A Decentralized Currency & Document Time-Stamping System

Harsh Borkar, Prasann Viswanathan, Vipin Ochiramani

Disadvantages of Centralized Systems:

1. Lack of transparency provided to users
2. There is no way of checking if data has been mutated
3. The server node is a bottleneck for both security and speed
4. Scalability of the system is heavily limited by the server capabilities

The solution to all these problems is Blockchain.

Although inefficient, blockchains provide immutability and trust.
Blocks chained together, with their contents hashed provide immutability and majority nodes must agree on a common truth, providing trust in transactions

The proposed solution

- Decentralized system for timestamping documents
  - File hashes are stored so any modification in the files can easily be detected
  - Files get time stamped so file submission time is known
  - System is distributed so there is no single point of failure

- परम्परियम Cryptocurrency
  - Acts as incentives to encourage mining of blocks
  - Can be traded for monetary benefits in future versions

Blockchain Structure

- Nonce
- File Hash
- Transaction Hash
- Previous block’s Hash
- Timestamp
- Transaction Summary Block Hash
- Additional Data Field

User Model & Transactions

Users are required to have an account characterized by a 1024 bit RSA public key. They also have a 1024 bit RSA private key to sign transactions.

- Transactions may involve the transfer of coins or files
- Coin transactions require signing by the payer’s private key
- File transactions include the hash of files which are added to the block. They also need to be signed by the sender’s private key
- We store a transaction summary block. The structure describes all transaction details merged in one block utilising merkle tree data structure

Network Hierarchy

- Passive Node
  - Create transactions and do not participate in mining blocks
- Active Node
  - All functions of passive node and also mine blocks
- Sub-Head Node
  - All functions of active node and also verify newly generated blocks
- Head Node
  - All functions of Sub-Head node and assigns certificates to sub-Head nodes

Rules of Operation

- Difficulty of mining is the number of leading zeros in block’s hash and this is kept dynamic:-
  - increases by 1 if block generated in less than 60 seconds
  - decreases by 1 if block generated in more than 120 seconds
  - same in all other cases
- Computations stored : sum of difficulty of mining of all blocks in the blockchain.
  - blockchain with the greatest computations stored is considered as the valid chain.
- Small percentage of the coins transferred is removed as transaction tax.
- Miner nodes are rewarded for every new valid block generated in the network.

References

- "Bitcoin: A Peer-to-Peer Electronic Cash System," Jan. 30, 2014. Accessed on: March. 19, 2022. [Online]. Available: https://bitcoin.org/bitcoin.pdf
- R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980

Thank You