PARALLEL MINING IN BLOCKCHAIN FOR BITCOIN USING GAME THEORY

[1]Milind Tote, [2]Ankit Kumar, [3]Mayank Mahankal, [4]Siddhesh Khadse, [5]Vrushabh Uprikar
[1]Professor, [2]Student, [3]Student, [4]Student, [5]Student
[1]Department of Information Technology,
[1]Rajiv Gandhi College Of Engineering And Research, Nagpur, India

Abstract: *In this paper, we are focusing on Bitcoin and its parallel mining. Cryptocurrency mining has become a challenge for a new miner to get Bitcoin in form of reward by mining them. We use game theory to generate nonce value in efficient and faster way using multiple threads with the help of parallel mining. We showed difference between sequential mining and parallel mining. How parallel mining helps to increase the hash rate to mines new and valid blocks for the Bitcoin. We further improve this using parallel processing for mining the Bitcoin using multi-threading combined with game theory to improve the efficiency of mining.*

IndexTerms - Proof of work, cryptocurrency, Blockchain, Bitcoin, Game Theory, parallel processing, serial processing.

I. INTRODUCTION

Bitcoin was created in 2009, it is a digital currency. The main motive for creation of bitcoin is to arrive at an agreement in a valid transaction in a decentralized fashion. There are various agents in a bitcoin network which contribute to increase computational power resulting in secure and further expanding public ledger, the blockchain.

The agents in bitcoin network are rewarded in from of small amount of bitcoin depending upon the the computational effort they have contributed in the mining process. The major security framework in bitcoin is provided by "proof-of-work" process where a transaction is considered valid once the computer gets a assurance that a sufficient amount of computation work has been exert by the valid node. To get the desired output the agents in the network also Called as miners attempts to solve the cryptographic puzzle which are in the form of hash function.

The blockchain contains a set of various transaction occurring and each block in stored in a shared data structure (linked list). Mining is the process of adding a fresh block in the blockchain. The mining process occurs when a miner wants to mine a block they must study the in a large possibility space X, so that directly they can get an input $x \in X$ so that, when hashed alongside with various other block content using a crypt hash function h, which will result in value below a set threshold t so that $h(b(x)) < t$ (where b(x) denotes the block with value x inserted into it).

To motivate a participant for searching a valid input would result in discovering of hash and mining of a block. Then the block is released in the network and if majority of miner (depending on computation power) would treat this block to be valid and build more blocks on top of it. The miner who has mined that particular block id rewarded with bitcoin. An input x selected at Random from X has a very small probability of having a low value under the hash, denoted as $pt = P\ rx \in X(h(b(x)) < t)$.

The only base needed is an electronic payment system which should be in a crypt method which is useful instead of trust. This results in two parties to perform transaction within each other without a third party. Transaction that are fraudulent in nature and are impractically incomputable will save the seller from a fraud, with routine escrow frame will protect buyers and are easily implemented.

2. LITERATURE REVIEW

We have studied various mining pools in bitcoin using a Game Theory model for the help of formation of team and sharing of rewards. We told that protocol of bitcoin results in a pool reward based on the computational power given by the miner.

The investigation showed us that relative rewards for an agent in different pools combines a practical application of Game Theory in the framework of automation agent. Ht agents might make decisions about which pool they can join so to maximize their rewards.

When a new miner wants to join a mining pool so that they can mine a crypto currency, the miner needs to make a decision about which mining pool would be most profitable for them. This utility values depend on various parameter which are specific to various miners.

While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for nonreversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hashing them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

3. OBJECTIVES

With the combination of both background and personal motivation, we have come to the main purpose of this thesis. The thesis will focus to resolve and answer these two objectives:

a.Explain and understand in simplified terms the concept of Bitcoin, the blockchain and the details of Bitcoin ecosystem & transaction procedure through nodes, block, block mining and Proof of Work.

