Chapter 1
The Vulnerability of the Blockchain Network From the Consensus Perspective

Mohamed Ikbal Nacer
Bournemouth University, UK

Simant Prakoonwit
Bournemouth University, UK

ABSTRACT

The blockchain is a registry shared among different participants intending to eliminate the need for a central authority to maintain information. The first proposal of this technology was to eliminate financial authorities in transactions of value. However, the application of the same technique for the transaction of information could facilitate trades and offer traceability and diamond tracking around the world. The consensus is at the core of the network because it orchestrates nodes to accept new information, but it operates over a data structure in an open network, consequently leading to many complex behaviours that introduce different vulnerabilities. This work aims to highlight the vulnerability within the blockchain network based on the different participant behaviours that dominate the shared registry. Moreover, different malicious behaviour can appear on the networking layer by taking advantage of the network topology.

INTRODUCTION

The bitcoin white paper (Nakamoto, 2019) pushed the boundaries of knowledge by regarding an old problem from a different angle by implementing competency among different maintainers to gain a reward for block validation. This technique has led to the rise of cryptocurrency and has been followed by the introduction of many proposals, such as Blackcoin and Zerocash (Vasin P., 2014), (Sasson et al., 2014). The implementation of business logic through the adoption of a smart contact following the Nick Zabo approach has been conveyed in the Ethereum white paper (Wood, 2014). Chen in (Chen, 2018) proposed the use of traceability mechanisms to validate business information, but the consensus was

DOI: 10.4018/978-1-7998-7927-5.ch001

based on the follower and leader mechanism. These different stages have declared the beginning of a new era within blockchain technology through the implementation of different mechanisms to handle various kinds of information. Nevertheless, the platform as a whole suffers from heavy state transition, monopoly, or vulnerability to attacks.

The goal of the blockchain was to eliminate the bank as a trusted third party as part of a financial verification of the transaction. However, the techniques can be adopted in many industries. It has been found through numerous observations that it can be applied to provide identity verification, secure diamond grading, and track shipments around the world. (Dillenberger et al., 2019). Since the blockchain network's first proposal, there was a huge hype that tended to show the virtue of its adoption. The rapid development of this technology has highlighted the different ways in which it can make everyday life easier. Thus, many works on the heart of blockchain technology, which is consensus, attempt to promote the importance of the approach to ensure confidentiality, transparency, accountability, traceability, and management of identities. Singh et al. in (Singh. et al., 2018) point out that blockchain technology is a game-changer in the IoT industry before discussing the security issues within the technology that arise from decision distribution, which provides transparency to different battery holders. Moreover, the paper introduced an architecture that separated the user and the miner to keep a record of the validity of the ledger. Fakhri et al. in (Fakhri. & Mutijarsa., 2018) implemented a blockchain and non-blockchain system to provide a test comparison of their performance, in which they were dedicated to the storage of data generated by IoT device. The comparison showed the conceptual contribution in terms of security provided by the blockchain implementation.

Buccafurri et al. in (Buccafurri. et al., 2017)studied the suitability of the blockchain within the context of the IoT. They claimed that the advantages of the network, such as record-keeping, coordination among stakeholders, transparency, and irrevocability of transactions, are characteristics that are also desirable within the IoT sector. Mendki in (Mendki, 2019) proposed an architecture to enable the use of the blockchain within a fog system to secure communication between a user and the fog end server, taking into consideration the limitations on horizontal scalability. The work by Singh et al in (Singh. et al., 2018) studied the possible impacts on the internet from the integration of the blockchain as a backbone communicative mechanism. They found that cyberattacks, such as the denial of service, arise from the centralization of the different services offered by the network. El Kafhali et al. (El Kafhali et al., 2019) introduced a raw data stream within the fog and cloud base by proposing the use of different blockchain networks for each part of the platform.

The work of Nada et al. in (Alasbali et al., 2020) raised concerns over the lack of standards of interoperability within the growing market of blockchain implementation. They proposed a model to handle heterogeneous data. The growth of the different sources to gather data within one running technique led to the discussion of the blockchain as a web by Naim et al. in (Naim et al., 2020). The solution aimed to propose an extension of the semantic blockchain platform by adding a layer of service to handle the different sources of data. Chou et al. (Chou et al., 2020) discussed the problem of data bloating within the blockchain due to immutability within the ledger. The solution was an integration of IPFS to manage the data through the injection of a clustering algorithm that aims to spot the cold and hot data to speed up the validation of the new data. Ismail et al. in (Ismail, et al., 2020) implemented and evaluated a platform that decentralizes access to the health care sector with the use of blockchain technology.

This work aims to provide a study on blockchain technology from a security vulnerability perspective. It addresses the consensus mechanism at the core of its functioning by providing the vulnerability within each step and analyses how each element of the platform can lead to exterior manipulation. The