Chapter 14
Securing Data Privacy in Blockchain Networks

Hakikur Rahman
https://orcid.org/0000-0002-2132-1298
Presidency University, Bangladesh

ABSTRACT

In this chapter, we tackle the significant obstacles linked to closing the information gap on blockchain technology adoption, promotion, and use between small and medium-sized enterprises (SMEs), businesses, organizations, government agencies, and the general public. We specifically concentrate on the two most important issues: data privacy and cybersecurity. Through an examination of data security management systems, regulatory frameworks, and legitimate encryption techniques, we put out a strong blockchain-based storage plan. This strategy promotes confidence and accountability across multiple industries by enabling safe digital transactions when paired with smart contracts. To improve openness and efficacy in data management, our study includes components including pseudonymity, transaction traceability and data leakage and privacy enhancing techniques.

1. INTRODUCTION

In an era of rapid digitalization, blockchain technology has emerged as a transformative solution for decentralized data management across numerous sectors, including finance, healthcare, supply chain, and knowledge management (Das & Parihar, 2019). As a distributed ledger, blockchain offers enhanced transparency, immutability, and security (Conti, Kumar, Lal, & Ruj, 2018). However, the very properties that make blockchain networks appealing also present unique challenges to data privacy. Unlike traditional centralized databases, blockchain networks

DOI: 10.4018/979-8-3693-3956-5.ch014

Copyright © 2025, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited.

inherently involve public, decentralized data storage and verification, which raises significant concerns about protecting user information and sensitive data (Zyskind, Nathan, & Pentland, 2015). Addressing these privacy challenges is critical to fostering broader adoption of blockchain technology, especially in knowledge-intensive applications where confidentiality is paramount (Rathi, Tiwari, & Sharma, 2020). This chapter delves into the privacy implications of blockchain networks, explores existing privacy-enhancing techniques, and assesses the regulatory landscape, aiming to equip readers with a comprehensive understanding of data privacy in blockchain environments and highlight avenues for future research (Liu, Liu, & Jin, 2019).

Importance of Data Privacy in the Context of Blockchain Networks

A distributed digital ledger with blocks of transactions is called a blockchain (Dorri, et. al., 2017). In a blockchain, a transaction that a user starts must first be signed with a private key and then sent to every node in the network to be included in a block. Next, the transaction is put into a candidate block together with other transactions. Before the candidate block is uploaded to the blockchain, it must first undergo validation through a procedure called mining. Depending on the blockchain's consensus method, the mining procedure varies, but it usually entails calculating a value based on the transactions in the block.

Following the mining process, the node will broadcast the block to every other node in the network, enabling them to quickly and easily confirm the accuracy of the generated value. The block is uploaded to the Blockchain if everything is correct; if not, it is removed (Christidis, & Devetsikiotis, 2016). Since a block added to the ledger cannot be changed without invalidating that copy of the blockchain, it is immutable by design (Bhosale, et. al., 2019).

The way individuals transact in the digital world has changed significantly as a result of the broad use of blockchain technology. People are able to transact in a transparent but anonymous way. Although the details of their transactions are open to the public, their identities are kept secret. While there have been advantages to this in some application areas, it may not be appropriate for transactions where it is crucial to know who you are dealing with or in situations where the blockchain may include confidential data. Because only authorized users are able to transact on private blockchain networks, these kinds of transactions are better suited for them. Since it is possible to limit who can view transaction information, sensitive data can also be stored on the blockchain (Ncube, Dlodlo, & Terzoli, 2020).

In the context of blockchain networks, privacy is the capacity of various entities to exchange digital products, such cash, data, or tokens, without having to divulge any information about their identities or previous transactions (Teo, Chow, & Williamson,

42 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/securing-data-privacy-in-blockchain-networks/366254

Related Content

Optimizing Sample Design for Approximate Query Processing
Philipp Röschand Wolfgang Lehner (2013). *International Journal of Knowledge-Based Organizations (pp. 1-21).*
www.irma-international.org/article/optimizing-sample-design-for-approximate-query-processing/101191

The Evolution of Inter-Firm Collaboration in Supply Chain Networks
Michael J. Gravierand M. Theodore Farris (2012). *International Journal of Knowledge-Based Organizations (pp. 1-31).*
www.irma-international.org/article/evolution-inter-firm-collaboration-supply/68971

A Research Model for Knowledge Management
Pamila Demblaand En Mao (2002). *Knowledge Mapping and Management (pp. 297-310).*
www.irma-international.org/chapter/research-model-knowledge-management/25402

Expliciting Tacit Knowledge: Exploring an Uncharted Path for a Questionable Trip
George Leal Jamiland Ângela Do Carmo Carvalho Jamil (2017). *Handbook of Research on Tacit Knowledge Management for Organizational Success (pp. 30-52).*
www.irma-international.org/chapter/expliciting-tacit-knowledge/181344

Strengthening Knowledge Transfer between the University and Enterprise: A Conceptual Model for Collaboration
José L. Pineda, Laura Esther Zapataand Jacobo Ramírez (2010). *Cultural Implications of Knowledge Sharing, Management and Transfer: Identifying Competitive Advantage (pp. 134-151).*
www.irma-international.org/chapter/strengthening-knowledge-transfer-between-university/36665