Indian Journal of Cryptography and Network Security (IJCNS)
ISSN: 2582-9238 (Online), Volume-1 Issue-1, May 2021

A Reward Based-Approach to Secure Blockchain Mining Pools from Selfish Miners

Kondisetty Sai Venkata Kowshik, Amanolla Harish Reddy, Vankadara Naga Nikhil, Judy Flavia

Abstract: ***People who create new blocks and process transactions on decentralized blockchain systems like Bitcoin, Ethereum etc., are known as miners. They are rewarded for processing the transactions and creating new blocks. Mining in blockchains requires high computation power. Mining is a resource intrinsic process and is associated with high operating costs. To overcome high operating costs, many miners across the world pool in their resources to process blocks in blockchain, the reward obtained from mining is shared among the miners based on their share of work and resource pooled into the common pool.***

Key Words: ***They Are Rewarded For Processing The Transactions And Creating New Blocks.***

I. INTRODUCTION

Some of the Attacks on miners, such as BWH (Block Withholding) and FAW (Fork After Withholding), give attackers an unfair advantage over the efforts of honest miners. When submitting shares, attackers retain their share of the block and appear to be contributing to the victim's shared capital.

The framework proposes an algorithm that enforces equal mining by leveraging important system parameters in applications of blockchain. To identify selfish mining behavior, the discrepancy between two heights that are expected transaction confirmation height and the block publishing height is used, and a network-wide method to revoke selfish-miners' rewards is implemented. Our scheme requires a minor adjustment to the transaction's data structure to obtain a "fact state" that can distinguish between a trustworthy and a greedy miner.

The design of our proposed system is based on a combination of already existing prior solutions, this provides a more effective defense mechanism. Our model is tested under various conditions and attack modes. Our proposed system is effective in detecting unfair practices by miners.

Manuscript received on 10 April 2021 | Revised Manuscript received on 20 April 2021 | Manuscript Accepted on 15 May 2021 | Manuscript published on 30 May 2021.

* Correspondence Author

Kondisetty Sai Venkata Kowshik*, Department of Computer-Science and Engineeering, SRM Institute of Science and Technology, Chennai

Amanolla Harish Reddy, Department of Computer-Science and Engineeering, SRM Institute of Science and Technology, Chennai

Vankadara Naga Nikhil, Department of Computer-Science and Engineeering, SRM Institute of Science and Technology, Chennai

Judy Flavia, Department of Computer-Science and Engineeering, SRM Institute of Science and Technology, Chennai

II. EXISTING SYSTEM

In the current scheme, a reputation-based method is used for PoW (Proof of Work) computation in the blockchain. In this system miners are paid their share of work based on ethical practices. Based on this theory, a game-based design is created to award honest miners, thereby increasing the revenue of the pool. Our proposed mechanism is supported with numerical and illustration data. Reputation mechanisms along with other designs can be used to reward honest miners and ethical practices.

A pool manager is appointed to analyze fluctuations in the reputation of each miner in the group. Higher the fluctuations, more likely the miner is involved in unfair practices. Based on the difference in the reputation levels at different intervals and fluctuations, the manager rewards the miner. The miner's reputation level fluctuation is also utilized as a parameter to let him join the pool group.

Because the resource of Proof of Work computation is restricted, miners engage in some nefarious activities during the competition mining phase. These malicious actions can waste distributed computation resources, putting blockchain network efficiency at risk.

We devise a trustworthy method for limiting miners' malicious activities, in which the miners' behavior history is elucidated, allowing miners to present honest mining.

III. PROPOSED SYSTEM

When two miners discover and send blocks that are valid at the same time, then the blockchain network splits due to networking and synchronization issues. Fork refers to this form of dispute. By mining a new block on the top of previous one a fork is resolved, which results in one chain that is longer than the other. Both miners should agree on the chain increment due to forking resolution, according to the protocol. Since there is high fluctuation in the rewards for solo-mining, miners usually pool their resources into a common pool and divide work among themselves. Reward for mining is based on their share of work in block transactions. Since the incentive is distributed based on individual members' contributions to the mining pool, in PoW, requires a method to track each miner's mining power and contributions.

IV. HARDWARE&SOFTWARE REQUIREMENTS

Hardware	Min Requirement
Disk space	32GB or more
Processor	1.4 GHz 64bit
Memory	512 MB
Display	(800X600)Capable video adapter

Software:

Back-end technologies:

=>Python

=>NumPy

=>Sci-learn

=>Eclipse IDE

Front-end Technologies:

=>Web Technologies

=>Bootstrap

V. ALGORITHM

The workflow of the algorithm is as follows:

• Basically, in a blockchain-network, every miner will try to construct an empty block- header which includes a previous block hash, the miner's public address, an index of the current block, and a nonce.

