Utilizing Block Chain Technology for trading goods

Daniyal Usman
COSC 4P03: Advanced Algorithms
Brock University
du11ph@brocku.ca

Abstract – **This paper describes my implementation of the Block Chain Technology. The goal of this project was to simulate a market that allows trading between users. To pursue this goal, I wanted to experiment with components that would still allow the Block Chain to be an incorruptible ledger but not necessarily follow its current implementation in the industry. The initial approach was to look at the possibility of a decentralized private ledger and the elimination of miners. Through the results, I was able to prove the implementation of a private ledger, but also the importance of miners towards the overall process. The simulation incorporating the Block Chain variant was implemented in Eclipse Neon Release (??) using JavaSE-1.8.**
Keywords – **Block Chain, Distributed Public Ledger, Miner, Bitcoin, BTC, Market Place, De-centralized structure, Peer-to-Peer**

1 INTRODUCTION

When it comes to the digital world, it is often difficult to come across an authentic copy. This is not an issue in the real-world because if I want give something to someone I can physically hand it to them, while in the virtual world I would make a copy and send them the copy, concluding in me still having possession of the virtual item. This wouldn't be an issue if we can just keep track of all the transactions that occur in a ledger and deduct accordingly. However, the problem now arises in the credibility of the said ledger. I aim to solve this problem with the use of Block Chain Technology and showcase my results with a simulation of a trading system which allows users to trade goods for crypto-currency.

2 BLOCK CHAIN TECHNOLOGY

The Block Chain Technology aims to implement computational security; it would be computationally expensive for anyone to corrupt the ledger. It manages this through the various components involved in its structure and process.

2.1 Block Chain

As a transaction is generated, it is verified through the Block Chain. The verification simply means that the user holds fair grounds towards issuing a particular transaction. For example, if Bob wishes to transfer four coins to Alice, it must be verified that Bob owns four coins to execute this transaction. A new block is created from the verified transaction(s) and the output of the previous block if it exists. The content inside the new block is then passed to the miners.

2.2 Miners

Once a miner receives the verified transaction(s) with the output of the previous block, it adds an integer to the content received and determines the block's output through a one-way algorithm (sha-256) by using the content as the input parameter. The miner iterates through all possible integer values until it receives an output with a particular amount of leading zeroes. This is a brute-force approach where it checks all integers from 0 to infinite until it receives the desired output. Once the integer has been determined, the miner passes this information back to the block where the content originated from. The block then adds the integer to its content and an output for that block is generated through the one-way algorithm (sha-256), which should contain a particular amount of leading zeroes. The entire block is now verified and can be added to the Block Chain.

2.3 De-Centralized Structure

The de-centralized structure is an essential component to the Block Chain Technology because it guarantees no single point of failure and further solidifies its computational security. Many entities are created that possess a copy of the Block Chain. As transactions are generated, they're verified through multiple Block Chains and as blocks are verified, they are added to all copies of the Block Chain.

2.4 Security

A single block in the Block Chain uses the previous block's output as part of it's content, and a block's output is mined until it includes a particular amount of leading zeroes. This process in itself adds a significant amount of computational security because any change in content would cause an output of a block to lose its condition of leading zeroes, which would also cause a change in content in all the following blocks. Since the de-centralized structure is also part of the Block Chain Technology, at the point of transaction, it would also need to verify with other entities holding the Block

Chain. This means that if an intrusion were to occur, it would need corrupt all the following blocks in a given Block Chain and all the other copies of the Block Chain simultaneously. Such a scenario is not very plausible.

3 INDUSTRY IMPLEMENTATIONS

Currently in the industry, Block Chain Technology implements its structure through a peer-to-peer network. It allows users to act as nodes, for which they hold a copy of the entire Block Chain and validate transactions as they come through. Users also partake in mining, where they find the required nonce once they receive the collection of transactions from the nodes. For the bitcoin implementation, the result from mining requires 15 leading zeroes. Since mining is the most computational expensive part of the overall process, financial reward in the form of crypto-currency is offered to the miner that can determine the correct nonce. The current reward for mining a bitcoin block is approximately 12.5 BTC and is halved every four years.
Some of the downfalls of this implementation of the Block Chain Technology is the fact that it uses the general public to validate transaction thus exposing possible sensitive information. Exposure to transactional information can limit this technology to be applied in other areas. The entire process also relies on the number of users who choose to run a node on their machine. Currently, there is no incentive provided for users to act as a node, resulting in a drop from 10,000 nodes to 7,000 nodes with in the last couple years.

