Academic Project – **Proof of concept for online peer-to-peer transactional Application using Blockchain. (By Suman Sourav)**

**Introduction:**

This report is an add-on to the demo that my team presented to the class (MSIS 512A Information Security taught by Mike Simon at Foster School of Business, University of Washington) and aims to describe the findings, improvements, and challenges that were faced while working on this project. The primary understanding of the technological nuances of blockchain was gathered from Satoshi Nakamoto’s white paper and from various other sources, which have been referenced below. The working code from [dvf](https://github.com/dvf/blockchain)( referenced below) was enhanced with this understanding. All references and citations are provided at the end.

**The Proof-of-concept(POC) and setup**:

The POC demo showed the micro-level technological aspects of how a P2P transactional app (like a de-centralized e-wallet) could play out on a blockchain. A distributed network of 3 peers (2 regular nodes and 1 miner’s node) was set up. Scenarios that started with making peers discover each other, peers claiming new transactions (asset transfers to other peers), a miner mining for that ‘proof-of-work’ followed by adding the transactions to the immutable blockchain and consensus based sharing of the chain(ledger) were explained in detail keeping in mind different states of the blockchain at each stage. The network infrastructure was set up on AWS EC2 instance and the front-end transactions were shown with the help of ‘Postman’. Supplementary set-up steps and ‘how to’ materials can be found in the ReadMe.md file on github.

**The objective:**

Our objective with the blockchain project was to help the class understand the steps that are at work in any blockchain based applications and this was achieved with an easy-to-understand proof-of-concept, which involved idea brainstorming, code study, concept understanding, code improvements and the demo infrastructure setup.

**The findings, enhancements and the future improvements:**

A behavior comparison of the reference code with the original white-paper was done. Issue logs of the dvf Github code base were read to identify issues with the existing code. With this research, the following problem statements were identified and a few of them were picked up for implementation:

|  |  |  |  |
| --- | --- | --- | --- |
| **Sl. No** | **Protocol Requirements** | **Reference Code** | **Our Improvements** |
| 1. | Miner should be able to discover transactions pending to be mined. | Requirement not implemented. | Implemented a transaction discovery feature in 2 phases:  1. Added end-point to nodes to provide requester a list of transactions when queried for. 2. Implemented a request-response based transaction discovery logic for the miner node to get a list of all pending transactions from the network using feature 1. |
| 2. | Chain should be immutable. | Requirement not implemented | Improved the hashing algorithm in proof-of-work(pow) logic and made necessary changes till the end points. The core change included adding previous hash to the pow algorithm. |

**Further Work:**

Given the constraints we had, all feature requirements of the blockchain protocol could not be implemented. However, with a detailed study several other improvement area as given below were discovered:

1. **Authenticated access**: ***Challenge:*** Our chain was accessible to all. ***Workaround:*** For the demo environment, we had selected IP whitelisting mechanism to prevent unauthorized access. ***Possible Solution:*** Implement a public-private key based mechanism to verify nodes’ accessing the network.
2. **Coin base Verification**: ***Challenge:*** User’s ability to spend and possibility of double-spends were not checked in the current implementation. ***Possible Solution:*** A coin-base check needs to be run at the creation of each transaction. However, this usually is done with actual cryptocurrency based blockchain (bitcoin, Ethereum, etc.) networks. It is complex to achieve this on off the network/ private chains!
3. **Transaction encryption:** ***Challenge:*** Transactions happening over the network used http protocol and were not encrypted. ***Possible Solution:*** The details of transactions (in our case: sender, recipient, amount and message and other critical fields of the block) should be encrypted with available >128bit key to maintain privacy.
4. **Race Condition Resolution:** ***Challenge:*** During our several runs, it was found that transactions were dropping out, especially when there were more than 1 miners in the network. ***Possible Solution:*** Implement ‘rule of democracy’ among miners to decide the authoritarian chain. Any transactions that are not part of the consensus based blockchain should be made available again for further mining**. This has been partially implemented now.**
5. **Automation: *Challenge:*** During our demo, we went under the hood to explain step by step processes and activities in a blockchain network with an intent to simplify it for the class’ comprehension. However, a blockchain node is not aware of all the sub-processes because many of these steps are automatically executing. ***Possible Solution:*** Automatic transaction mining, consensus, transaction discovery are some areas that need to be implemented using true two-way peer to peer communication frameworks like [web sockets](https://socket.io/)/ web real time communication([WebRTC](https://webrtc.org/)). The http (request-response – not truly automatic) based transport layer of the existing code could be replaced with either of these two secure protocols to support instant two-way communication for automatizing the mentioned points.

**Conclusion:**

The project taught us important aspects of the blockchain technology and exposed us to the aspects of software deployment, application of the technology to real world problems and translating requirements to relevant code. The key take ways from this project are the immutability, security and distributed network aspects of blockchain that makes it a disruptively applicable technology in the current era of Information Security (Cryptocurrency, Smart Contracts, Online Voting, P2P transaction tracking services, etc.).

**References:**

<https://hackernoon.com/learn-blockchains-by-building-one-117428612f46>

<https://medium.com/@rodkey/deploying-a-flask-application-on-aws-a72daba6bb80>

<https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-overview> - All the video lessons.

<https://bitcoin.org/bitcoin.pdf> - The full white paper.

<https://github.com/dvf/blockchain/issues/10>