• The node will deliver the empty block header to the blockchain network after producing one that fulfils the current difficulty requirements.

The header of such kind of a block is treated as the data received from the pseudo-random owners, by all the nodes in the network. A follow-the-Satoshi algorithm is used to pick stakeholders using a hash of the block header which is sent and a hash of the preceding block+N presets.

• The validity of the empty block header is verified by everyone whoever is online at that time. Everyone who received the header will verify if they are one of the first N-1 lucky stakeholders in this block throughout the validation. If this is the case, then they use a secret key to sign the empty block header and submit it to the blockchain network.

VI. PROJECT MODULES

Exploratory data analysis:

Exploratory data analysis is of two types. Each method in the first method is either graphical or non-graphical. The second method is multivariate or univariate. As the name implies, a graphical method is used to summarize data from diagrams or illustrations. Calculations of summary statistics are involved in a non-graphical way. Univariate analyses one data variable (like data column) at a time whereas multivariate is involved in multiple variables at a time. Generally multivariate is involved with one or two data objects hence it is known as bivariate. Sometimes more than two objects are also involved in multivariate. Before performing a multivariate EDA, it is virtually always a good idea to run the univariate EDA on each of the multivariate EDA's components.

Data visualization is a methodology that uses a variety of statistics and interactive graphics to help people understand large sets of data. The information is often presented in a narrative style, which highlights patterns, trends, and associations that would otherwise go unnoticed.

Preprocessing:

Observation errors in large sets of data cannot be ignored as they can affect the result in a negative way. A continuous chain of steps and processing are done on datasets to reduce the effect of observation errors, this chain of steps is known as preprocessing and it is a very crucial step. The sample is divided into intervals, with categorical values replacing the intervals. Indicator variables: Indicator variables are used to transform categorical data into boolean values. We must construct n-1 columns if we have more than two values (n). By subtracting the mean from all values, we can center the data of a single function. We should divide the centered function by the standard deviation to scale the results.

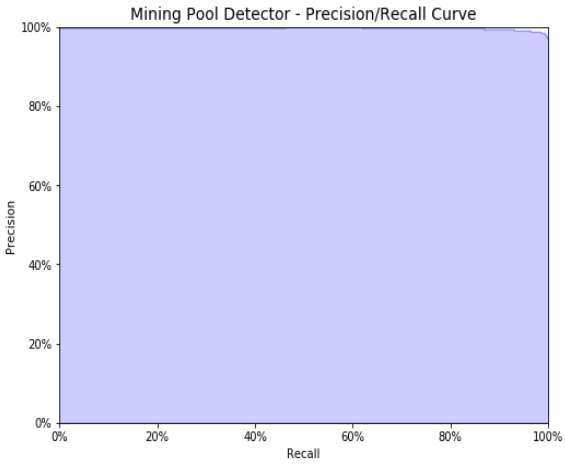
Prediction:

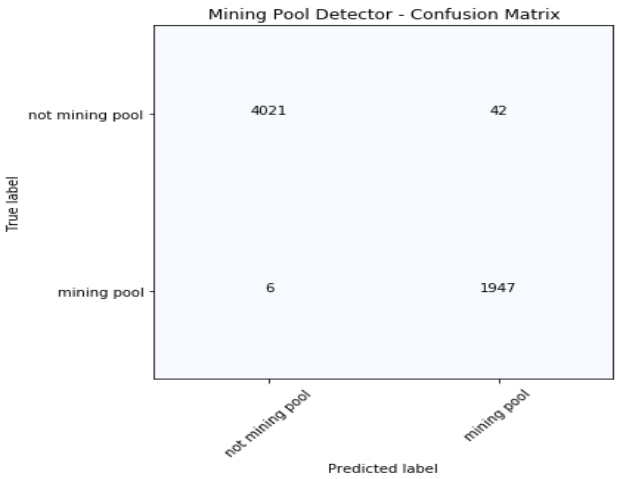
A set of prediction trees makes up the random forest classifier. Random vectors are sampled separately for each tree. This classifier was originally created for machine learning applications, but it has since gained popularity in the remote sensing community. Due to the high accuracy of this classifier, it is applied in remote, sensory image classification and other related projects. Random samples with the highest vote for prediction are selected for classifier. The uniqueness of the trees is crucial in the process. Because of the qualities mentioned below, each tree is guaranteed to be unique. To begin, each tree in the sample is trained using random subsets of the initial training samples. Second, the optimal split is chosen from the randomly selected features of the unpruned tree nodes. Finally, no tree should be pruned because it grows at its own pace.