4. PROPOSED SYSTEM

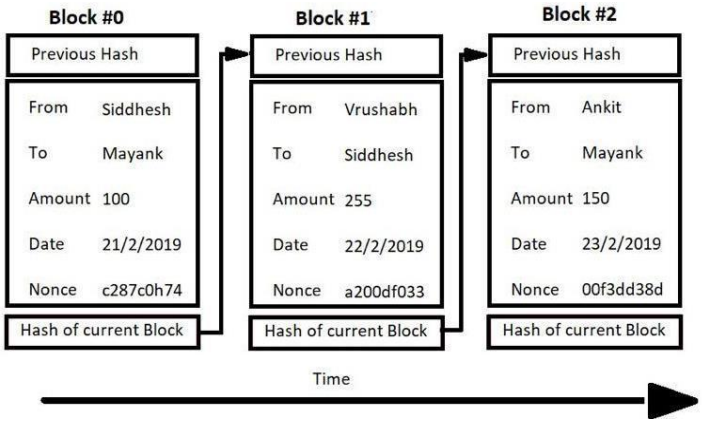
We start with a brief overview of bitcoin. It is a decentralized crypto-currency. Two agents participate in the bitcoin network: one client being the trader in the currency and other being the miner who validates fiscal transaction. By giving our total focus on interaction occurring among miners. The whole transaction history is stored on a shared data structure called as blockchain. Each block in a blockchain contains information of recent transaction which are valid.

The block formation resembles a form of tree and is rooted at genesis root created by the bitcoin inception with every block being the child of the first block and a reference in its header. Mining of a block is the process of adding a new block in the blockchain. A block is considered to be valid when the hash value in the header is less than the threshold value t. The nonce value is utilized later to make changes in the hash's result so that the value of't' can be satisfied. Random search method is best suited to find the appropriate value of nonce field. A miner is an agent that continuously tries to mine blocks. When more hashes a miner is able to compute per time unit, the more likely they are likely to mine a next mine. When a miner mines a valid block, they publishes it to the Bitcoin network; if the block is eventually extended and is part of the longest chain, its creator is rewarded with Bitcoin.

A fixed reward is assumed for every block is mined. Probability of a single hash based on random nonce results in a valid block is extremely low and the number of blocks mined per time unit by a miner can be roughly related as a Poisson process. A path form a child block to the genesis block is a chain in the block tree. In the bitcoin protocol the longest chain is considered to be valid. When a transaction is not recorded in a block that is present in the longest chain is not considered valid. Miners are only rewarded for the block in the longest chain so that they are given an incentive to motivate the miners for extending the longest chain

5. METHODOLOGY

For occurrence of dummy transactions we need to build a blockchain model. Transaction will to done in order to evaluate the creativity of the model. We would generate various block using different nonce value in order a final constrained block as per the blockchain model can be generated. Then the block can be generated using game theory approach and evaluation of performance can be evaluated. Multi-Threading tools are used for creation and generation of blocks in order to improve the performance of the system



6. BLOCKS

Data is permanently recorded in the Bitcoin network through files called blocks. A block is a record of some or all of the most recent Bitcoin transitions that have not yet been recorded in any prior blocks. Blocks are linked in a chain of transaction verifications called a blockchain used to prevent double-spending (refer to Chapter 3). Outstanding transactions get bundled into a block and are verified roughly every ten minutes on average. Each subsequent block strengthens the verification of previous blocks. Each block contains one or more transactions. Reward is given to a miner, who has successfully hashed a transaction block. This can be a mixture of coins and transaction fees, depending on the policy used by the cryptocurrency and whether all of the coins have already been successfully mined. Bitcoin currently awards 25 Bitcoins for each block. The block reward halves when a certain number of blocks have been mined. In Bitcoin's case, the threshold is every 210,000 blocks. New blocks are created by a process of mining.

7. HASH FUNCTION

Hash function is a computer algorithm which takes an arbitrary amount of input data and deterministically produces fixed length output, known as the data's "hash," that can be used to easily verify that data has not been altered. If you change any single bit of the original data and run the hash algorithm, the hash will completely change. Because the hash is seemingly random, it is prohibitively difficult to try to produce a specific hash by changing the data that is being hashed. Hash is the output of a hash function. The hash rate is the measuring unit of the processing power of the Bitcoin network. The Bitcoin network must make intensive mathematical operations for security purposes. When the network reached a hash rate of 10 Th/s, it meant it could make ten trillion calculations per second.

8. Mining

Mining is defined in the protocol, implemented in software, and is an essential function in managing the Bitcoin network. Mining verifies transactions, prevents double-spending, collects transaction fees and creates the money supply. Mining also protects the network by piling tons of processing power on top of past transactions.

Mining verifies transactions by evaluating them against the transactions that happened before. Transactions cannot spend bitcoins that do not exist or that were spent before. They must send bitcoins to valid addresses and adhere to every rule defined by the protocol.

