Blockchain

Money Transaction Security Blockchain Project

Shivam Vatshayan
Software Engineer
vatshayan007@gmailcom

CONTENT

1. ABSTRACT
2. BLOCKCHAIN
3. BLOCKS
4. REQUIREMENTS
5. PROCESS
6. CONCLUSION
7. REFERENCES

ABSTRACT

Many sectors, like finance, medicine, manufacturing, and education, use blockchain applications to profit from the unique bundle of characteristics of this technology. Blockchain technology (BT) promises benefits in trustability, collaboration, organization, identification, credibility, and transparency. In this project, we conduct an analysis in which we show how open science can benefit from this technology and its properties. For this, we determined the requirements of an open science ecosystem and compared them with the characteristics of BT to prove that the technology suits as an infrastructure. We will use Blockchain here for secure transactions of money between friends.

BLOCKCHAIN

A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger.

BLOCKS

Every chain consists of multiple blocks and each block has three basic elements:

The data in the block. A 32-bit whole number called a nonce. The nonce is randomly generated when a block is created, which then generates a block header hash. The hash is a 256-bit number wedded to the nonce. It must start with a huge number of zeroes (i.e., be extremely small). When the first block of a chain is created, a nonce generates the cryptographic hash. The data in the block is considered signed and forever tied to the nonce and hash unless it is mined.

REQUIREMENTS

Software Requirements:

Python IDE(Online/Offline)
* We will Mainly use Google Collab for better performance, easy execution and platform Independent.

Hardware Requirements:

Any Hardware as Mobile, Ipad, Laptop or Desktop will work

PROCESS

1. We will Write code on Google Collab
2. Will use libraries like import hashlib,json,sys
3. Create a function to generate exchanges between friends.
4. We'll construct our transactions to always be between the two users of our system, and make sure that the deposit is the same magnitude as the withdrawal- i.e. that we're neither created nor destroying money.
5. Now we will construct blocks

Continue to next page

Cont.

6. Next step: making our very own blocks! We'll take the first k transactions from the transaction buffer, and turn them into a block. Before we do that, we need to define a method for checking the validity of the transactions we've pulled into the block. We'll define our own, very simple set of rules which make sense for a basic token system: The sum of deposits and withdrawals must be 0 (tokens are neither created nor destroyed) A user's account must have sufficient funds to cover any withdrawals If either of these conditions are violated, we'll reject the transaction.

7. Each block contains a batch of transactions, a reference to the hash of the previous block (if block number is greater than 1), and a hash of its contents and the header

8. For each block, we want to collect a set of transactions, create a header, hash it, and add it to the chain

9. Now that we know how to create new blocks and link them together into a chain, let's define functions to check that new blocks are valid- and that the whole chain is valid.

CONCLUSION

We’ve created all the architecture for a blockchain, from a set of state transition rules to a method for creating blocks, to mechanisms for checking the validity of transactions, blocks, and the full chain. We can derive the system state from a downloaded copy of the blockchain, validate new blocks that we receive from the network, and create our own blocks. The system state that we’ve created is effectively a distributed ledger or database- the core of blockchain for secure transfer of money.

This is a new and unique way to develop a system for securing transactions. Third Parties, Attacks or any system will take a lot of time to crack this system. We can say it is tough to break the transactions.

REFERENCES

1. https://www.investopedia.com/terms/b/blockchain.asp
2. https://www.ibm.com/in-en/topics/what-is-blockchain
3. https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain
4. https://en.wikipedia.org/wiki/Blockchain
5. https://builtin.com/blockchain
6. https://www.pwc.com/us/en/industries/financial-services/fintech/bitcoin-blockchain-cryptocurrency.html

-Shivam Vatshayan-
Software Engineer
vatshayan007@gmailcom
https://www.cse-projects.com