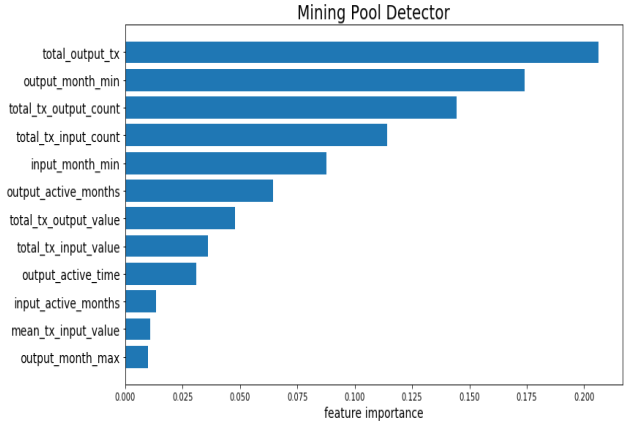
VII. CONCLUSION

The proposed system defines a mechanism to identify and block selfish-mining attack on pooled blockchain mining communities. Selfish attacks by unethical miners are done to maximize rewards and minimize operational costs, these attacks result in denial of rewards for honest miners. A confirmed height is assigned to each transaction on the block to identify attacks. Our proposed system effectively and efficiently deters selfish attacks in the community and encourages honest miners by making sure they get their reward for the work done by them. In the future, we want to assess the fee overhead associated with attaching the predicted confirmation height to every transaction, as well as the processing overhead associated with applying our methodology at the software client. Because of the cumulative advantages, many miners prefer to be truthful when using the credibility mechanism. This scheme proposes a reputation-based framework for incentivizing rational miners to mine ethically.

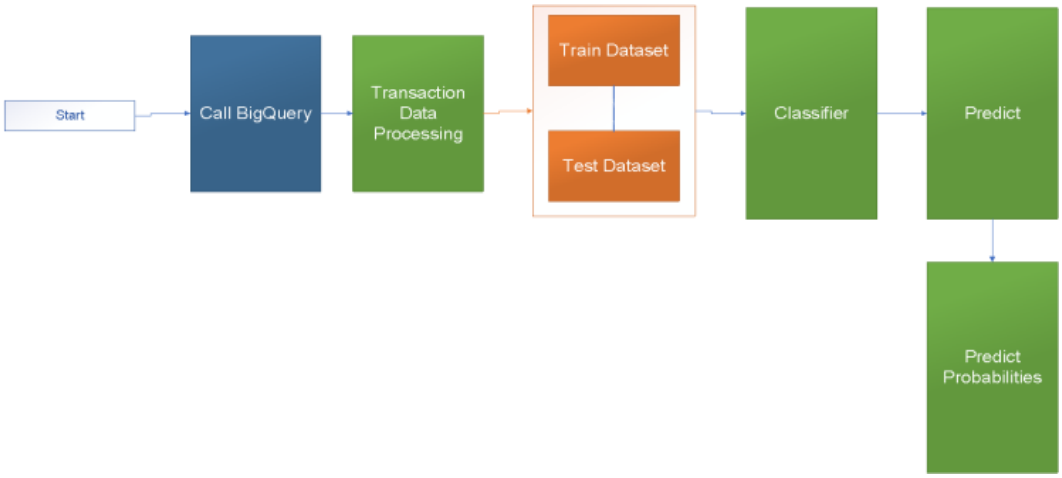
DIAGRAMS







ARCHITECTURE DIAGRAM



REFERENCES

1. Y. Zhang, R. Deng, J. Shu, K. Yang, and D. Zheng, "TKSE: trustworthy keyword search over encrypted data with two-side verifiability via blockchain," IEEE Access, vol. 6, pp. 31077-31087, 2018
2. YA. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. Anyigor Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," IEEE Internet Things J., vol. 4, no. 6, pp. 1832-1843, 2017
3. Y. Zhao, et al., "Secure pub-sub: Blockchain-based fair payment with reputation for reliable cyber physical systems," IEEE Access, vol. 6, pp. 12295-12303, 2018
4. D K. Tosh, et al., "Security implications of blockchain cloud with analysis of block withholding attack," in Proc. 17th IEEE/ACM Int. Symp. Cluster, Cloud and Grid Computing, Madrid, Spain, pp. 458-467, May 14-17, 2017.
5. Eyal, "The miner's dilemma," in Proc. 2015 IEEE Symp. Security and Privacy, San Jose, CA, USA, pp. 89-103, May 17-21, 2015
6. K. Nayak, S. Kumar, A. Miller, and E. Shi, "Stubborn mining: generalizing selfish mining and combining with an eclipse attack," in 2016 IEEE European Symp. Security and Privacy, Saarbrucken, Germany, pp. 305-320, Mar. 21-24, 2016.