4 SIMULATION AND CONCLUSION

For my simulation of a market place utilizing the Block Chain Technology, I decided to implement a different approach than the current industry implementations. I explored the possibility of implementing a private distributed ledger, where it keeps the fundamentals of having a de-centralized structure without using users as a resource. The main incentive behind this decision was to expand the capabilities of the Block Chain Technology in the case where it needs to hold sensitive information. Another reason for this decision was to remove the uncertainty in participation due to the lack of incentive. This implementation does still make use of utilizing users as a resource for mining, however, in order to keep the ledger private, the collection of transaction is encoded into a single output of the sha-256 algorithm. This allows the content of the transaction to be concealed from the miners as they mine for the nonce in return for a financial reward.

4.1 Purchasing Coins

Once a user logs in to the simulation, they can easily purchase coins with the press of a button Fig 4.1. This creates a new transaction where the user requests coins from the market. This transaction is then verified by the private servers that are initialized at the beginning of the simulation. The transaction is then encoded through the sha-256 algorithm and then sent to the miner with the inclusion of the previous block's output if it exists. The miner is only aware of the encoded transaction Fig 4.2 and then proceeds to mine for a nonce which concludes with an output of four leading zeroes. This information is then passed back to the private servers, where each servers forms its own block to add to its Block Chain Fig 4.3. If the block's output ends with four leading zeroes, this means that the block has been verified and sets its colour to green. The verified block then executes its transactions, updating the balance of everyone involved in the transaction and adding the transaction to their history Fig 4.1.

