PeerCoin

Austin Loza 9715590

March 4, 2018

Abstract

The main purpose is to be able to share small amounts of data from peer to peer without use of a server. On top of that, the blockchain should be capable of secure payments as well as capable of hosting some simple applications related to its previously stated purposes. Essentially, the person would pay a coin to get some data from a particular peer or a few coins along the way to get chunks from several peers, with the core of every request or application being a transaction of coins. To that end, there will be symmetric RSA encryption to secure the transaction between the two parties, and SHA-2 hashed "fingerprints" of past transactions to verify the chain. The "currency" aspect of this project is more like a fuel for receiving and isn't meant to be worth anything. The purpose of implementing a peer-to-peer file sharing network using a blockchain is to attempt to solve the problem of "leechers" in bittorrent.

Introduction

A blockchain is a distributed data structure made up of "blocks" that contain a hash of the previous block, a timestamp, and other data. This is usually implemented on a peer-to peer basis, where as transactions are made between peers, the chain increases in length. This allows every transaction to be verified and peers to be connected amongst themselves. Oftentimes this is used for secure and anonymous cryptocurrencies, where clients can exchange "coins" between anonymous addresses or create "contracts", as in the case of

Etherium, for compensation to be doled out when some task or set of tasks is completed.

Research Done

I have read the documentation for Bitcoin [1] and Etherium [2], as well as looked at some open-source implementations of cryptocurrencies on GitHub. Furthermore, I've looked into blogs [6] that explain how to build and generate peer-to-peer blockchains as well as papers outlining extensions to blockchains [3] [4]. Foundations for the use of blockchain as a transport layer for files and data have been laid by groups like Protocol Labs, the creators of Filecoin [8]. It's becoming ever clearer that the future of the internet will be found and possibly defined my blockchains and the unrealized potential they currently possess.

Implementation

I am basing my blockchain implementation on the structure of Bitcoin with some of Etherium's contract/application focus. Furthermore, I've looked into RSA encryption and implemented a small RSA pseudo-library myself for the purposes of securing the transactions. The data section of the blocks in my chain will contain pieces of files which can be distributed amongst the peers. This data may be whatever the client wishes to share with the rest of the network. Timestamps will be set in yyyy-mm-dd and hashes will be done using SHA-256 to get a good, secure "fingerprint" of the previous block. Coins themselves will be the "fuel" for file exchanges. Whenever a person hosts a file, that constitutes "mining" the blockchain. This "mining" is, in a sense, adding some form of value to the blockchain by giving computational power of some sort. (There will be other forms of mining to be added later.) The longer a file is hosted, the longer one mines the chain for coins. Additionally, whenever someone requests a file, all those who are distributing that particular file will receive payment from the requester. This payment will be split amongst the distributors according to how much of the file they provided.

Results

Currently the project is in too early a state of development to determine results. See comments below.

Comments

General Comments

I was a lot busier than expected this quarter, preventing me from making as much progress and with as many updates on this project as I would have liked. However, I will definitely be able to get this project to at least milestone three on my timeline below. Progress has been slow, but I'm still confident in my ability to finish the core of this project. Currently, RSA encryption and decryption with key generation is the only portion implemented. Hashing is currently in progress. Once the hasher has been completed (I insist on implementing the SHA algorithm myself), I will begin working on transactions and inter-node operations. By the time I've completed the second milestone, I believe the core of the project would be complete. The second milestone would contain a network simulation as a proof of concept for the networked implementation that would be created by the third milestone. The third milestone would be scaling things up into a real network, providing a method for these distributed nodes to connect to each other between different machines, plausibly even in different networks.

Deliverables

My deliverables will be source code and progress reports submitted as required as well as available on GitHub in a folder named ”Reports”

(Link: https://github.com/SystemicCypher/PeerCoin)

Timeline

The first milestone is to have a functioning CLI program that encrypts, decrypts, and hashes in the blockchain's format.

The second would be a CLI program that can send a payment into another instance of the CLI program, that decrypts it. (e.g a second node in the blockchain)

The third would be implementing the ability to share data along with payment between the computers in the network, utilizing this software. (distributed nodes)

The final would be providing a GUI for the program and refining the interactions with the blockchain.

Further refinements will be made if time permits.

References

1. Nakamoto, Satoshi Bitcoin: A Peer-to-Peer Electronic Cash System

   https://bitcoin.org/bitcoin.pdf

   (Used to gain understanding of cryptocurrency/blockchain implementation and functions.)

2. Wood, Gavin ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER

   http://gavwood.com/Paper.pdf

   (Used to gain a better understanding of cryptocurrency/blockchain implementation and functions along with the Bitcoin paper. I've based my project a bit more on this specification over Bitcoin's.)

3. Greenspan, Gideon

   MultiChain Private Blockchain - White Paper

   https://www.multichain.com/download/MultiChain-White-Paper.pdf

4. Back, Corallo, Dashjr, et al.

   Enabling Blockchain Innovations with Pegged Sidechains

   https://www.blockstream.com/sidechains.pdf

5. Okupski, Krzysztof

   Bitcoin Developer Reference

   http://enetium.com/resources/Bitcoin.pdf

6. Ecomunsing, Build Your Own Blockchain: A Python Tutorial, Blog

   http://ecomunsing.com/build-your-own-blockchain

7. Cohen, Bram
   The BitTorrent Protocol Specification
   http://bittorrent.org/beps/bep_0003.html

8. Filecoin: A Decentralized Data Storage Network
   https://filecoin.io/filecoin.pdf