Chapter 68
A Comprehensive Review of the Security and Privacy Issues in Blockchain Technologies

Mangesh Manikrao Ghonge
https://orcid.org/0000-0003-0140-4827
Sandip Foundation's Institute of Technology and Research Centre, India

N. Pradeep
https://orcid.org/0000-0001-7351-5265
Bapuji Institute of Engineering and Technology, India

Renjith V. Ravi
https://orcid.org/0000-0001-9047-3220
MEA Engineering College, India

Ramchandra Mangrulkar
https://orcid.org/0000-0002-9020-0713
Dwarkadas J. Sanghvi College of Engineering, India

ABSTRACT

The development of blockchain technology relies on a variety of disciplines, including cryptography, mathematics, algorithms, and economic models. All cryptocurrency transactions are recorded on a digital and decentralized public ledger known as the blockchain. Customers may keep track of their crypto-transactions by looking at a chronological list rather than a centralized ledger. The blockchain's application potential is bright, and it has already produced results. In various fields, blockchain technology has been incorporated and deployed, from the earliest days of cryptocurrencies to the present day with new-age smart contracts. No comprehensive study on blockchain security and privacy has yet been done despite numerous studies in this area over the years. In this chapter, the authors talked about blockchain's security and privacy issues as well as the impact they've had on various trends and applications. This chapter covers both of these topics.

DOI: 10.4018/978-1-6684-7132-6.ch068

INTRODUCTION

In the business network, a Blockchain is a distributed, decentralized ledger or database that makes it easier to record commercial transactions. It can also be explained as an open-source, decentralized database that is accessible to all members of the network at all times. A majority of the network's participants must agree on every transaction before it can be recorded in the public ledger. A transaction uploaded to the blockchain can't be deleted or tampered with once the block contains verification information about it. Blockchain was first used in 2009 with the introduction of Bitcoin. This electronic payment system or cryptocurrency is cryptographically safe because it makes use of peer-to-peer (P2P) network technology. Payments cannot be made to any central institutions, such as a bank, because there is no trusted third-party authority to whom payments can be made. The owner of a Bitcoin is free to use it whenever and wherever they want without having to deal with a centralized authority. Bitcoin's arrival has sparked a lot of interest in Blockchain, which has now garnered the attention of academics as well as industry. The Blockchain's features enable security, privacy, and data integrity without the involvement of a third party in transaction control, which is why it's attracting attention.

Although the financial industry has embraced blockchain as its foundational technology, customers have expressed reservations about the platform's inherent security. Integrity, confidentiality, and availability are common concepts used to describe security. Public blockchain systems are mostly based on distributed networks and have limited levels of confidentiality, but their integrity and availability are guaranteed by these systems. In these blockchain systems, data accessibility is always on the higher end. Data replication for distributed systems increases readable data availability, but it decreases write availability. Despite the fact that the blockchain's underlying architecture is extremely safe, implementations of cutting-edge technologies have taken use of the blockchain's security features. Because all of the network's public keys are visible to everyone, the blockchain system is likewise susceptible to the leaking of transactional privacy. Ethereum and smart contracts have recently been found to have a number of security flaws. For instance, thieves exploited a smart contract recursive calling vulnerability in June 2016 and stole $60 million. Blockchain security and privacy issues have been investigated in several research, however, none have provided answers for enhancing security. In this chapter, we'll examine blockchain technology from a broader perspective, including the security concerns that go along with it. In this chapter, we'll go over the numerous security issues associated with popular blockchain systems, including a real-world assault and an analysis of the vulnerabilities exploited. For the sake of data security and preventing vulnerabilities, we'll also cover various encryption approaches in this chapter.

As you can see, the chapter is organised in the following manner. Our definition of blockchain technology and related concepts and techniques is found in Section 1. Blockchain is discussed in Sections 2 and 3, while Section 4 focuses on security-related issues. Finally, in Section 5, we talk about blockchain privacy issues. Sections 6 and 7 then present blockchain applications and challenges. Section 6 then wraps up the chapter.

STRUCTURE OF BLOCKCHAIN

While relational databases can be shared between various users, blockchains are decentralised electronic ledgers that produce an immutable record of transactions, each of which is time-stamped and connected to the one before it. In the digital ledger, each block is referred to as a digital record or transaction, and