Journal of Global Information Management
Volume 31 • Issue 2

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 Bharadwaj, 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

INTRODUCTION

Proving one's digital identity has become crucial when accessing government and commercial services or participating in the digital and mobile economy (Rannenberg, 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