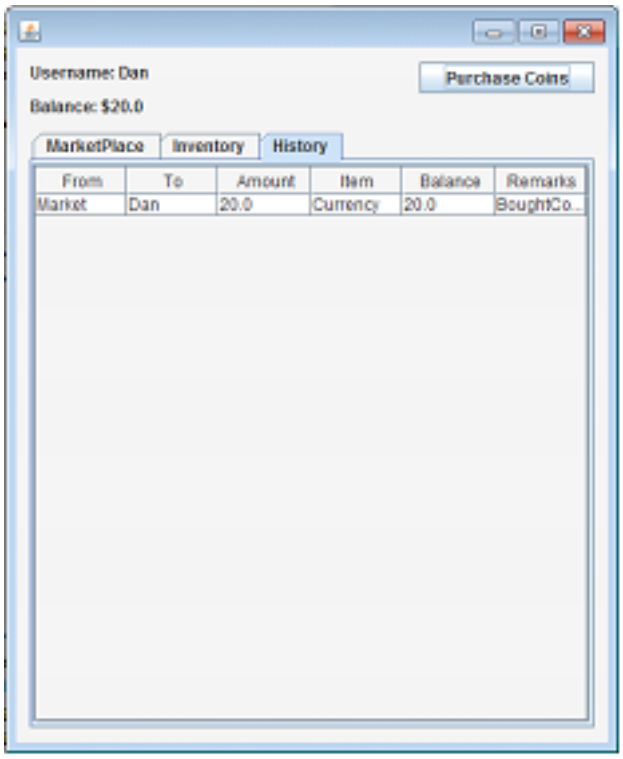

Fig 4.1 – User's History

Fig 4.2 – Miner's log

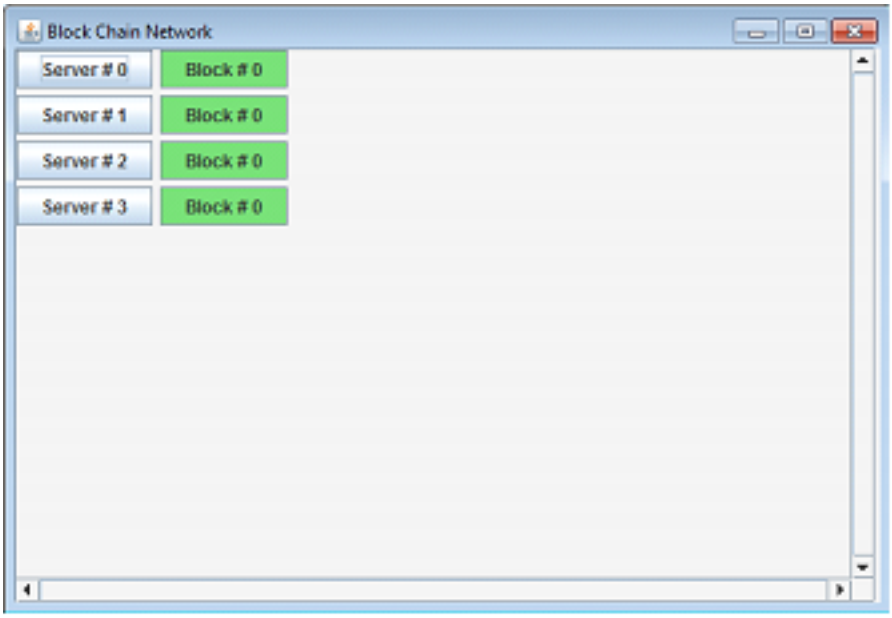

Fig 4.3 – Verified blocks in different copies of a Block Chain

4.2 Adding Items

Users also have the option of adding their items to the market for others to purchase. This feature can be used in the "Inventory" tab Fig 4.4. This transaction follows the same process as the one mentioned above. However, the execution of this transaction slightly differs. Since the transaction doesn't require the balance to be updated, it displays the added item in the user's inventory Fig 4.4. The user can choose to issue another transaction to delete the added item.

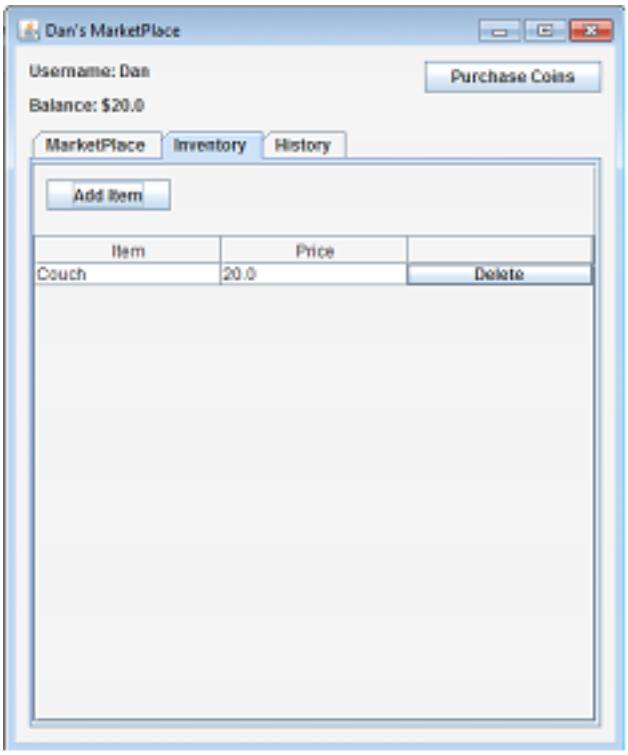

Fig 4.4 – Inventory Tab

4.3 Purchasing Item

The item added by one particular user will not be displayed in their "MarketPlace" tab since they already own the item. Another user would be able to view this item from their "MarketPlace" tab and can issue a transaction to purchase the particular item Fig 4.5. If the transaction to purchase a particular item is issued, the transaction would be verified by the private servers where they check to see if the user is in possession of the required funds to purchase the particular item. This transaction would consist of transferring coins from the purchaser to the seller. Once this transaction has been verified, another transaction is issued from the system where it removes the item from the Market Place to refrain other users from purchasing the same item Fig 4.6.

