework. Like other self-sovereign distributed identity products, decentralized identifiers or DIDs, together with associated public keys and Sovrin protocol, are the primary components of Indy. Sovrin registry and protocol are responsible for the creation, verification, and revocation of related activities. The Sovrin framework supports both private and public DIDs, enabling off-ledger peer-to-peer encrypted communication between any two agent endpoints. The Sovrin registry enables an interoperable exchange of credentials by allowing the storage of schema definition and credential definitions. The same schemas can be used by multiple credential issuers. At the same time, credential definitions can draw from multiple schemas. The Sovrin revocation of credential is based on a decentralized and asynchronous revocation registry process. The revocation registry utilizes zero knowledge proof of revocation to establish validity. The same process is utilized for agent authorization policies. As a result of the above framework, Hyperledger Indy and Sovrin are among the most famous DID implementations across the globe.

Microsoft Entra Verified ID

This is based on a decentralized blockchain electronic ledger approach. It gives control to individuals or organizations on the submission of their identity information, including the ability to revoke it (Microsoft, 2022). This open standard DID was developed while working with the Decentralized Identity Foundation (<https://identity.foundation/>), W3C Credentials Community (W3C, 2021), and the wider identity community. It uses a W3C DIDs standard and is developed via an identity overlay network (ION) blockchain (<https://identity.foundation/ion/>). The Blockchain Layer 2 open, permissionless network is based on the purely deterministic side tree protocol. This requires no special tokens, trusted validators, or other consensus mechanisms due to a linear progression of Bitcoin's time chain. Launched in August 2022, it helps to customize and configure verifiable credentials for individuals through a pre-built template with user rules and design files. It promises to reduce organizational risk by simplifying the identity audit process, empowering users to own and control their digital identity for improved privacy. It helps in verifying and issuing user credentials, education status, certifications, or any unique identity attributes using Azure Active Directory (<https://azure.microsoft.com/en-in/services/active-directory/>).

Polygon

Polygon (<https://polygon.technology/>) is a decentralized Ethereum-based (Wood, G., 2014) interoperable blockchain platform that enables developers to build scalable user-friendly distributed apps with low transaction fees. It is a self-sovereign and decentralized identity management system

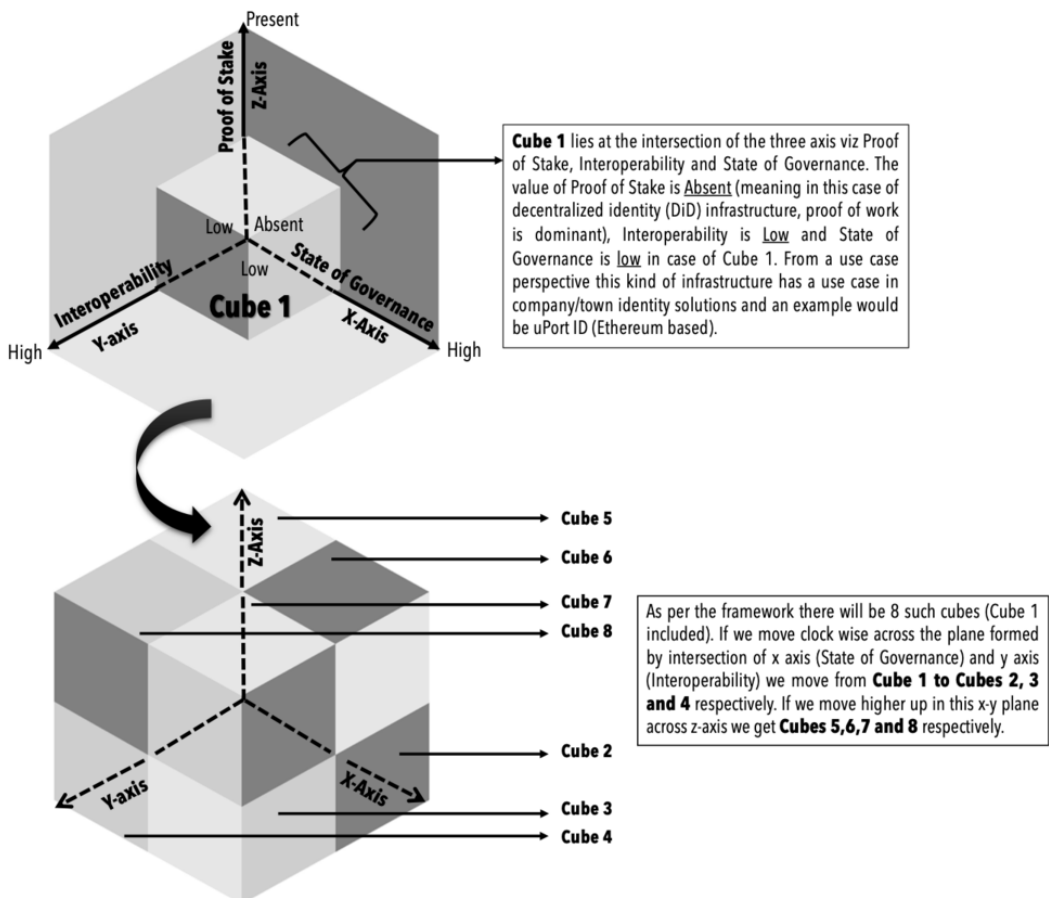
developed by Polygon ID. Zero knowledge protocols have been implemented to secure user data and identity. Smart contracts can verify identity via the system. It is expected to fully launch by the end of 2022.