With a frequency that is targeted at every 10 minutes, mining creates new blocks from the latest transactions and produces the amount of bitcoins defined by the current block reward (50 BTC until late 2012). Miners also verify blocks produced by other miners to allow the entire network to continue building on the blockchain.

a) Serial mining: A process of mining in which a miner is serially computing hashes to satisfy the certain rule to generate particular type of hash on the basis of nonce that signifies how much number of 0's will be in the prefix or postfix of the hash and that hash will be termed as low input hash which satisfies the given conditions or rule. Serial mining consumes more time to generate the results and the mean delay is also high due to its sequential processing. Sequential mining will have decreased pools mining efficiency.

b) Parallel mining: Parallel mining is the process where several different threads are engaged in a competitive way to achieve the low input hashes and then generated hash is only accepted when it's the unique and new and is not repeated earlier and all of this hash is compared with the central list where it has the record of all previously generated and accepted hashes, after satisfying the given rule the hash will be added and new block will be included in blockchain, the more threads are engaged the more faster the results will be generated and it will consume less time and the efficiency will be improved accordingly. If applied in distributed systems the efficiency will increase and faster processing can be achieved and the pools mining efficiency will be increased using parallel mining.

9. PROOF OF WORK

Mining is a process in which people use computer hardware to complete a complex 11 mathematical calculation autonomously for the cryptocurrency network to confirm transactions and increase security. It authenticates the wealth transfer as sales takes place, or money is sent from one wallet to another. For all intents and purposes is a digital signature hidden behind code that authenticates the originator and the recipient of the transaction that has taken place. The mining hardware must solve an algorithm to create a block that is the unit of data containing pieces of currency, and that occurrence is then verified by other miners. A lock is solved about every ten minutes on average, with slight variance as an increasing or decreeing amount of computational power comes online. As a result, the complexity of the problem varies with the cumulative amount of computational power of the cryptocurrency network. As a reward for their services, Bitcoin miners can collect transaction fees for the transactions they confirm, along with newly created Bitcoins. Mining is a specialised and competitive market where the rewards are divided up according to how much calculation is done. Today mining is done in pools where a bunch of people combine their processing power to uncover these blocks of data. So the stronger hardware that can try the most numbers before it is unlocked gives the most of the bounty. But everybody who put work in gives a little bit of the bounty. It depends on how much processing power you added to the pool.

Proof-of-work has been dominating the peer-to-peer cryptocurrency design since the early 2009 when Bitcoin was created by Satoshi Nakamoto. It provides initial minting and security for cryptocurrency network system. Miners use their hash rate to find valid blocks and build the blockchain exactly as with the pure PoW system. It is a random process to produce a proof-of-work with low probability so that a lot of trial and error is made on average before a valid proof-of-work is generated. The most widely used proof-of-work scheme is SHA-256, which was introduced by Bitcoin . 12 The proof-of-work solves the problem of determining representation in majority decision making. The majority decision is represented by the longest chain, which has the greatest amount of proof-of-work effort invested in it. If the majority of CPU power is controlled by honest nodes, the honest chain will grow fast and outpace any competing chains.

10. CONCLUSION

After comparing Serial mining and Parallel mining, we can find that parallel mining is more efficient and requires less computational power as the mean delay required is not as much of Serial mining. As in Serial mining, a miner serially generates hash function to satisfy a certain rule. As in parallel mining several threads are engaged in a competitive way so that a low hash function can be achieved if and only if the generated hash function is unique and not repeated in the decentralized list.

