Analysis of the Blockchain Protocol in Asynchronous Networks

By: Rafael Pass, Lior Seeman and Abhi Shelat

Presented By: Keshav Agarwal

What is a Blockchain?

- According to Google, a blockchain is a system in which a record of transactions made in bitcoin or another cryptocurrency are maintained across several computers that are linked in a peer-to-peer network.
- In this specific research paper, blockchain is defined as a chain of blocks that links to one another based on their previous hash values.
- In the real world, blockchain can be a ledger that records online transactions such as bitcoin.
- Blockchain ensures the integrity of a cryptocurrency by encrypting, validating, and recording transactions.
- For example, when you swipe your credit card, the charge has to go through the credit company or a bank. They have to confirm the transaction and then takes out money from the cardholder's account, and gives the money to the seller from whom the person bought the item from.

Problem Statement

- According to Nakamoto, his idea of the blockchain protocol has a “so-called permissionless setting .. -- anyone can join (or leave) the protocol execution, and the protocol instructions do not depend on the identities of the players.”
- Because of this permissionless setting, we have no way of knowing if the participants or players of the system are real people or not.
- Nowadays, people have to rely on third party applications to process transactions of any kind.
- With technology advancement, the buyer can pretend to have never purchased an item or the seller can pretend that they sent the item to the buyer.

Proposed Work

- In the research paper, Satoshi Nakamoto proposes to use bitcoin instead of relying on a third party.
- Nakamoto created a protocol that is used on a network with message delays. In this protocol, some users would receive a message whereas some users would not.
- Nakamoto's confirmed consistency suggests that all the users on the chain need to be honest or actual users that are not hiding their identity.
- In terms of bitcoin, that means the consistency verifies and ensures that the users are not spending their money multiple times on the same transaction.

My Implementation

- With Netbeans IDE 8.2, I was able to create a JAVA program that creates blocks and a blockchain.
- It creates blocks that has a digital signature, hash value, previous hash value, date / time, and the actual transaction.
- All of this goes through the SHA-256 Algorithm.
- After the hash algorithm completes, the program outputs the block hash values
- It also authenticates that the current hash value of the blocks and previous hash values are equal. If they are equal, it means the blocks have connected forming a blockchain.
- It also verifies that the actual blockchain is valid or not. It will not be valid if even if a single block in the program is not valid.

Blockchain Program - Essentials

```
/* In a blockchain, a block has a digital signature, a hash value for
for the current and previous block, the actual transaction, and a
date a time of the transaction to know when the transaction occurred.
All of these will be strings except for the Date/Time;
The digital signature and hash value will be public
But the date/time and the actual TXN will be private for the user's
privacy */

public class Block {
    public ArrayList<Block> blockchain = new ArrayList<Block>();
    public String DigitalSignature;                 // Digital signature
    public String HashValuePrev;                    // Hash value of the previous block
    private long DateTime;                          // Date + time of the transaction
    private String TXN;                             // TXN = Transaction
    private int nonce;                              // Arbitrary number to randomize hash values

    //Added an empty constructor to store all the information for the blockchain
    Block(){
    }
```

Blockchain Program - Get Values for Blocks

```
/* We need a previous hash value for the current or first block
For that, we need to create an empty non-real block */
Block(String Transaction, String PrevHashValue){
    this.HashValuePrev = PrevHashValue;   //Creates the Previous hash value of the block
    this.TXN = Transaction;               //Creates the transaction
    this.DateTime = createDateTime();     //Creates Date time in milliseconds
    this.DigitalSignature = makeTHEHASH();
}

// Get the current hash value for the current block in question
public String getTHEHASH(){
    return this.DigitalSignature;
}
// Get the previous hash value for the current / first block
public String getPreviousHashValue(){
    return this.HashValuePrev;
}
/* The transaction needs to have a date and time so the user knows
when the transaction occurred */
public long createDateTime(){
    Date BLKDate = new Date();
    long time = BLKDate.getTime();   // This will return the time in milliseconds
    return time;
}
```

Blockchain Program - Authenticate Hash Values

```
    public void addBlocktoChain(Block block){
     blockchain.add(block);                 // Add all blocks to the actual blockchain
}
    // Checks if the blockchain itself is valid or not
    public void Authenticate(){
        Block beforeBLK;        //Before and present hash values have to be equal
        Block presentBLK;
        int count = 0;           // Count the blocks
        for(int i = 1; i < blockchain.size(); i++){
            presentBLK = blockchain.get(i);
            beforeBLK = blockchain.get(i-1);
            if(presentBLK.getPreviousHashValue().equals(beforeBLK.makeTHEHASH())){
                System.out.println("Block " + i+ " Hash Value" + " = Block " + (i+1) + " Previous Hash Value");
                count++;
            }
            else{
                System.out.println("Block " + (i-1)+ " Hash Value" + " = Block " + i + " Previous Hash Value");
            }
        }

        // if all the blocks in the blockchain are valid, then the blockchain itself is valid */
        if(count == blockchain.size() - 1){
          System.out.println("\nBlockchain = VALID!");
        }
        else{
            System.out.println("Blockchain = NOT VALID!");
        }
    }
}
```

Results

```
run:
Block 1 Hash Value: eab92b4023c69080602e3fafeb9ec4da74a8be54679f61a96cf700d8c11d9d14
Block 2 Hash Value: c36251a83cf4808170d3ceca31e7e5c81570f266d06ec0824a4951daf3f9d832
Block 3 Hash Value: d46150afa777455c734a5d798a645a7b55ce64bbc93041f87720af5e744ccd66
Block 4 Hash Value: 883887fa58185081cfa6f0c160e296b5bd5d5ef8d2ef98d9a9d5c078eabc6f72
Block 5 Hash Value: c116d3ab594432b87aacb47d97a6ddb02e4ae0c06da2d5aa29d053efff1bbdf2
Block 1 Hash Value = Block 2 Previous Hash Value
Block 2 Hash Value = Block 3 Previous Hash Value
Block 3 Hash Value = Block 4 Previous Hash Value
Block 4 Hash Value = Block 5 Previous Hash Value

Blockchain = VALID!
BUILD SUCCESSFUL (total time: 0 seconds)
```

- The program has successfully displayed the hash values of each block and has also checked current hash value of the current block is equal to the previous hash value of the next block.
- The program also checks if the blockchain itself is valid or not. If the blockchain is not valid, the program will not output any of the hash values and will just output “Blockchain = NOT VALID!”
- If a user runs the program again and again, the hash values will change and the blockchain will still be valid. Because it makes sure that the current hash value and previous hash value are equal.

Conclusion

- In conclusion, Nakamoto invented the idea of the blockchain in 2008 to perform as a registry or log for all the transactions in the Bitcoin or cryptocurrency world.
- Bitcoin came around a long time before the idea of blockchain, around the 1980s.
- There can be many hackers out there in systems that may try to fool the systems to make people pay multiple times for a single transaction.
- This digital currency helped bring a new level of security in our world of technology trying to find more and more ways to encrypt and secure our personal transactions and information.
- Hopefully, with the idea of blockchain, it will create more opportunities to do just that.

References

- “Blockchain Definition.” *Bankrate*, https://www.bankrate.com/glossary/b/blockchain/.
- Pass, Rafael, et al. *Analysis of the Blockchain Protocol in Asynchronous Networks*.