DID Cross Platform Comparison

It is necessary to anchor a comparison of DID platforms by a defining criterion. The researchers based their work on a critical analysis of the seven platforms in this study, thematic content analysis, and discussion with leading experts in the domain. They identified block creation (proof of stake, proof of work), state of governance (W3C Standards and unequivocal definition of regulations for varied roles and functions encompassed in the overarching DID platform framework), and interoperability (ability of two DID platforms to exchange information seamlessly) as the defining criteria for building a taxonomy for DID platforms. This enabled the researchers to capture fundamental nuances and provide sufficient discriminatory power to represent most existing DID platforms comprehensively. These criteria have been envisaged as orthogonal to each other, with two possible states on either axis (see Figure 6).

The three axes form a larger cube, creating eight smaller cubes. The smaller cubes have specific values for each of the three dimensions: (1) proof of stake (two levels, present or absent); (2) state of governance (two levels, high or low); and (3) interoperability (two levels, high or low). An example is

Figure 6. DID Comparison Cube Framework



used to demonstrate how levels of the axes converge into a specific cube. Cube 1 is positioned at the intersection of the three axes. The value of proof of stake is absent (in the case of DID infrastructure, proof of work is dominant). Interoperability is low and state of governance is low in Cube 1. From a use case perspective, this kind of infrastructure has a use case in company/town identity solutions. An example would be uPort ID (Ethereum based). A close review of Figure 6 shows that a clockwise movement across the plane formed by the intersection of the x axis (state of governance) and y axis (interoperability) will move from Cube 1 to Cubes 2, 3, and 4, respectively. Moving higher up the x-y plane across the z-axis results in Cubes 5, 6, 7, and 8, respectively. Details of these eight cubes, along with specific details of elements (i.e., level of the axes, use case, and available DID framework in the international market for each of the cubes) is presented in Table 1.

Next, the study presents an overview of zones in the primary cube. These are identified as sub-cubes. The details are summarized in Table 1. Further, the cube framework identifies a minimal infrastructure or necessary and sufficient identity infrastructure required to host a specific kind of application. The exposition of infrastructure to application mapping may be looked upon from the lens of the application of technology-task fit framework.

Cube 1: This cube represents an absence of proof of stake, minimal governance, and low-to-no interoperability between peer blockchain types. Absence of proof of stake translates into lower total number of transactions per unit time. This will impact scalability negatively, making the entire application energy intensive. Absence of governance framework renders the system of limited usage for richer credential exchange or evaluation. Lastly, absence of interoperability negatively impacts the diversity of end-user applications and scalability, as well as forces long-term commitment from end users in terms of choice of blockchain infrastructure. Overall, this

Table 1. DID Comparison Cube Enabled Classification of DID Frameworks and Use Cases

Description of Axes	State of Governance (X-Axis)	Proof of Stake (Z-Axis)	Interoperability (Y-Axis)	Use Case	DID Framework
Cube 1	Low	Absent	Low	Company/Town Identity Solutions	uPort ID (Ethereum)
Cube 2	High	Absent	Low	BC University Diploma	European Blockchain Services Infrastructure (EBSI)
Cube 3	High	Absent	High	Metaverse	X
Cube 4	Low	Absent	High	Digital Physical Mashup	Polygon ID
Cube 5	Low	Present	Low	Virtual World, Loyalty Card	Earth ID (Hedera)
Cube 6	High	Present	Low	National Identity Solution, CU Credit Union, NHS Healthcare	Sovrin + Indy (Hyperledger), EverID (Everest), Microsoft Entra Verified ID
Cube 7	High	Present	High	Financial (KYC) and Critical Identity Solutions	X
Cube 8	Low	Present	High	Multi-mode Transportation	X

cube fits applications like city/state identity cards because they work on a smaller scale and do not require a defined governance framework (the only objective is ordinary secure authentication).

