Chapter 16
Blockchain Forensics for Cryptocurrency-Driven Cybercrime

Seema Verma
https://orcid.org/0000-0002-7893-671X
Delhi Technical Campus, Greater Noida, India

Padmesh Tripathi
https://orcid.org/0000-0001-9455-1652
Delhi Technical Campus, Greater Noida, India

Pridhi Arora
https://orcid.org/0009-0002-5790-1742
Delhi Technical Campus, Greater Noida, India

ABSTRACT

Blockchain and cryptocurrencies have transformed the way digital transactions work by introducing decentralisation, transparency, and immutability. However, these features also allow some individuals to use them for cybercrimes. This chapter explains how blockchain records can be used to trace, investigate and mitigate such crimes. It also talks about how understanding the behaviour of users can help in finding out who the attackers are. This chapter begins with the basic ideas of blockchain and cryptocurrency, after this, it describes different types of cybercrimes that usually happen using cryptocurrency and also explains that traditional ways of investigating cybercrimes don't work well with blockchain and new frameworks are required to investigate and solve these cases. A key section of the chapter examines

DOI: 10.4018/979-8-3373-4898-8.ch016

how blockchain forensics helps in detecting cybercrimes. User-centric threat intelligence will be explored to understand the people behind cybercrimes that can help in investigations. In the chapter, Legal and ethical considerations will be addressed.

1. INTRODUCTION

The emergence of blockchain technology and its most well-known application, cryptocurrency, has introduced a model shift in digital transactions, creating a novel line for commerce, finance, and inevitably, crime. This technology, designed to operate beyond the reach of central authorities, simultaneously creates a permanent, transparent, and publicly auditable record of every transaction (Tripathi et al. 2023). This built-in contradiction, a tool for illicit actors that is also a rich source of evidence-forms the foundation of blockchain forensics. This chapter provides a comprehensive exploration of this field, beginning with the core technological principles that enable both crime and investigation. This chapter focuses on providing an overview of the domain of blockchain forensics in the context of cybercrime involving cryptocurrency. It aims to create the "street view" of the technology in question, by outlining the foundational criminal ecosystem, explaining the fundamental techniques of attribution, and tracing the paths to the criminal participants as well as the critical methods of de-anonymisation. The provided roadmap will walk the reader alongside the investigator's arsenal, provide and assess the critical breach inflicted by technologies aimed to enhance privacy, and analyse the significance of the on-chain information in the context of forensic investigations. The chapter will also address the intricate legal, regulatory, and ethical aspects of the work, anchored in empirical case studies. It will analyse evolving trends and directions for investigation in this fast-moving domain.

1.1 Core Concepts of Blockchain Technology

At its core, blockchain is a specific implementation of a comprehensive class of technologies known as Distributed Ledger Technology (DLT). A DLT is a decentralised, peer-to-peer digital system for recording transactions between parties in multiple places at the same time. A distributed ledger is a database that is synchronised across the network of participants, often referred to as nodes, not like a traditional database that relies on a central administrator. This structure eliminates the need for a trusted mediator like a bank or broker, and allows individuals to securely verify, execute, and record their transactions.

The security and ownership of assets on a blockchain are governed by asymmetric cryptography, which utilises a pair of mathematically related keys: a private