Jaber A. H.

DEVELOPMENT OF A MODERN AND SIMPLE MINING PROGRAM

Vinnytsia National Technical University

Summary

A user-interface based desktop application that allows users to mine without any background knowledge on mining, cryptocurrency or even blockchain required.

Keywords: mining, cryptocurrency, blockchain, java desktop application.

Introduction

Our community today is gradually leaning forward towards a more simplified and decentralized economic system, but for many up until today mining is still considered to be a complex approach and requires a decent PC knowledge. My goal is to simplify and make this approach easy for all people with capable hardware using a user-friendly software and begin mining a pool with other miners. What's the difference between pooled and solo mining? Pooled mining "pools" all of the resources of the clients in that pool to generate the solution to a given block. When the pool solves a block, the coins generated by that block's solution is split and distributed between the pool's participants, while solo mining is when a miner performs the mining operations alone without joining a pool. All mined blocks are generated to the miner's credit. [1]

Research Analysis

By the year 2020 most casual PC users will've probably upgraded their rig and be acquainted with cryptocurrency which would qualify them to join in the mining process and populate mining pools to help others evolve this system, so an application like this would be of outmost convenience to be able to make money using their PC hash power whenever they're not using it. With the availability of tons of open source mining algorithms, I could build a complex system and combine them into a single user-friendly application. To dive deeper into those algorithms, we have to at least understand the process of mining itself.

To simplify the sketch of the mining process we need to see what problem we're facing and how it's being solved. Let's take a bitcoin mining example and cover a simple md5 hashing algorithm. So, let's say we have a hash of our latest block (e.g. 00000000000001adf44c7d69767585 – shortened to 30 chars) and hashes of a few valid transactions waiting for inclusion (5572eca4dd4 and db7d0c0b845) and a special transaction that we've crafted with a hash of 916d849af76. Now, let's use a gross approximation of what a new block might look like (the real one uses binary format). It contains the hash of the previous block and the hashes of those 3 transactions: 00000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-916d849af76--...

Now let's do mining by hand! Our goal is to complete this block with a nonce (a piece of garbage) such that the hash of the new block starts with 13 zeros (considering the previous hash, it seems that 13 zeroes is the current difficulty!).

First iteration:

Let's try with nonce=1, and compute the hash of the block (I'm using the md5 hash algorithm, but Bitcoin uses double sha256):

"00000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-916d849af76--1" | md5sum

8b9b994dcf57f8f90194d82e234b72ac

As we sees the hash does not start with a 0… So, it is needed to keep incrementing...

If we pursue until nonce=16, we get our first leading zero.

00000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-916d849af76--16" | md5sum

03b80c7a34b060b33dd8fbbece79cee3

For nonce=208, we get two leading zeroes.

00000000000001adf44c7d69767585--5572eca4dd4-db7d0c0b845-916d849af76--208" | md5sum

0055e55df5758517c9bed0981b52ce4a

Continue like this… If we finally find a hash that has 13 leading zeroes… That`s a good result. Other miners will now build upon our block, we've just got 25BTC.

If someone manages to build a block before we do, we'll have to start again from the beginning with the new block's hash (the one of the winners'). [2]

So, while we might not have that much of a chance to solo mine that block, we could join a mining pool to help each other solve the block, for example:

The mining pool coordinates the workers. Think of it like a lottery. If you and your friends all buy tickets in the lottery the group has a better chance of winning. To be fair in the lottery example everyone should be rewarded proportional to the amount of money spent on tickets. So, if there are 20 tickets for the pool one person purchased 10 and two people purchased 5 each - if one of the 20 tickets win the person who purchased 10 gets 50% and the other two get 25% each.

What a mining pool does is function as a coordinator for all the pool participants doing:

1.Taking the pool members hashes

2.Looking for block rewards

3.Recording how much work all the participants are doing

4.Assigning block rewards proportionally to participants

Miners mine differently by running pool software instead of the bitcoin client and just performing hashes for the pool. [3]

Solution

Originally, the problem was that there's way too much PC power not active globally when it could be benefiting society and its users, but another problem occurs is when not everybody has the chance. What I've decided to do is build an application that connects users to active mining pools and uses their PC power (hash) to mine and discover new blocks along with others on the network. With a constant expected share, the user will never fail to get a share out of a block where they gave away hashes for, thus, blocks will keep being discovered, users will keep getting payouts and the road to a fully decentralized network would get closer. So, with a software that's easy to use and a share solution that's already existent and evolving, the chances of growing the miners' community would be incredible.

So, for a small summary on what the project actually is; an application (java) that automatically detects the user's hardware components and tries to generate hash rates using different (existing) algorithms, then chooses the best (easiest to mine with highest hash rate) algorithm and connects to a mining pool and starts mining with other users, when the user starts mining actual data and starts sending transactions, he/she will be rewarded by the pool with a certain percentage of coins (depending on how they mined). This solution would be incredible provided an easy to use platform and a fair payout. With today's existing algorithm solutions and their evolving states, I believe that it is very likely for mining to become faster and easier in the near future.

Conclusion

In conclusion, I believe that our society should strive for a decentralized economic system and I believe that it would be the solution for many economic problems our society faces, thus why I am eager to be helping in the development process of this system. By creating a modernized mining utility, I would hope for an evolving mining community and the attention of a wide range of developers who would support such a project and help improve it. The goal is very simple, to "simplify mining" and have it become an "as easy as a phone call" kind of operation, and from there I'd continuously trial at making utilities that would be of ease of use to whoever catches interest in moving towards a decentralized system.

LIST OF USED LITERATURE

- [1] The Internet of Money (Andreas Antonopoulos)
- [2] Solo mining md5 iterations (Jacob Twif - reddit)
- [3] captainaltcoin.com/what-is-pool-mining/ (Admir Tulic)

Supervisor: **Yevhen A. *Palamarchuk.*** —Professor, Docent, Vinnytsia National Technical University, Vinnytsia