Cube 2: This cube improves on Cube 1 by bringing in a comprehensive governance framework and keeping the other two dimensions unchanged. The presence of a rich governance framework is associated with defined roles and responsibilities, as well as a hierarchy of stakeholders that can establish credibility and a working network to approve or evaluate a set of standard documents. This cube fits with the requirements of hosting college degrees or diplomas, as well as other formal documents, that may require regular, secure access.

Cube 3: This cube adds a layer of interoperability over Cube 2 (in addition to an existing governance framework). Interoperability enables a wider reach and easier exchange of tokens (for example, between gamers and niche e-commerce portals). The existence of a governance framework allows for the implementation of rules and regulations specific to certain virtual environments not limited to transactions. This cube fits with the requirements of authentication and control across various forms of metaverse.

Cube 4: This cube offers only a layer of interoperability with no governance framework and no proof of stake validation. While interoperability enables a wider reach, as explained in Cube 3, the lack of governance and absence of proof of stake makes the platform proprietary in nature. This reduces the scalability in terms of transactions per unit time. The interoperability in such cases is likely to be utilized for pure exchange of tokens. However, it could enable multiple end use applications that may not require a high level of credibility, such as the uploading of sensitive documents. This cube fits with the requirements of simple (but secure) transactions on a limited scale.

Cube 5: Cube5 offers a proof of stake as the validation mechanism. There is no benefit of either interoperability or a governance framework. Cube 5 is suited for a sustainable high rate of transactions per unit time. However, lack of interoperability reduces the reach and diversity. The lack of governance makes credibility dependent on the players who are participating as stakeholders in the proof of stake system. It is close to a centralized clearing house that operates in a blockchain environment. It can offer a suitable infrastructure for loyalty cards for a brand or a large retail store with multiple branches.

Cube 6: Cube 6 offers a solid governance framework and presence of proof of stake. It does not offer interoperability. A good governance framework ensures higher credibility. This is further bolstered by the possibility of a high transaction rate per time, making the system amenable for higher loads from varied applications with the caveat that they are hosted on a single chain-based infrastructure. This cube represents the most market-ready infrastructure for applications like national- or health-based identity cards.

Cube 7: This cube offers an ideal scenario with all three dimensions (governance, proof of stake, and interoperability). It adds to Cube 6 in terms of interoperability, offering the potential for diverse applications and widespread use. It, thereby, overcomes the need for implementation on a single chain. The Cube 7 infrastructure is suitable for very critical identity use cases. However, it can also be utilized for other services.

Cube 8: Cube 8 represents the presence of dimensions of interoperability and proof of stake. This cube offers a suitable identity solution for pre-filled cash cards or specialized cards for access to varied infrastructure across geographies, such as metro railways or multi-mode transportation access cards.

The study presented eight sub-cubes; however, a higher cube or cube with higher attributes (e.g., Cube 7 has all three attributes as compared to Cube 6 or Cube 8) can be used for the same application or purpose as a cube with lesser attributes. It may be interesting to note that the first four cubes represent a pure distributed application. The last four are proof of stake-based, representing semi-distributed solutions.

CONCLUSION

Extant academic and practitioner literature is explored to understand and differentiate between centralized and decentralized identity management. Seven leading platforms with DID services are identified and evaluated via purposive sampling. A taxonomy of DID services is created, which follows the researchers' methodology. The seven platforms are categorized on the taxonomy with three orthogonal criteria (represented as the three axes of a cube): (1) state of governance; (2) proof of stake; and (3) interoperability. A good state of governance creates credible, robust deployments and supports a community of developers and users to augment the use of the DID framework. A proof of stake (or a similar approach for enabling new block creation) can mitigate the time needed to create a new block, introducing energy efficiency into the system. Interoperability enables a disjointed (but compatible) DID infrastructure to exchange information. The researchers utilize their taxonomy to map the three attributes to possible end-user requirements. This establishes a baseline infrastructure for varied contexts. In the process, the study identifies and establishes Cube 6 as the most market-ready and contemporary implementation in the field.

This work offers unique contributions to both theory and practice. To the authors' knowledge, this study is one of a few scholarly works that presents existing DID use cases and in-depth architectural and procedural overviews of distributed identity management. In addition, it establishes an operating taxonomy. From a theoretical perspective, this work represents early theory-building efforts that align identity and distributed logic to achieve a value-adding service.

This work also presents obstacles in the adoption of a blockchain-based infrastructure, as well as a framework for overcoming challenges. This research can be utilized by academicians as a roadmap for future research in the field of DID. Still, many questions remain unanswered. For example, what are the characteristics of a global DID? What are the potential pitfalls of DID compared to traditional centralized ID? Does DID lead to truly decentralized ID if driven by POS? How does it help the end-user? Is blockchain the only core infrastructure option available to implement DID (or are there other alternatives)? How will DID work in areas with low or no network coverage? How will it support users who do not have smartphone access? How will DID governance evolve? Would governments enact applicable laws? How will layer 2 blockchain help in growth of DID?