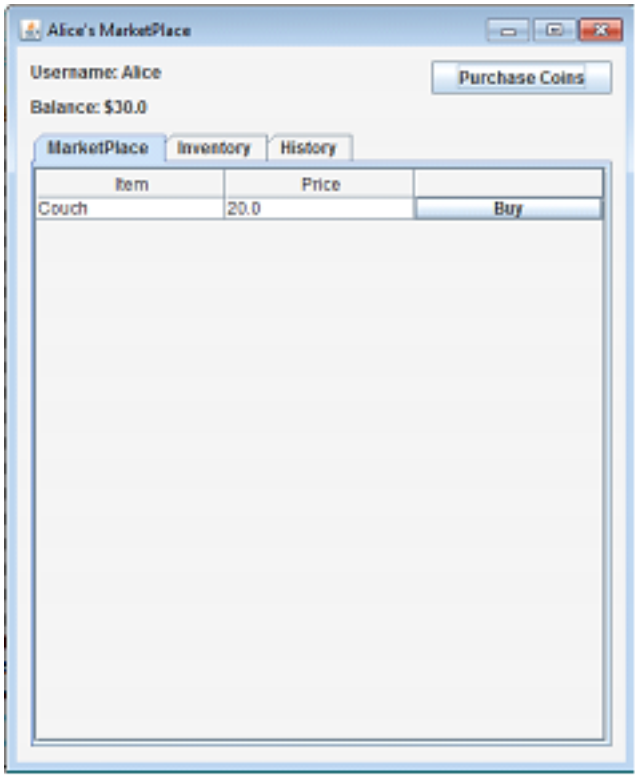

Fig 4.5 – Market Place

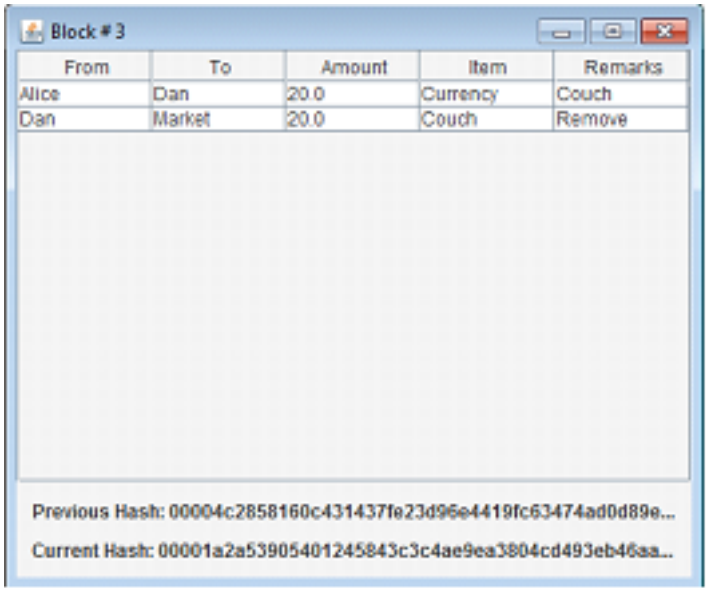

Fig 4.6 – Block # 3, removing purchased item from the market

4.4 Block Chain

It can be noted in Fig 4.7, as more blocks are added to the Block Chain. Output of the previous nodes are utilized to determine the output of the current node.

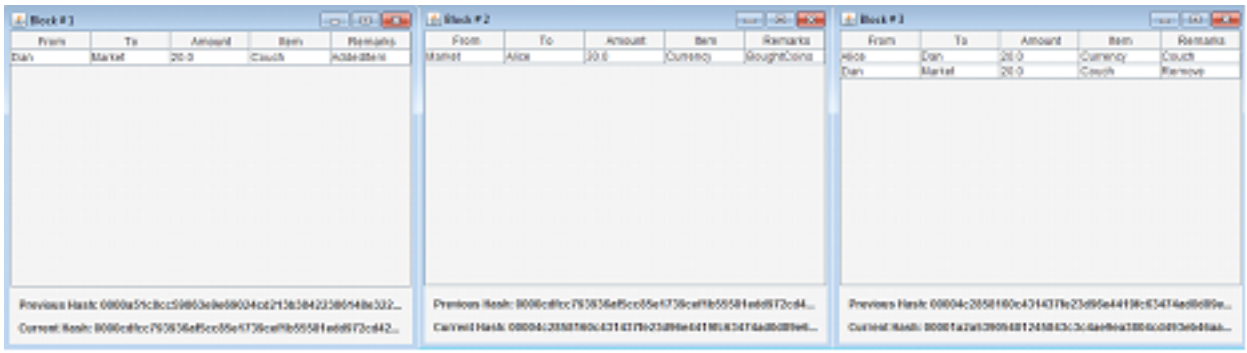

Fig 4.7 – Chain of blocks utilizing their previous hash outputs

4.5 Security

The static copies of the Block Chain for each server are stored in the "BlockChain" folder. If anything within the static copies of the Block Chain is altered, it will be immediately detected. Once its detected, it can be handled in many ways, however, for this simulation I chose to leave it unhandled to showcase the intrusion detection. In this particular case, the change from "Alice" to "Eve" was made in the second block Fig 4.9. The intrusion is immediately spotted, breaking all the affected blocks since their output doesn't end with four leading zeroes Fig 4.8. To simulate this error, it was required to execute transactions, close the program, change the text file and then restart the program.

