Chapter 59
Security, Privacy, and Trust Management and Performance Optimization of Blockchain

Priti Gupta
Banaras Hindu University, India

Abhishek Kumar
Banaras Hindu University, India

Achintya Singhal
https://orcid.org/0000-0003-0242-2031
Banaras Hindu University, India

Shantanu Saurabh
The Maharaja Sayajirao University of Baroda, India

V. D. Ambeth Kumar
Department of Computer Science and Engineering, Panimalar Engineering College, Anna University, Chennai, India

ABSTRACT

Blockchain provides innovative ideas for storing information, executing transactions, performing functions, creating trust in an open environment, etc. Even though cryptographers, mathematicians, and coders have been trying to bring the most trustable protocols to get authentication guarantee over various systems, blockchain technology is secure with no central authority in an open network system because of a large distributed network of independent users. If anyone tries to change the blockchain database, the current hash will also change, which does not match with the previous hash. In this way, blockchain creates privacy and trust in digital data by removing malleability attacks. In this chapter, security and privacy on the blockchain has been focused. The safety and privacy of blockchain are mainly engrossed on two things: firstly, uncovering few attacks suffered by blockchain systems and, secondly, putting specific and advanced proposals against such attacks.

DOI: 10.4018/978-1-6684-7132-6.ch059

INTRODUCTION

Why Blockchain – does it secure? Can we trust on it?

Blockchain technology has been called the one of the greatest innovations since the internet. Blockchain is a peer-to-peer distributed ledger or public registry that permanently records transactions in a way that cannot be erase or update. Blockchain is designed to use a cryptographic hash and timestamps so that record cannot be change once they are created. This makes easier for the blockchain experts to inspect record ledger or registry to determine the facts of any given transactions or to detect attempts to tamper with the ledger.

Blockchain is secure. 'Secure' doesn't means to hide information but it simply means that nobody going to tamper records on the blockchain. Even if somebody does attempt to fraudulently alter records, original records will still exist on the valid ledger and can be pinned down by comparing information on duplicate records.

Billions of people in the world who can't trust intermediaries such as banks, and other legal system for transactions or accurate record keeping. Particularly, Blockchain are useful in these cases to provide trust and assurance to people when transacting with one another. Centralized databases and institutions work when there is trust in the system of regulations, laws, government and people. Even sometimes, this trust is betrayed, causing people to lose money and assets. Blockchain is a decentralized database which remove the need of centralized institutions and databases. With all people connected to the blockchain network having access to the blockchain ledger in a way they can view and validate transactions which create transparency and trust. Although blockchain removed intermediaries to maintain the trust between the people involved in the transactions. The removal of intermediaries improved transparency and decentralized structure of the blockchain (Mark Gates, 2017).

Figure 1. Blockchain architecture diagram