Chapter 2
Blockchain Technology for Evidence Integrity

Vijayakumar Ponnusamy
https://orcid.org/0000-0002-3929-8495
SRM Institute of Science and Technology, India

Nandini Manickam
SRM Institute of Science and Technology, India

Arivazhagan N
SRM Institute of Science and Technology, India

ABSTRACT

Forensic science plays a crucial role in investigating crime events through scientific methods. It collects evidence based on fingerprints and DNA analysis that must be presented in court for judgment. It faces difficulties in investigating the data between interconnected devices and also faces data privacy and security issues. Blockchain technology provides solutions by creating immutable and transparent records through a chain of interconnected blocks. Since it creates a copy of transactions and makes it available for all the nodes in the chain, modifying or deleting a transaction becomes difficult. This chapter discusses the role of blockchain in enhancing data privacy and security in evidence integrity and also discusses the various techniques, advantages, and challenges faced by blockchain in cyber forensics.

DOI: 10.4018/979-8-3693-9405-2.ch002

INTRODUCTION

People have become more dependent on emerging technologies for daily activities, communication, and remote access using media which creates a lot of chances in exchanging data from one system to another. This has led to an increase in cybersecurity to preserve data privacy. Investigations of crime events, and their corresponding evidence like fingerprints, and documents need to be preserved. These data are collected and organized through digital devices like mobile, computers, and the cloud. Digital forensics is a branch of cybersecurity mainly used for analyzing, retrieving, and examining digital evidence. There are mostly two groups of people who make use of digital forensics. The first group of people are law enforcement agencies in criminal and civil cases. Law enforcement agencies use digital forensics to analyze the digital evidence of criminal cases to ensure justice at the crime scene. The second group of people are incident response teams in many organizations who are the responders to cyber attacks to prevent the events from threats. The investigators conduct a structured investigation based on the evidence collected and integrate the proof as a document which has to be produced as proof in the court. Digital evidence can be either volatile or non-volatile. There are a few forensic tools that support the process of inspecting devices to maintain data integrity.

- File analysis tool: extracts and analyses individual files
- Network analysis tool: monitors network traffic and payload
- Database analyzer: extracts, analyses, and examines the database to extract information.
- Registry tools: user activities are stored in registries
- Data capture tools: captures data, encrypts, and stores data
- Email scanners: scan all mail communications for investigating attacks.
- Mobile device scanners: scan internal and phone memories present in the devices.

IMPORTANCE OF DIGITAL FORENSICS

The advancements in technology have rapidly developed in many industries. Though the growth in technology has a lot of advantages like streamlined processes and efficiency yet faces cyberattack threats. The attack surface has multiple ports of entry that expose the network to external threats. Incident response and compliance auditing are crucial factors in digital forensics. If there is a legal component to the incident, investigators are required to present the documented results of the forensic investigation. Standard regulations are required to preserve the security and privacy