Practitioners are often given ways to conceptualize and identify the right infrastructure for identity solutions. This study also highlights a vital characteristic that is missing from the existing DID platforms. It emerged that "interoperability," which is critical for financial services, was a low-ranking criterion on most existing platforms. The study, therefore, claims that current platforms and services are operating within silos, and future DID platforms should focus on being interoperable among themselves and across institutions. Interoperability will ensure that a single ID can be used across government services and financial services, providing users with a significant incentive to create a DID using such a platform. Cube 7 and Cube 8 point in the direction of what could be expected from the DID infrastructure industry in the future.

This work, like any other scientific endeavor, suffers from several limitations. First, it is usually advised that primary data be the basis for case-based research. The researchers have tried to capture the nuances of the context, especially given the novel technology scenario and constraints of travel imposed by limited funding within the research team. Second, regarding the nature of the research team's training in the information science domain, this analysis and presentation may suffer from inherent bias. The researchers have tried to mitigate the effect by bringing in a wider, more diverse perspective through researchers from other areas. However, it is difficult to establish that such a bias does not exist. Third, given the changing nature of technology, certain aspects of the analysis may be rendered obsolete. Irrespective of constraints, the analysis represents the next step in DID, as well as the adoption of a blockchain infrastructure for business across the world.

REFERENCES

- W3C. (2021). *DID specification registries*. <https://w3c.github.io/did-spec-registries/>
- Aggarwal, S., & Kumar, N. (2021). Hyperledger. *Advances in Computers*, 121, 323–343. doi:10.1016/bs.adcom.2020.08.016
- Akerlof, G. A., & Kranton, R. E. (2000). Economics and identity. *The Quarterly Journal of Economics*, 115(3), 715–753. doi:10.1162/003355300554881
- Alamango, Y. (2021). *Healthcare decentralized identity case study*. <https://www.techuk.org/resource/healthcare-decentralised-identity-case-study-nhsx.html>
- Allen, C. (2016). The path to self-sovereign identity. *Life with Alacrity*. <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>
- Allison, A., Currall, J., Moss, M., & Stuart, S. (2005). Digital identity matters. *Journal of the American Society for Information Science and Technology*, 56(4), 364–372. doi:10.1002/asi.20112
- Alter, S. (2008). Defining information systems as work systems: Implications for the IS field. *European Journal of Information Systems*, 17(5), 448–469. doi:10.1057/ejis.2008.37
- Andrews, L. (2012). Facebook is using you. *The New York Times*. <https://www.nytimes.com/2012/02/05/opinion/sunday/facebook-is-using-you.html>
- Annas, G. J. (2003). HIPAA regulations: A new era of medical-record privacy? *The New England Journal of Medicine*, 348(15), 1486–1490. doi:10.1056/NEJMLim035027 PMID:12686707
- Arner, D. W., Zetsche, D. A., Buckley, R. P., & Barberis, J. N. (2019). The identity challenge in finance: From analogue identity to digitized identification to digital KYC utilities. *European Business Organization Law Review*, 20(1), 55–80. doi:10.1007/s40804-019-00135-1
- Back, A. (2002). *The Hashcash proof-of-work function*. <http://www.hashcash.org/papers/draft-hashcash.txt>
- Baird, L. H., Harmon, M., & Madsen, P. (2019). *Hedera: A public hashgraph network & governing council [whitepaper]*. <https://www.scribd.com/document/489094536/Hedera-A-Public-Hashgraph-Network-Governing-Council-Whitepaper>
- BarnardB. (2022, October 30). *Verified*. <https://policyexchange.org.uk/wp-content/uploads/2020/10/Verified.pdf>
- Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The case research strategy in studies of information systems. *Management Information Systems Quarterly*, 11(3), 369–386. doi:10.2307/248684
- Bose, I., & Leung, A. C. M. (2019). Adoption of identity theft countermeasures and its short-and long-term impact on firm value. *MIS Quarterly*, 43(1).
- Buthlezi, B. E., Ndayizigamiye, P., Twinomurinzi, H., & Dube, S. M. (2021). A systematic review of the adoption of blockchain for supply chain processes. *Journal of Global Information Management*, 30(8), 1–32. doi:10.4018/JGIM.297625
- Cameron, K. (2005). The laws of identity. *Microsoft Corp*, 12, 8–11.
- Camp, J. L. (2004). Digital identity. *IEEE Technology and Society Magazine*, 23(3), 34–41. doi:10.1109/MTAS.2004.1337889
- Carter, M., & Grover, V. (2015). Me, myself, and I(T): Conceptualizing information technology identity and its implications. *Management Information Systems Quarterly*, 39(4), 931–958. doi:10.25300/MISQ/2015/39.4.9
- Casino, F. D., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81. doi:10.1016/j.tele.2018.11.006
- Cassell, C., & Symon, G. (1994). *Qualitative methods in organizational research: A practical guide*. Sage Publications.
- Chadwick, D. W. (2009). Federated identity management. *Foundations of Security Analysis and Design*, 96–120.

