Chapter 7
Study and Survey on Blockchain Privacy and Security Issues

Sourav Banerjee
Kalyani Government Engineering College, India

Debashis Das
https://orcid.org/0000-0003-4422-3196
University of Kalyani, India

Manju Biswas
Kalyani Government Engineering College, India

Utpal Biswas
University of Kalyani, India

ABSTRACT

Blockchain-based technology is becoming increasingly popular and is now used to solve a wide range of tasks. And it's not all about cryptocurrencies. Even though it's based on secure technology, a blockchain needs protection as well. The risks of exploits, targeted attacks, or unauthorized access can be mitigated by the instant incident response and system recovery. Blockchain technology relies on a ledger to keep track of all financial transactions. Ordinarily, this kind of master ledger would be a glaring point of vulnerability. Another tenet of security is the chain itself. Configuration flaws, as well as insecure data storage and transfers, may cause leaks of sensitive information. This is even more dangerous when there are centralized components within the platform. In this chapter, the authors will demonstrate where the disadvantages of security and privacy in blockchain are currently and discuss how blockchain technology can improve these disadvantages and outlines the requirements for future solution.

DOI: 10.4018/978-1-7998-8954-0.ch007

INTRODUCTION

The evolution of Blockchains (or integrated ledger technology) has been likened to the growth of the Internet. As a result, there have been remarks and discussions about the ability of technology to disrupt various sectors such as healthcare, the public sector, energy, manufacturing and, in particular, financial services (Grut, 2016). This means the emergence of evolved suppliers to evolved industrial sectors. Blockchain is popular today, but there are still critics who challenge the technology's scalability, safety, and sustainability.

If one assumes a peripheral device that does not have a single point of error and is resilient to the cyberattacks that make news these days. This is the value presented by Blockchain. This value is enabled by the shared ledger, which today is used for cryptocurrencies like Bitcoin and Ethereum, which challenges the conventional model of server/client architecture. Bitcoin has become the first application developed using Blockchain in 2009. A safe decentralized currency exchange system eliminated the use of internal intermediaries. Recently, in other areas, Blockchain has proved its worth (Dickson, 2016). It could be said that Blockchain is the continuation of centuries of cryptography and safety studies and breakthroughs. This breakthrough offers a completely distinct strategy towards saving data and performing tasks, making it particularly appropriate for settings with strong safety demands and mutually unidentified performers. Participants who are already acknowledged by the ledger validate and process requests within a permitted Blockchain transaction.

Technologies based on Blockchain are becoming common. Today Blockchain serves a broad variety of functions and not everything has to do with cryptocurrencies. Blockchain technology is the main component in the establishment of business operations that can be used in the manufacturing sector. In the Internet of Things (IoT) networks, scalability governance applications, cryptocurrencies, and many other areas, the Blockchain technique is also being applied. Therefore, Blockchain is now a vital and cutting-edge element for a whole range of enterprises. However, Blockchain can itself be subjected to multiple hazards based on security-driven metric. This is because Blockchains include confidential data regarding particular participants, businesses resources and services, therefore it is essential to provide extensive security. This chapter will demonstrate areas of disadvantages towards safety and privacy in Blockchain. This chapter also will discuss how Blockchain technology can improve safety and privacy as well as outlines future difficulties and problems.

BLOCKCHAIN TECHNOLOGY

Blockchain is a decentralized computation and information sharing platform that enables us to connect multiple authoritative domains where no one can trust each other in order to cooperate, collaborate and coordinate with each other in an intelligent decision-making process. Figure 1 shows that Blockchain is also a data structure which stores all the ordered set of block-organized transactions (Zheng et al., 2017). The first block of the Blockchain is called genesis block. A block in a Blockchain can contain only a single transaction or more.

Once, there was a traditional way of sharing information and this environment was and 'is' still centralized. The main problem with this type of environment is that of the single point of failure. This implies that if the central node crashes then all other nodes, which are connected, with the central node are disconnected. In a Blockchain, every node maintains a local copy. This copy, which is identical to