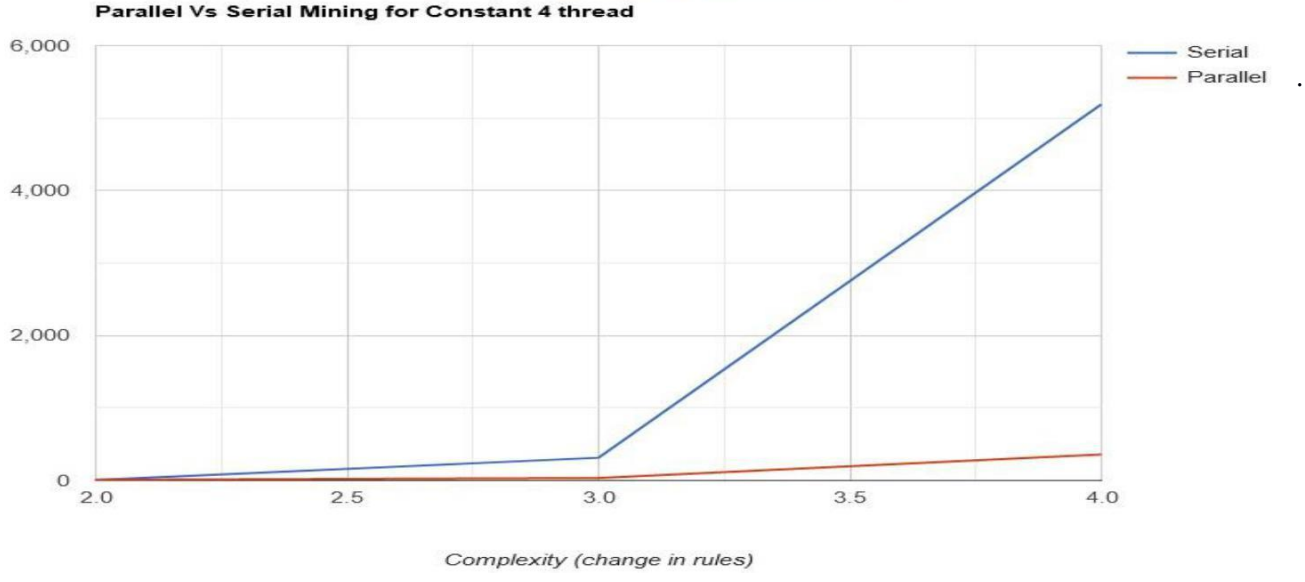


Fig1:- Parallel vs Serial mining for constant thread. Over here we can see that serial mining takes a lot of computational power and requires a lot of time to give an output. While Parallel mining gives output much quicker.

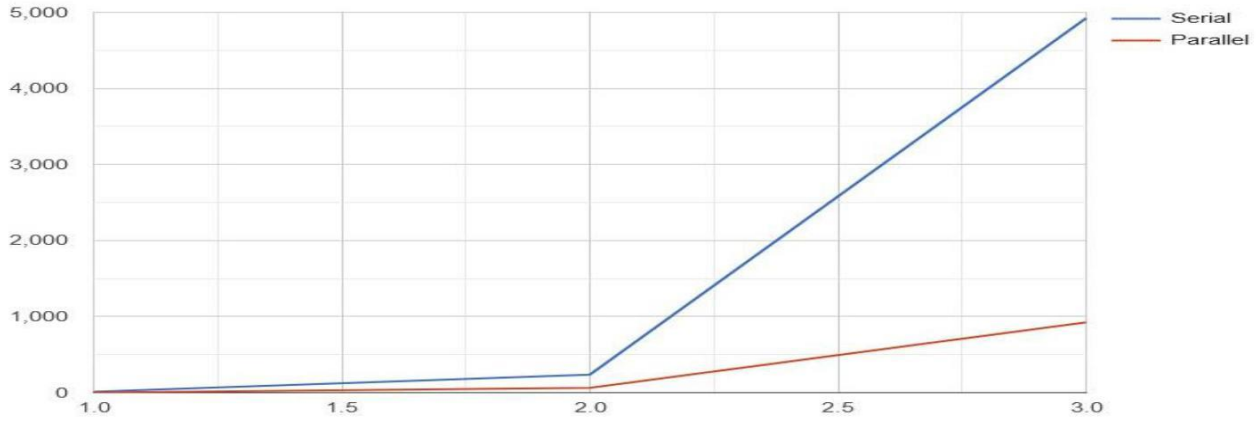


Fig2:- Parallel vs Serial mining for constant transaction. Over here we can see that serial mining takes a lot of computational power and requires a lot of time to give an output. While Parallel mining gives output much quicker.

11. ACKNOWLEDGEMENT

I would like to thank my guide Prof Milind Tote who supported me through the different phases of the project. Also, I am grateful to Rajiv Gandhi College of Engineering and Research for providing me the resources which led to successful implementation of the project.

12. REFERENCES

I. Lam, P.N., and D.K.C. LEE. "Introduction to Bitcoin." Handbook of Digital Currency, edited by D.K.C. Lee, pp. 5-30. San Diego: Elsevier, 2015.

II. Nirupama, D.B., and D.K.C. LEE. "Bitcoin Mining Technology." Handbook of Digital Currency, edited by D.K.C. Lee, pp. 45-65. San Diego: Elsevier, 2015.

III. Ong, B., T.M. Lee, L. Guo, and D.K.C. LEE. "Evaluating the Potential of Alternative Cryptocurrencies." Handbook of Digital Currency, edited by D.K.C. Lee, pp. 81-135. San Diego: Elsevier, 2015.

IV. Trimborn, S., and W.K. Härdle. "CRIX an Index for Blockchain Based Currencies." Working paper, 2016. http://crix .hu-berlin.de/data/CRIXpaper.pdf.

V. Trimborn, S., M. Li, and W.K. Härdle. "Investing with Cryptocurrencies—A Liquidity Constrained Investment Approach." 2017. https://papers.ssrn.com/sol3/papers .cfm?abstract_id=2999782