- Chango, M. (2022). *Building a credential exchange infrastructure for digital identity: A sociohistorical perspective and policy guidelines*. Blockchain.
- Columbia, B. (2019). *Use case spotlight: The Government of British Columbia uses the Sovrin Network to take strides towards a fully digital economy*. <https://sovrin.org/use-case-spotlight-the-government-of-british-columbia-uses-the-sovrin-network-to-take-strides-towards-a-fully-digital-economy/>
- Cruz-Jesus, F., Oliveira, T., & Bacao, F. (2018). The global digital divide: Evidence and drivers. *Journal of Global Information Management*, 26(2), 1–26. doi:10.4018/JGIM.2018040101
- Cuijpers, C. M. (2014). *eIDAS as a guideline for the development of a pan European eID framework in FutureID*. Academic Press.
- DaiW. (1998). *B-Money*. <http://www.weidai.com/bmoney.txt>
- Davis, J. P., Eisenhardt, K. M., & Bingham, C. B. (2007). Developing theory through simulation methods. *Academy of Management Review*, 32(2), 480–499. doi:10.5465/amr.2007.24351453
- Davis, M. (2020). *Web 3.0 Manifesto*. https://project10x.com/bio_downloads/web3_manifesto_2009.pdf
- De Clercq, J. (2002). Infrastructure security. In *International Conference* (pp. 40-58). InfraSec.
- Digital Identity. (2020, Nov 20). *A billion people have no legal identity - but a new app plans to change that*. <https://www.weforum.org/agenda/2020/11/legal-identity-id-app-aid-tech/>
- Diploma, B. C. (2018). *Digital credentials on the blockchain*. <https://www.bcdiploma.com/en>
- Earth, I. D. (2018). *Frictionless, secure, and trustworthy*. <https://www.myeearth.id/>
- Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, 14(4), 532–550. doi:10.2307/258557
- Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, 50(1), 25–32. doi:10.5465/amj.2007.24160888
- European Blockchain Services Infrastructure (EBSI). (2022, August 17). <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home>
- Evernym. (2012). *Evernym: The world's leading platform for verifiable credentials*. <https://www.evernym.com/>
- Faber, B. M. (2019). BPDIMS: A blockchain-based personal data and identity management system. *Proceedings of the 52nd Hawaii International Conference on System Sciences*. doi:10.24251/HICSS.2019.821
- Fair, L. (2019). *\$575 million Equifax settlement illustrates security basics for your business*. Federal Trade Commission. <https://www.ftc.gov/business-guidance/blog/2019/07/575-million-equifax-settlement-illustrates-security-basics-your-business>
- Gavrilova, M. L., Anzum, F., & Hossain Bari, A. S. M. (2022). A multifaceted role of biometrics in online security, privacy, and trustworthy decision making. In K. Daimi, G. Francia III, & L. H. Encinas (Eds.), *Breakthroughs in digital biometrics and forensics*. Springer. doi:10.1007/978-3-031-10706-1_14
- Grassi, P., Garcia, M., & Fenton, J. (2020). Digital identity guidelines (No. NIST Special Publication (SP) 800-63-3). National Institute of Standards and Technology.
- Gupta, P. S. (2015). Phoneypot: Data-driven understanding of telephony threats. *NDSS*, 107, 108.
- Hammack, P. L. (2008). Narrative and the cultural psychology of identity. *Personality and Social Psychology Review*, 12(3), 222–247. doi:10.1177/1088868308316892 PMID:18469303
- Harvey, C. R., Moorman, C., & Toledo, M. (2018). How blockchain can help marketers build better relationships with their customers. *Harvard Business Review*, 9, 6–13.
- He, W., Zhang, J. Z., Wu, H., Li, W., & Shetty, S. (2022). A unified health information system framework for connecting data, people, devices, and systems. *Journal of Global Information Management*, 30(11), 1–19. doi:10.4018/JGIM.305239

