Chapter 28
Blockchain Technology–Security Booster

Harsha Kundan Patil
https://orcid.org/0000-0002-1801-4086
Ashoka Center for Business and Computer Studies, Nashik, India

ABSTRACT

"Blockchain" as the name suggests is the chain of blocks. It is the chunk of digital information (blocks) that are connected through the public databases (Chain). It is nothing but the newer version of file organisation. Blocks store digital information like actual record of any transaction, details of involve entities in the transaction, time stamps, and other metadata of the transactions. Blocks also have unique ids, which are known as hash. Blockchain technology is built using peer-to-peer networking. Anyone who is on network can access the blocks. There is no centralised community to control the blockchain. It is operated by miners, the peoples who lend their computing power to the network to solve the complex computation algorithm problems. These blocks are stored in multiple computers. Due to its distribution and decentralisation, the validation process is broadcast in nature, which provides it "the trusted approach". Blockchain enables security and tamperproof capabilities for storing data and smart contracts. Any tampering of data attempted by a node or user in a block changes the hash of the block. The blockchain technology has the capability to face and provides the solution to fight with the problem of risk and security concern online. In 2008, a mysterious white paper titled "Bitcoin: A Peer to Peer Electronic Cash System", by visionary Satoshi Nakamoto gave birth to the concept of blockchain. The chapter explains the structure of blockchain technology in detail and enlighten the aspects that make blockchain technology the secure concept of today's world.

INTRODUCTION

"Blockchain" as the name suggest is the Chain of Blocks. The Chunk of digital information (Blocks) which are connected through the public databases (Chain). It is nothing but the newer version of the File organisation. Blocks stored digital information like actual record of any transaction, details of involve entities in the transaction, timestamps and other metadata of the transactions. Blocks also has unique id which is known as hash.

DOI: 10.4018/978-1-6684-7132-6.ch028

Blockchain technology is built using peer-to-peer networking. Anyone who is on network can access the blocks. There is no centralised community to control the Blockchain. It is operated by miners; the peoples who lend their computing power to the network to solve the complex computation algorithm problems. These blocks are stored in multiple computers. Figure 1 shows step by step working of Blockchain.

Step1: Whenany online transaction like purchasing through Amazon occurred and successfully completed the details of transaction is recorded.

Step2: The next step is verification. The details of the transaction verified through network of computers. Thousands of computers connected through global network are utilised for verification process. Which involves verification of purchased article details, transactiontimestamp, cost and parties involved in it.

Step3: After transaction details verified it stored in block with digital signatures of involved parties. One block may contain many verified transactions. The block also have the hash key which gives the unique identification to the block. This block is then added to existing chain of block. So in this way the blockchain grows. Once the block is added to blockchain it is publically available for all.

Each computer which is connected to the blockchain network has their own copy of blockchain and whenever new block added on it the copy of each computer is updated. That means all the computers of the blockchain network have the same copy of network and each time whenever any block is access or added the verifications are done by all connected computers. As we know it is easy to hide from one's eye but difficult to hide from all's eyes. This 360 degree verification of public network makes blockchain very secured.

Concept of Blockchain Technology and its Emergence

Blockchain, the underlying technology behind cryptocurrencies has its origin that stem from a problem of verifying timestamp digitally in the late 1980s and early 1990s. In 1990, Haber & Stornetta published a paper titled 'How to Timestamp a digital Document'. In this paper, they proposed to create a hash chain by linking the issued timestamps together so that the documents get prevented from being either forward dated or back dated, (Haber,1990). Then, Wei Dai one of the noted researchers, introduced the concept of b-money which is used to create money through solving computational puzzles and decentralized consensus. But this proposal lacks implementation details (Dai, 1998). A concept called "reusable proofs of work" was introduced by Hal Finney. This concept combined the ideas of both b-money and computationally difficult Hash cash puzzle by Adam Back for the creation of cryptocurrency.

Block chain technology is having the focus of Ecommerce developer due to its quality of exchange of value units without the need of intermediaries (Nakamoto, 2008). It allow us to secure our digital assets like art or digital data from sensors on a marketplace (Draskovic and Saleh, 2017), or allowing property owners to transfer their land without a notary (Kombe et al., 2017). Technology is also get used to address several other scientific problems (Dhillon, 2016; Golem, 2016; Wolf et al., 2016; Breitinger and Gipp, 2017; van Rossum, 2017; Androulaki et al., 2018) like trust problems in the form of malicious behavior in peer-review processes (Stahel and Moore, 2014; Degen, 2016; Dansinger, 2017), lacking quality and redundancy of study designs (Belluz and Hoffman, 2015), and the restriction of free access to scientific publications (Myllylahti, 2014; Teplitskiy et al., 2017; Schiltz, 2018).