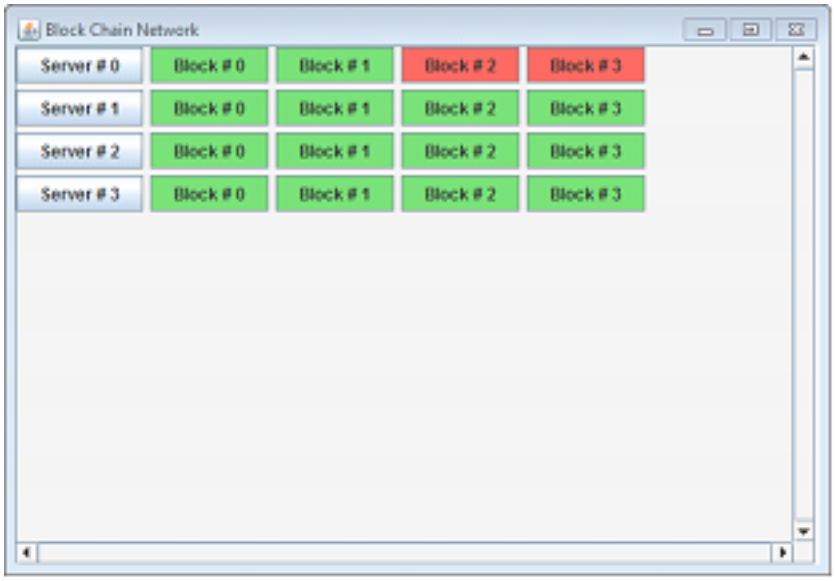

Fig 4.8 – Break in the Block Chain

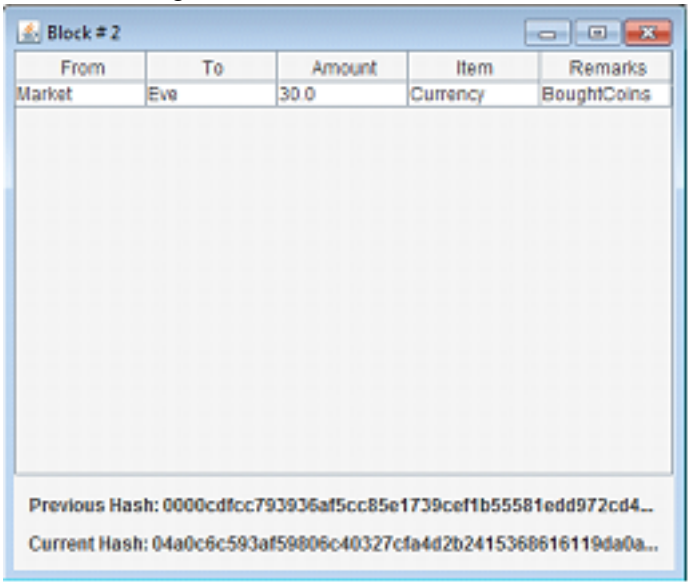

Fig 4.9 – Change in Block # 2

4.6 Future Work

My implementation of the Block Chain Technology did manage implement a private distributed ledger. However, I believe this technology can be further

utilized if the concept of miners were to be removed. As part of curiosity, I did experiment with removing the role of miners and insure authenticity through cross verification of Block Chains from different private servers. However, that approach didn't allow you to determine which individual Block Chain was the original Block Chain, when implementing the miners allows you to determine that with the use of leading zeroes. I would like to further explore the possibility of removing the extensive computation of the miner by implementing RSA as part of encoding instead of brute-forcing sha-256.

5 References

[1]https://blockgeeks.com/guides/what-is-blockchain-technology/
[2]http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/
[3]https://github.com/ethereum/wiki/wiki/White-Paper
[4]http://www.coindesk.com/bitcoin-nodes-need/