Blockchain

Abstract

1 Introduction

2 Design and Implementation

Only relevant values of objects are hashed, does not provide redundant info

3 Test Results

4 Research

According to Wikipedia[1], a blockchain is a growing list of records, called blocks, that are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. The transaction data is generally represented as a Merkle tree, which allow efficient and secure verification of the contents of large data structures.

A blockchain can be used as a distributed ledger, as its design makes it resistant to data alteration. Each block being linked to the previous one by its cryptographic hash, modifying transaction data in one block would require a modification of every subsequent block, which requires consensus of the network majority. This design solves some of the long-standing problems of digital currencies without the need of a trusted authority.

The decentralized design of this system makes it secure by not having a central point of failure, whereas traditional databases may be subject to exploits because all the data is held centrally.

Blockchains can be permissionless (open), only requing new entries to include a proof of work. They can also be permissioned (private), in which case the access to the chain is restricted to authorized users only. Private blockchains do not benefit from the network advantages, and are closer in design to traditional databases.

To achieve overall reliability in blockhains, users rely on consensus protocols. These protocols dictate whether a new block is accepted in the chain or not. The most commonly used consensus protocols are Proof of Work (PoW) and Proof of Stake (PoS), which are described below.

The main idea behind Proof of Work is that the requester (of a service) must prove that it has performed a measurable effort in order to submit its request. In blockchain, this effort is to solve a Hascash-like[2] cryptographic puzzle. By solving such a puzzle, a user can prove that it has performed a computationally expensive task, which can be verified easily by the service provider. Let's take the Bitcoin blockchain as an example. In order to add a block to this chain, a network of users must "mine" it by discovering a nonce which, when hashed together with the current block, produces a hash value below the current target value. To do so, the users have no other choice than to bruteforce different nonces until the hash value begins with the necessary amount of zeros.

To add new blocks to the chain ... Bitcoin uses Hashcash puzzles, but with double SHA-256.

5 Discussion

6 Conclusion

References

[1] Wikipedia contributors. Blockchain — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Blockchain&oldid=921399625, 2019. [Online; accessed 23-October-2019].

[2] Adam Back et al. Hashcash-a denial of service counter-measure, 2002. URL http://www.hashcash.org/papers/hashcash.pdf. Accessed: 2019-10-23.
https://rosettacode.org/wiki/MD5/Implementation
https://www.ietf.org/rfc/rfc1321.txt
https://en.wikipedia.org/wiki/MD5