Bilkent University
Department of Computer Engineering

CoinAMI
Coin Application Mediator Interface

Supervisor
Can Alkan

Members
Ahmet Kerim Şenol
Alper Gündoğdu
Halil İbrahim Özercan
Muhammed Yusuf Özkaya

Jury Members
Buğra Gedik
Cevdet Aykanat

Progress Report
October 9, 2014

Contents

1 Introduction

Cryptocurrencies lately acquired considerable attention from the public. First cryptocurrency was Bitcoin that was created in 2009 by an unknown person with pseudonym Satoshi Nakamoto[1]. Its aim was creating a distributed currency that is free from any controlling authority. Because of its success, other cryptocurrencies are proposed afterwards such as Litecoin[2] Peercoin[3] and Dogecoin[4] but power of their mining network is negligible compared to the Bitcoin's.

Bitcoin mining network's total computation power is 77.46 PetaHash/s[5]. In comparison, world's most powerful scientific computation grid BOINC (Berkeley Open Infrastructure for Network Computing) has a computation power of 7.54 PetaFLOP/s[6] because hashing uses integer operations and BOINC's power measured in floating point operations, even 1 to 10 scaling makes Bitcoin network as powerful as BOINC network. This computation power mainly used to maintain currency's integrity. We propose a system where this computation power will be used for scientific computation as well as integrity purposes. We chose genome sequence alignment problem for our initial proposal.

1.1 Description

In this project we aim to create a cryptocurrency system which uses DNA sequence alignment as proof-of-work.

Our system consists of 2 parts, Transactions and Mining. Transactions represent money exchange between two parties. Simply, they are records of participants, input amount and output amount. Every time a transaction occurs, the original (input) coins are destroyed and new (output) coins are generated. With this scheme, every coin can be spent only once. Transaction operation is handled by other peers in the network and these machines are awarded new coins.

Generation of a new block (coin) is called mining. To mine a coin users should solve an assignment that is assigned to them by the server. This assignment will be a small part of a DNA sequence aligment problem for 2 or more people, so that the user can not build an individual's genome from the assignment. When the user calculates the result for the assignment, the server will validate the result and grant the user a coin upon a succesful calculation.

1.2 Constraints

1.2.1 Testing of the system

Testing of the mining system does not require a large network as every peer should be running in the same manner. But the server should exchange DNA sequencing data and results with clients each time a transaction occur. So server's bandwidth could be a bottleneck during transactions.

1.2.2 Computational Power

Computational power is based on peer-to-peer network and size of network can change dynamically. Difficulty is calculated every 2016 blocks in Bitcoin system and we will be using the same system.

1.2.3 Social Constraints

We are trying to create a new cryptocurrency system and sequencing of the DNAs rely on size of the network and public usage of the cryptocurrency. So people should be using this to exchange money in order to achieve the system's initial purpose which is sequencing of the DNAs.

1.3 Professional and Ethical Issues

Due to nature of the project, DNAs will be sequenced by personal computers in a public and peer-to-peer network. So the DNA should not be reconstructible with the data we sent to clients because the DNA data is private.

Also the protocol can be reimplemented by other developers and the server can be deceived with wrong sequencing data. We also need to consider this possibility and avoid it by confirming some of the results that are received from client.

2 Requirements

2.1 Functional Requirements

1. The user should be able to make coin transactions.
2. The user should be able to earn coins through running the program.
3. People can create account and wallet id to use the system.
4. Server side administrator should be able to add new genome sequences to the system.
5. Server has to distribute the genome's content among users such that the divided content could not be rebuilt. This is needed to protect the human rights of genome owners.
6. Server should be able to distinguish any fake result from actually calculated results.
7. Server should be able to merge received data according to appropriate genome sequence.
8. Each completed genome data should be preserved correctly.

2.2 Non-functional Requirements

1. The validation of the results from user should take a small amount of time, not overwhelming the server side with validation process.
2. Transactions should be user friendly, efficient and simple so that user does not feel confused.

3 References

[1] https://bitcoin.org/bitcoin.pdf

[2] https://litecoin.org/

[3] http://peercoin.net/

[4] http://dogecoin.com/

[5] http://blockchain.info/stats

[6] http://boinc.berkeley.edu