- Höller, T., Roland, M., & Mayrhofer, R. (2022). Evaluating dynamic tor onion services for privacy preserving distributed digital identity systems. *Journal of Cyber Security and Mobility*, 141–164.
- Hossain, C. A., Mohamed, M. A., Zishan, M., Rahman, S., Ahasan, R., & Sharun, S. M. (2022). Enhancing the security of e-health services in Bangladesh using blockchain technology. *International Journal of Information Technology*, 14(3), 1179–1185. doi:10.1007/s41870-021-00821-9 PMID:35128304
- Hughes, L. D., Dwivedi, Y. K., Misra, S. K., Rana, N. P., Raghavan, V., & Akella, V. (2019). Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda. *International Journal of Information Management*, 49, 114–129. doi:10.1016/j.ijinfomgt.2019.02.005
- Hyperledger Foundation. (2015). *Case study: How CULedger protects credit unions against fraud with Hyperledger Indy*. <https://www.hyperledger.org/learn/publications/culedger-case-study>
- JacksonD. (1996). *E-Gold*. <https://cs.stanford.edu/people/eroberts/cs201/projects/2010-11/Bitcoins/e-gold.html>
- Juma'h, A. H., & Alnsour, Y. (2021). How do investors perceive the materiality of data security incidents? *Journal of Global Information Management*, 29(6), 1–32. doi:10.4018/JGIM.20211101.0a4
- Karwatzki, S., Trenz, M., Tuunainen, V. K., & Veit, D. (2017). Adverse consequences of access to individuals' information: An analysis of perceptions and the scope of organizational influence. *European Journal of Information Systems*, 26(6), 688–715. doi:10.1057/s41303-017-0064-z
- Koshutanski, H., Ion, M., & Telesca, L. (2007, October). Distributed identity management model for digital ecosystems. In *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)* (pp. 132–138). IEEE. doi:10.1109/SECUREWARE.2007.4385323
- Kruk, S. R., Grzonkowski, S., Gzella, A., Woroniecki, T., & Choi, H. C. (2006, September). D-FOAF: Distributed identity management with access rights delegation. In *Asian Semantic Web Conference* (pp. 140–154). Springer. doi:10.1007/11836025_15
- KTDI. (2018). *Unlocking the potential of digital identity for secure and seamless travel*. <https://ktidi.org/>
- Kubach, M., Schunck, C. H., Sellung, R., & Roßnagel, H. (2020). Self-sovereign and decentralized identity as the future of identity management? *Open Identity Summit 2020*.
- Lacity, M. C., & Van Hoek, R. (2021). How Walmart Canada used blockchain technology to reimagine freight invoice processing. *MIS Quarterly Executive*, 20(3), 219–233. doi:10.17705/2msqe.00050
- Land, F. (1985). Is an information theory enough? *The Computer Journal*, 28(3), 211–215. doi:10.1093/comjnl/28.3.211
- Lawler, S. (2015). *Identity: sociological perspectives*. John Wiley & Sons.
- Lee, J., & Geistfeld, L. V. (1999). Elderly consumers' receptiveness to telemarketing fraud. *Journal of Public Policy & Marketing*, 18(2), 208–217. doi:10.1177/074391569901800207
- Lehmann, H. (2003). An object-oriented architecture model for international information systems? *Journal of Global Information Management*, 11(3), 1–18. doi:10.4018/jgim.2003070101
- Lesavre, L. V. (2019). *A taxonomic approach to understanding emerging blockchain identity management systems*. <https://arxiv.org/pdf/1908.00929.pdf>
- Litan, A. (2022). *Gartner Hype Cycle for Blockchain and Web3*. <https://blogs.gartner.com/avivah-litan/2022/07/22/gartner-hype-cycle-for-blockchain-and-web3-2022/>
- Lutz, W. S., Sanderson, W., & Scherbov, S. (2008). The coming acceleration of global population ageing. *Nature*, 451(7179), 716–719. doi:10.1038/nature06516 PMID:18204438
- Madon, S., & Schoemaker, E. (2021). Digital identity as a platform for improving refugee management. *Information Systems Journal*, 31(6), 929–953. doi:10.1111/isj.12353
- Masiero, S., & Bailur, S. (2021). Digital identity for development: The quest for justice and a research agenda. *Information Technology for Development*, 27(1), 1–12. doi:10.1080/02681102.2021.1859669

- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359. doi:10.1287/isre.13.3.334.81
- Microsoft. (2022, August 17). *Introduction to Microsoft Entra Verified ID*. <https://docs.microsoft.com/en-IN/azure/active-directory/verifiable-credentials/decentralized-identifier-overview#why-we-need-decentralized-identity>
- Mikula, T., & Jacobsen, R. H. (2018). Identity and access management with blockchain in electronic healthcare records. In *21st Euromicro conference on digital system design (DSD)* (pp. 699–706). IEEE. doi:10.1109/DSD.2018.00008
- Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage Publications.
- Morgan, S. (2020, Nov 13). Cybercrime to cost the world \$10.5 trillion annually by 2025. *Cybercrime Magazine*. <https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/>
- Mühle, A. G., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30, 80–86. doi:10.1016/j.cosrev.2018.10.002
- Mulaji, S. S., & Roodt, S. S. (2021). The practicality of adopting blockchain-based distributed identity management in organizations: A meta-synthesis. *Security and Communication Networks*, 2021, 1–19. doi:10.1155/2021/9910078
- Naik, N., & Jenkins, P. (2020). uPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain. In *IEEE International Symposium on Systems Engineering* (pp. 1–7). IEEE. doi:10.1109/ISSE49799.2020.9272223
- Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. <https://bitcoin.org/bitcoin.pdf>
- Ngwenyama, O., Henriksen, H. Z., & Hardt, D. (2021). Public management challenges in the digital risk society: A critical analysis of the public debate on implementation of the Danish NemID. *European Journal of Information Systems*, 1–19. doi:10.1080/0960085X.2021.1907234
- Niehaves, B., & Plattfaut, R. (2014). Internet adoption by the elderly: Employing IS technology acceptance theories for understanding the age-related digital divide. *European Journal of Information Systems*, 23(6), 708–726. doi:10.1057/ejis.2013.19
- Nyst, C., Makin, P., Pannifer, S., & Whitley, E. (2016). *Digital identity: Issue analysis: executive summary*. Guildford.
- Ometov, A. B., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-factor authentication: A survey. *Cryptography*, 2(1), 1. doi:10.3390/cryptography2010001
- Padhi, S. (Creator). (2020). *Jamtara – Sabka Number Aeyga* [series]. Netflix. Retrieved from <https://www.netflix.com/title/81183491>
- Pedersen, A. B., Risius, M., & Beck, R. (2019). A ten-step decision path to determine when to use blockchain technologies. *MIS Quarterly Executive*, 18(2), 99–115. doi:10.17705/2msqe.00010
- Peng, G., Chen, S., Chen, X., & Liu, C. (2021). An investigation to the Industry 4.0 Readiness of Manufacturing Enterprises: The ongoing problems of information systems strategic misalignment. *Journal of Global Information Management*, 29(6), 1–20. doi:10.4018/JGIM.291515
- Prasad, M. D., & Menon, S. C. (2020). The Personal Data Protection Bill, 2018: India's regulatory journey towards a comprehensive data protection law. *International Journal of Law and Information Technology*, 28(1), 1–19. doi:10.1093/ijlit/etaa003
- Preukschat, A., & Reed, D. (2021). *Self-sovereign identity*. Manning Publications.
- Quine, W. V. (1950). Identity, ostension, and hypostasis. *The Journal of Philosophy*, 47(22), 621–633. doi:10.2307/2021795
- Raddatz, N., Coyne, J., Menard, P., & Crossler, R. E. (2021). Becoming a blockchain user: Understanding consumers' benefits realization to use blockchain-based applications. *European Journal of Information Systems*, 1–28. doi:10.1080/0960085X.2021.1944823

