Chapter 8
Role of Blockchain in Digital Forensics:
A Systematic Study

Amit Kumar Tyagi
https://orcid.org/0000-0003-2657-8700
National Institute of Fashion Technology, New Delhi, India

Bukola Fatimah Balogun
Kwara State University Malete, Nigeria

Shrikant Tiwari
https://orcid.org/0000-0001-6947-2362
Galgotias University, Greater Noida, India

ABSTRACT

Digital forensics plays an important role in investigating cybercrimes, data breaches, and other digital misdeeds in an increasingly connected world. With the proliferation of blockchain technology, a new dimension has emerged in the world of digital forensics. This work presents a comprehensive review of the intersection between blockchain and digital forensics, exploring the various ways blockchain technology influences and challenges the traditional practices of digital forensic investigations. This work begins by elucidating the fundamental concepts of blockchain technology, emphasizing its decentralized and immutable nature, cryptographic underpinnings, and its uses in cryptocurrency transactions. Subsequently, it delves into the potential benefits of blockchain for digital forensics, such as providing transparent and tamper-proof logs of digital activities and transactions. However, this chapter also discusses the unique challenges posed by blockchain in digital forensic investigations.

DOI: 10.4018/978-1-6684-8127-1.ch008

INTRODUCTION TO BLOCKCHAIN AND DIGITAL FORENSICS

A. Blockchain Fundamentals: Definition, Concepts, Types, Key Components of Blockchain Technology

Blockchain is a distributed and decentralized digital ledger technology that records transactions across multiple computers in a way that ensures the security, transparency, and immutability of the data (Al-Khateeb, Epiphaniou, & Daly 2019; Kumari, Tyagi, & Rekha, 2021). It consists of a chain of blocks, each containing a batch of transactions, which are linked together and secured through cryptographic hashes. Now here few of the key concepts of Blockchain are:

- Decentralization: Blockchain operates on a decentralized network of computers (nodes) rather than relying on a central authority. Each node has a copy of the entire blockchain ledger, ensuring redundancy and resilience.
- Distributed Ledger: The ledger, containing transaction data, is distributed across multiple nodes. This distribution prevents a single point of failure and enhances transparency.
- Blocks: Transactions are grouped into blocks, and each block contains a set of transactions. Blocks are linked together chronologically to form a chain.
- Transactions: Transactions represent actions or data changes recorded on the blockchain. These can include cryptocurrency transfers, smart contract executions, or any data update relevant to the blockchain's purpose.
- Consensus Mechanisms: Blockchain networks use consensus algorithms to validate and agree on the state of the ledger. Common consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS).
- Cryptography: Cryptographic techniques, such as hashing and digital signatures, secure data on the blockchain. Hashes uniquely identify blocks and their contents, while digital signatures ensure transaction authenticity.
- Immutability: Once data is added to the blockchain, it becomes extremely difficult to alter. This immutability ensures the historical integrity of transactions.
- Public vs. Private Blockchains: Public blockchains, like Bitcoin and Ethereum, are open to anyone, while private blockchains restrict access to authorized participants. Consortium blockchains are semi-private, allowing a group of organizations to participate.
- Smart Contracts: Smart contracts are self-executing contracts with predefined rules and conditions. They automatically execute actions when the specified conditions are met, providing automation and trust in various applications.

Related Content