Chapter 4
The Paradigms of Blockchain Technology: Myths, Facts & Future

Robin Singh Bhadoria
Indian Institute of Information Technology (IIIT) Bhopal, Madhya Pradesh, India

Vaibhav Agasti
Indian Institute of Information Technology (IIIT) Nagpur, Maharashtra, India

ABSTRACT

The invention of blockchain technology has paved the way for the decentralization of existing systems. Blockchains have consistently delivered prominent applications, particularly in the finance sector. The most popular application of blockchain is cryptocurrency. Blockchain technology however has a variety of applications beyond cryptocurrencies. This article discusses the basics of blockchain technology along with some of its potential applications. With the rising use of this technology, the security of these systems is a major concern. The security threats and risks to blockchain systems are also reviewed along with the tools and methodologies to prevent and handle it in more sophisticated manner.

INTRODUCTION

Blockchain is essentially public ledger of digital events or transactions that have occurred in a system. It can be thought of as a distributed database of transactions that is encrypted and cannot be tampered with. This feature of blockchain has very promising applications in finance, medicine, IoT, governance etc. since there is a rising demand for platforms to carry out secure and smoother transactions in these domains (Huckle et al., 2016). However, there are some security threats to the blockchain system that can affect its regular operations. Thereby, there is need of incorporating additional security enhancements to these systems. When the blockchain technology becomes mature enough, it will have the potential to disrupt the way current systems function by shifting the focus towards decentralization of these systems.

DOI: 10.4018/978-1-7998-5351-0.ch004

This paper begins with an introduction to the blockchain technology Mayer (2016) and its common applications Juels, Kosba and Shi (2016). The following sections review the security risks Juels, Kosba, and Shi (2016) to a blockchain system and analyses the attacks that can be executed on this system Nakamoto, S. (2008). Section 5 discusses the security enhancements that can be made to the existing systems. Finally, section Heilman, Kendler, Zohar and Goldberg (2015) discusses about the future prospects of the technology.

FUNDAMENTALS OF BLOCKCHAIN

Structurally, a blockchain, as the name suggests, is a chain of blocks in which each block represent digital event(s) that have been executed. Every block in this blockchain contains some information about the particular transaction, a reference to the previous block in the chain and an answer to a complex mathematical question which validates the data within the block. This chain of blocks collectively constitutes the ledger and a copy of it resides on every node in the network. These copies are synchronized at regular intervals to maintain consistency of the records (Wright & De, 2015).

To execute an event or a transaction within the system, a block representing that event is created. This block is then verified via a consensus mechanism by majority of nodes on the network. If the block is invalid, the event is not executed and the transaction is declared as void. However, if the block is verified as valid by majority of nodes in the system, the event is executed and the block is appended to the blockchain. Every node makes this update to their copy of the database as consistency of records is crucial for this mechanism to function.

In order to verify the new proposed transaction, certain consensus mechanisms are used. Some of these are given below. Each of these mechanisms takes a different approach and utilizes different resources for the verification process.

1. **Proof of Work (PoW):** In the Proof of Work model (Figure 1), the miners within the network compete against each other to verify the transaction or to generate the next block of the blockchain. This is mainly done by solving complex mathematical and cryptographic puzzles. The first node to solve this puzzle proposes the solution and the new block to the rest of the nodes on the network. These nodes check the validity of the proposed solution and the new block that is generated. The miner receives a reward as compensation for the computational power and electrical energy that was spent. The reward is mainly in cryptocurrencies such as bitcoin that are mined during this process. This protocol however has a disadvantage of wasting a lot of computational resources.
2. **Proof of Stake (PoS):** The Proof of Stake model requires nodes to invest coins if they want to participate in the validation process which is contrast to investing high computational power as per PoW model. The process of mining does not take place in this protocol. The validators are paid by the parties that participate in the transaction. Every validator gets a chance to create or to propose the new block corresponding to the amount of investment that he/she made. In this mechanism, one node is selected in a pseudo-random fashion and thereby no validator knows when he gets his turn.
3. **Proof of Burn (PoB):** In the Proof of Burn model, miners burn their coins to get the privilege to propose the next block. This means that the coins are sent to a location where they are 'lost' and can't be retrieved. The more coins a node burns, the better there are for it to be selected to mine the next block. This method also faces the drawback of wasting resources by burning coins.