- Rannenbergh, K. R. (2009). *The future of identity in the information society: Challenges and opportunities*. Springer. doi:10.1007/978-3-642-01820-6
- Reaves, B. B., Bowers, J., Scaife, N., Bates, A., Bhartiya, A., Traynor, P., & Butler, K. R. B. (2017). Mo (bile) money, mo (bile) problems: Analysis of branchless banking applications. *ACM Transactions on Privacy and Security*, 20(3), 1–31. doi:10.1145/3092368
- Ricoeur, P. (1992). *Oneself as another*. University of Chicago Press.
- Rudman, R., & Bruwer, R. (2016). Defining Web 3.0: Opportunities and challenges. *The Electronic Library*, 34(1), 132–154. doi:10.1108/EL-08-2014-0140
- Security Magazine. (2017, Nov 6). *Average business user has 191 passwords*. <https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords>
- Seltsikas, P., & O'Keefe, R. M. (2010). Expectations and outcomes in electronic identity management: The role of trust and public value. *European Journal of Information Systems*, 19(1), 93–103. doi:10.1057/ejis.2009.51
- Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems*, 32(2), 314–341. doi:10.1080/07421222.2015.1063315
- Soltani, R., Nguyen, U. T., & An, A. (2021). A survey of self-sovereign identity ecosystem. *Security and Communication Networks*, 2021, 1–26. doi:10.1155/2021/8873429
- Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. *Blockchain: Research and Applications*, 2(2), 100014. doi:10.1016/j.bcr.2021.100014
- Symons, V. J. (1991). Impacts of information systems: Four perspectives. *Information and Software Technology*, 33(3), 181–190. doi:10.1016/0950-5849(91)90132-U
- Szabo, N. (1997). *Formalizing and securing relationships on public networks*. <https://firstmonday.org/ojs/index.php/fm/article/download/548/469>
- Thomson, I. (2014). South Korea faces \$1bn bill after hackers raid national ID database. *The Register*. https://www.theregister.com/2014/10/14/south_korea_national_identity_system_hacked/
- United Nations. (2015). *Transforming our world: The 2030 agenda for sustainable development*. Department of Economic and Social Affairs.
- Van Fenema, P. C., & Keers, B. M. (2018). Interorganizational performance management: A co-evolutionary model. *International Journal of Management Reviews*, 20(3), 772–799. doi:10.1111/ijmr.12180
- Vescent, H. Y. (2019). *A comprehensive guide to self sovereign identity*. The Purple Tornado.
- Voigt, P., & Von dem Bussche, A. (2017). *The EU general data protection regulation (gdpr). A practical guide* (1st ed.). Springer International Publishing. doi:10.1007/978-3-319-57959-7
- Wang, F., Shan, G. B., Chen, Y., Zheng, X., Wang, H., Mingwei, S., & Haihua, L. (2020). Identity authentication security management in mobile payment systems. *Journal of Global Information Management*, 28(1), 189–203. doi:10.4018/JGIM.2020010110
- Wang, H. (2021). Big data security management countermeasures in the prevention and control of computer network crime. *Journal of Global Information Management*, 30(7), 1–16. doi:10.4018/JGIM.295450
- Wayner, P. (1997). *Digital cash commerce on the Net*. Academic Press Professional.
- Windley, P. J. (2005). *Digital identity: Unmasking identity management architecture (IMA)*. O'Reilly Media.
- Wood, G. (2014). *Ethereum: A secure decentralized generalized transaction ledger*. Ethereum project yellow paper.
- Yin, R. K. (2014). *Case study research: Design and methods*. SAGE publications.
- Young, A., & Verhulst, S. (2018). *Self-sovereign identity for government services in Zug, Switzerland*. GovLab. <https://blockchan.ge/blockchange-government-services.pdf>

Ashish Singla is a doctoral candidate and research scholar at the Management Development Institute, Gurgaon, with a research focus on "Business applications of Decentralized Identity Management (DID) using Blockchain." He is a senior digital transformation professional with over 25 years of global information systems experience in program management, product management, and engineering with leading multinationals mostly in the financial services, telecom, and energy sectors. He is currently employed as Director, General Ledger Platform, for Natwest Group, UK.

Nakul Gupta is a faculty at Management Development Institute Gurgaon, India. His field of work and interest is Information Management with a focus on Data Visualization.

Prageet Aeron is a Fellow of Management (Computers and Information Systems) from Indian Institute of Management, Ahmedabad. At IIM Ahmedabad he was a recipient of the IDEA IIMA Telecom Centre of Excellence Research Award. Before he joined MDI Gurgaon, he was an Assistant Professor at IMI (2013-2015), New Delhi, and prior to that Assistant Professor at Jindal Global Business School (2010-2013), Sonapat. Prior to his doctoral education he was working as a Scientist with DRDO, HEMRL, Pune, working on research and development related to explosives and propellants (with a focus on Gun propellants). He holds a Bachelor's Degree in Chemical Engineering & Technology from Indian Institute of Technology, Banaras Hindu University (IIT-BHU).

Anshul Jain is an Associate Professor at the Management Development Institute in Gurgaon, India. His research focuses on Financial Market Microstructure and FinTech.

Divya Sharma is a faculty in the area of Information Management at MDI Gurgaon. She has completed the Fellow Program in Management from Indian Institute of Management Calcutta. She is the recipient of the Satish K Sehgal Doctoral Student Award (2018) for excellence in scholarship and organisational citizenship at IIM Calcutta. After completing her doctoral studies, she started her academic journey at the Indian Institute of Management Rohtak, and was thereafter employed with the OP Jindal Global University. She has also offered courses in a visiting capacity at IMI, New Delhi.

Sangeeta Shah Bharadwaj is Professor Information Management Area, MDI. She is MSc (Maths), MMS (Master of Management Studies), ME (Systems and Information), and PhD from BITS, Pilani. She is Dean Administration, Quality and Compliance. She has also held position of Dean Executive Education and Chairperson Digital Infrastructure. As Dean (AQC) she is leading projects related to National and International accreditation. As Chairperson Digital Infrastructure, she has successfully implemented Oracle Peoplesoft ERP at MDI, RFID project of Library, Document Management System, RFID project of Fixed Assets, etc.