CRYPTOGRAPHY PROJECT

Group Number 38

BITSCoin
A simple
blockchain wallet

WHAT IS BITCOIN?

As you may know, blockchain is a way of storing digital data. In BITSCoin, it's the transactions (logs of transfers of BITSCoins from one account to another). The data here is stored in the form of blocks, which are chained together using cryptographic hashes. Students at the start of each semester, get ₹12,000 worth of BITSCoins that they get to spend on outlets, merchandise and workshops. We can integrate this with the existing smart campus application to make the system more robust and dependable.

Functionality provided

- View Blockchain
- View All Transactions by a given user
- Add Block
- Mine Block
- VerifyBlock
- Check Balance
- Reject Transaction (if low balance)

Compulsory Functions

- CreateBlock(): This function is used to create new blocks.
- VerifyTransactions(): This function is used to verify a transaction before it can be added to the blockchain. Each transaction's validity is checked and then only block for that particular transaction is added to the blockchain.
- MineBlock(): This function is used to mine(search) blocks in a blockchain.
- ViewUser(): This function gives a list of all the completed transaction of a user.

Problems identified in the current system

- Our current smart campus systems have a centralized ledger, which stores all the digital transactions at a single location.

- This means that if any data is corrupted, the entire data is lost.

- A centralised database is quite expensive to maintain for the students because it involves setting up servers and databases. On the other hand, this system would not require a centralised server.

- The current system is not very secure and is prone to tampering etc.

Our idea

1. To counter this, we propose a blockchain based wallet which will be linked to the students’ other advances account .

2. This system provides increased transparency, reduced costs, improved accuracy and makes the system more robust.

BITCOIN · DIGITAL · DECENTRALIZED · PEER TO PEER
MONETARY METALS
MJB COPPER FINE 999 ZOYOXT

Security

Proof of work

In Proof of Work, in order for an actor to be elected as a leader and choose the next block to be added to the blockchain they have to find a solution to a particular mathematical problem. In our system, in order for a transaction to be confirmed, hash function is used. Each user produces blocks by solving this problem(hashing) and if it is approved by the consensus of the nodes,the block is added to the chain. It works so well due to its following properties:

- It is hard to find a solution for that given problem (the probability of getting a random success is very low).
- When given a solution to that problem it is easy to verify that it is correct

In the next slides, we will talk about why a blockchain based system is the best fit and what makes it so secure.

Prevention of tampering

One of the motivations behind this was the lack of security in the current system. To prevent any tampering with the transactional data, we try to detect any tampering using cryptographic hash functions(in our project, we are using SHA-256 hashing function. The consequence of this is that it becomes virtually impossible to guess the input(other than a brute force attack). Also, if the input and hash functions are known, one can simply pass the input through the hash function to verify.
This asymmetry allows us to get security without compromising much on the performance and is what is leveraged by Blockchain to obtain its properties.

Chaining

Although the individual blocks are now tamper free, an attacker could get around that by creating another block, computing its hash, and replacing it with the original. To ensure that this never happens, we create dependencies amongst consecutive blocks by chaining them with the hash of the previous block (include it’s hash to the Block). This ensures that the entire data is protected from tampering and helps improve the security of the system.

BITCOIN · DIGITAL · DECENTRALIZED · PEER TO PEER
MONETARY METALS
TROYOZ 999 FINE COPPER MJB

Advantages

- The vendors wouldn’t have to worry about maintaining their own database.
- Students wouldn’t have to deal with the payment issues because of bank servers.
- There would be a universal payment method in the campus that everybody uses which would make transactions simpler.
- It will help students keep track of their expenses.

LIMITATIONS

- Since, blockchain systems are slower and have a higher cost associated with storing the data, it might be an issue.
- There is a lack of a central authority in the system.
- A blockchain system represents a total shift away from the traditional ways of doing things. It places trust and authority in a decentralised network rather than in a powerful central institution which for most people, can be deeply unsettling.
- Although this application provides pseudo - anonymity, there is still a risk of privacy.

TEAM DETAILS :

1. ANUBHAV SAURAV 2017A7PS0135H
2. NILESH TIWARI 2017A7PS0212H
3. HARSHIT JAIN 2017A7PS0208H