Chapter 31
The Intersection of Cybercrime and the Blockchain

Vishnu Venkatesh
Babson College, USA

Steven Gordon
Babson College, USA

ABSTRACT

The immutability of blockchains and the transparency of their transaction records would appear to limit the benefit of exploiting them for criminal activity. However, blockchains also offer a high degree of anonymity, similar to fiat paper currency; the technology was intended to facilitate trustless transactions. Coupled with a global, borderless reach, blockchains have become an enabler of cybercrime. They are a new class of assets that, like all other assets, possess security risks and become potential targets of attack. In particular, cryptocurrencies, which depend on blockchain technology, provide significant incentives for attack because of their value. The goals of this chapter are to identify and classify blockchain-based cybercrimes and to explore the avenues for protecting against them at individual, organizational, and policy levels.

INTRODUCTION

For much of the public, the term “blockchain” is synonymous with “bitcoin.” For many years, blockchain and bitcoin were, for all practical purposes, one and the same. But, over time, innovators found ways to improve and extend the bitcoin protocol and apply blockchain technology to many other uses. In 2020, blockchain applications encompass a broad array of technologies, each with a promise of improving how value is exchanged in the real world, but each containing the potential for hidden flaws that criminals might exploit. The objective of this chapter is to explain how criminals can exploit blockchain technologies, both to steal from its users and to hide the gains from other criminal activities in which they participate.

DOI: 10.4018/978-1-7998-5728-0.ch031

In March 2020, the top 100 blockchain cryptocurrencies were valued at more than $230 billion per coinmarketcap.com. Daily transaction volume at the major exchanges exceeded $72 billion. Clearly, the cryptocurrency market presents a huge opportunity for criminal activity.

In the early days, the world of cryptocurrency drew parallels to the "Wild West." Regulation and oversight were absent, security was lax, and bandits were everywhere. In one of the most famous blockchain thefts, in February 2014, 850,000 bitcoins, worth about $450 million at the time, were stolen from the leading cryptocurrency exchange, Mt. Gox. Cryptocurrency thefts continued despite an increased awareness of criminal activity after Mt. Gox and increasing regulation. For example, in January 2018, Coincheck, a Japanese exchange, experienced a theft of 523 NEM coins worth an estimated $533 million. Cryptanalysis reported that illicit entities received more than $11 billion in cryptocurrency in CY2019.

In this chapter, we explore the intersection of blockchain and cybercrime. First, we present a high-level overview of how blockchains and their complementary technologies work. Next, we describe many of the attacks known to exist on blockchain assets. Then, we examine how cybercriminals have used blockchains to fund illicit activities. Finally, we present the conclusions of this chapter and opportunities for further research.

BACKGROUND

To appreciate how a cybercriminal might attack blockchain assets, it is necessary to understand what blockchain assets are and how a blockchain maintains them. The sub-section on *Technology Overview* covers the technology behind the blockchain itself as well as two related technologies, smart contracts and state channels, which augment the capabilities of a blockchain. The next sub-section *The Scalability Trilemma* addresses the technological tradeoff among decentralization, security, and scalability of blockchain networks.

Technology Overview

The following description omits many details and greatly simplifies how blockchains actually work. Nevertheless, it should provide sufficient background for understanding possible types of attacks.

A blockchain's assets are called tokens. Tokens represent real assets, such as a currency, a commodity, a promise of future returns, or a bid at an auction. A blockchain is a distributed ledger that records the assets owned by its users. A blockchain's users are identified by addresses that correspond to a private key that they can create without the help of a third party. This private key, also called a secret key, is used to sign transactions that the user creates. Anyone can verify a signature given the signer's address. It is not necessary to know the private key to verify a signature, nor is it possible to derive the private key from a user's address. However, anyone who knows a user's private key can generate a transaction to send the user's assets to himself or herself.

The blockchain network consists of "nodes" that maintain the integrity of the ledger. Owners of an asset can transfer ownership to another party by signing a transaction authorizing the transfer. Upon verification of the owner's signature, one of a subset of the blockchain nodes, typically called miners or validators, assembles the validated transaction with others into a block of transactions. This block is transmitted to other nodes, which update their copies of the blockchain to record the new asset ownership.