Chapter 63
Decentralizing Privacy Using Blockchain to Protect Private Data and Challanges With IPFS

M. K. Manoj
VIT University, India

Somayaji Siva Rama Krishnan
VIT University, India

ABSTRACT

Blockchain technology is a distributed framework for sharing data that is validated through cryptographic functions. The nodes of the network come to a consensus regarding addition of data to the blockchain. Every blockchain operation requires a processing fee. This fee makes storing of large data on the blockchain infeasible. An indirect alternative for this challenge could be use of IPFS, which is a decentralized peer-peer network that facilitates storage of file. This is accomplished by storing the hash of the IPFS as data on the blockchain.

WHAT IS BLOCKCHAIN?

A blockchain is a time-stamped series of immutable records of data that is managed by a cluster of computers. Information held on a blockchain exists as a shared and continually reconciled database. This means that data of a blockchain is not owned by a single entity. Each of these blocks of data is secured and bound to each other using cryptographic principles (Rosic, 2016).

If all the data is shared then this means that there is no centralized version of this information. Thus, a blockchain has no centralized authority. The information on the chain is open for anyone and everyone in the network to see. Hence, anything that is built on blockchain is very transparent by nature and everyone involved is accountable for their actions (Hales, 2019).

DOI: 10.4018/978-1-6684-7132-6.ch063

WHY BLOCKCHAIN?

The blockchain is considered a disruptive technology; one that significantly alters the way businesses or entire industries operate. It often forces companies to change the way they approach their business or fear losing market share and to become irrelevant.

Blockchain brings into picture something truly unique. It gives a new no trust mechanism. Imagine a situation where a transaction made by a person A is shown to be done but due to a malicious intruder (hacker) or software error it does not show up but the amount is lost, or a case where the bank balance of A is different from the actual balance that A thinks it is. For situations like these, the third party trust is a must. A person trusts a bank and uses its features. If in case know that a bank is not trustworthy or is fraudulent then the obvious choice is to not use that particular bank's services. If an unfortunate error happens, the bank is held liable for any mistakes made.

Such situations will never arise with blockchain being similar to a public ledger with so many people acting as proof of one's transaction. There is no need to rely on a third party and hence it has become a huge concept seeking attention. The blockchain provides a trust and authentication protocol that has already disrupted banking and is on the verge of revamping healthcare, financial services, social apps and more.

Blockchain brings the proof of trust in the form of cryptographic functions i.e. mathematical equations that are solvable and can give a definitive analytical proof and not in the form of a developer who developed it (prone to human error) or any other means. So, for the first time in human existence, blockchain brings about a trust mechanism that is trustless. In other words, it is independent of where it resides and who operates it, as the trust mechanism is mathematically proven. This removes the need for human intervention in the system altogether. That is the major problem that blockchain solved for the world, which no one was able to solve before it.

HOW DOES A BLOCKCHAIN WORK?

Blockchain works mainly on the basis of hashing. Hashing is a technique used to map data of arbitrary size into a fixed size. Hashing is a one-way function. It means that once converted to a hash it is not possible to get back the previous data. Now this means that sharing of a hash of a password to anyone, it would not be possible to find the original password from it.

Hashing has a lot of advantages. It is used widely in password store where a database stores the hash of a person's password in a database, so even if the database is compromised, there is no actual leakage of confidential information to a third party. When requires the site can then hash the input password and check if it matches with the one in the database to let the user have access.

Some Properties of Hashing

Deterministic: This means that no matter how many times a single input is passed through a hash function, the output will always be the same. This is critical because if there is different output over time for the same input then it will be impossible to keep track of input.