Shawn Feleppa

Research Domain

Cryptocurrency has become a leading topic on the technological front ever since the inception of bitcoin has turned people's ideas on digital currency and decentralization on its head. Whereas previously the thought of a purely digital currency was thought to be vulnerable and fraught with risk and the lack of a centralized banking system to govern, protect, and insure it left people uncertain and fearful. However, cryptocurrency has proven resilient and viable as a potential alternate currency as we move away from the physical society of yesteryear and into a more and more digital landscape where every transaction and interaction can be done remotely from a terminal or smartphone. For this reason, I have decided to focus on blockchain technologies for my research project, looking into its securities, vulnerabilities and the public trust surrounding it.

Hypothesis

In order to handle all the calculations in creating the blocks that make up blockchain, Ethereum uses a method of trusting the one that did the most work. This method makes it difficult for fraud because you would have to own 51% of the processing power of the entire blockchain in order to alter the block and control the transaction records. However, since it also trusts the longest chain, you would also have to keep this up indefinitely otherwise another miner would eventually surpass you for the longest chain and the record would be corrected. This makes it possible but mostly infeasible to exploit with two notable exceptions. Exception one would be a state sponsored effort to undermine blockchain, whether to destroy public trust in the technology or devalue a particular crypto coin, by taking control of the blockchain and adding in fraudulent transactions or dropping valid transactions until confidence was lost. Exception two would be a more subtle state sponsored effort where they took control but did not commit any obvious fraud, performing shadow transactions and controlling the cryptocurrency from behind the scenes.
To combat these vulnerabilities, I hypothesize that changing the method of evaluation from the one that did the most work being the trusted chain to a more collaborative effort where we compare multiple high performers. I believe if we looked at the top 10 of the most worked miners and compare the data and results, this way, even if the top one is fraudulent, it is likely the majority of the others remain valid. In order to defraud this system, I believe you would need to control 5 of the top 10 performers, meaning you cannot put all your resources behind one hive of miners. You would instead have to split your overall processing power five ways and ensure all five of those divisions reach the top 10 in the amount of work achieved. This method would make it far more difficult for any one entity to control the entire blockchain.

Related Research

Many different blockchain protocols use a system known as Proof-of-Work (PoW). PoW is a method of keeping track of transactions and preventing double spend issues without the need of a central entity or leader to keep track of all transactions or the value each wallet contains. Using the PoW algorithm, the "ledger" is shared among everyone and the longest, most complete "chain" is the accepted true ledger. The reason being that everyone competes to compute the next block so the only way to defraud the PoW algorithm is by possessing 51% of the processing power of all miners on the chain.

As a known issue, referred to as the 51% attack, there have been multiple attempts to mitigate this problem. Such as using machine learning[4][6] to detect attacks or incorporating an additional step like Proof-of-Stake[3]. Some previous methods have shown some merit yet may introduce new risks. For example, the Proof-of-Work with a historical weighted difficulty[11] has shown to increase the difficulty of a 51% attack by two orders of magnitude but requires the history of the miner to be known, potentially risking the privacy of the miner. The table below, compiled by [1] shows several methods proposed by various researchers with a summary of their advantages and risks. The approach I seek to investigate will look at a collective of top miners and trust the majority consensus.

[1]

Technique	Advantage	Risks	Vulnerability Identification	Cost	Underlying Blockchain
2-hop Blockchain - [3]	Even if a malicious node manages to control more than 50 hash rate, honest nodes may still defend the blockchain through honest participation	higher centralization and resource consumption	May not identify the vulnerability in advance	Its implementation may involve a cost	TwinsCoin
Encoder-decoder deep learning mode - [4]	Use of a sequence-to-sequence neural network model to recognize anomalous changes in the Blockchain network	Wrong detection	Detects anomalous situations and trigger an alert	Its implementation may involve a cost	Any Blockchain with sequential data
Proof of work based on historical weighted difficulty (HWD-PoW) - [11]	Increase the cost of the attack by two orders of magnitude	Not efective against a slow gradual increase of hash rate and may affect the privacy and security of miners	May not identify the vulnerability in advance	Its implementation may involve a cost	Blockchain based on Proof of Work (PoW)
Methodology with intelligent software agents - [6]	Implement an intelligent agent in the application layer of the blockchain network system	Wrongly deducts the level of importance of the product	May identify the vulnerability before it is adopted by the main chain	It is just a proposed methodology	Blockchain based on Proof of Work (PoW)
Delayed block sending penalty - [12]	It forces the attacker to privately mine a large number of consecutive blocks before being able to join the main chain, consequently carrying out the attack is much more expensive	Not enough to completely mitigate the attack, it is a very weak solution for a cryptocurrency with low hashing	May identify the vulnerability before it is adopted by the main chain	It does not require, the technique is a prototype	Blockchain based on Proof of Work (PoW)
Delayed proof of work (DPoW) - [13]	Ignore the longest chain rule, the use of notarial nodes adds security to the protocol	A malicious node with at least 51% hash rate could execute an attack within the notarial period	May not identify the vulnerability in advance	There is a cost to adopt this technique	Any blockchain based on Unspent transaction output (UTXO)
PirlGuard - [14]	Employ a penalty system for attack nodes	Using master nodes for notarization weakens the network due to a single point of failure	Identify vulnerability as soon as it is recognized	Its implementation may involve a cost	Blockchain based on Ethash Algorithm
ChainLocks - [15]	Very fast transaction confirmation	Confirmation with a single block may enable double-spending with a low hash rate	Lock the first block as a legitimate block, discarding any other blocks	Require a cost for its implementation	Dash CryptoCurrency
Merged Mining - [16]	Merge the hashing power of two blockchains, making the attack more costly	A malicious node with a high hash rate may perform an attack	May not identify the vulnerability in advance	No cost for implementation	Auxiliary Proof of Work (PoW)
Proof of Adjourn - [2]	offer sufficient protection to the network regardless of the hash rate of the attackers. shorter confirmation time for very large transactions	Participants with ample hash rate may get an advantage through the mining process	May identify the vulnerability before it is adopted by the main chain	It is a proposal, a proof of concept was made	Any blockchain based on Unspent transaction output (UTXO)

References

[1] F. A. Aponte-Novoa, A. L. S. Orozco, R. Villanueva-Polanco and P. Wightman, "The 51% Attack on Blockchains: A Mining Behavior Study," in IEEE Access, vol. 9, pp. 140549-140564, 2021, doi: 10.1109/ACCESS.2021.3119291.

[2] S. Sayeed and H. Marco-Gisbert, “Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack,” *Applied Sciences*, vol. 9, no. 9, p. 1788, Apr. 2019.

[3] T. Duong, L. Fan and H.-S. Zhou, "2-hop blockchain: Combining proof-of-work and proof-of-stake securely", *Proc. 25th Eur. Symp. Res. Comput. Secur. (ESORICS)*, pp. 697-712, Sep. 2020, [online] Available: https://eprint.iacr.org/2016/716.pdf.

[4] F. Scicchitano, A. Liguori, M. Guarascio, E. Ritacco and G. Manco, "A deep learning approach for detecting security attacks on blockchain", *Proc. CEUR Workshop*, vol. 2597, pp. 212-222, 2020.

[5] K. O'Shea and R. Nash, "An introduction to convolutional neural networks", *arXiv:1511.08458*, 2015, [online] Available: https://arxiv.org/abs/1511.08458.

[6] S. Dey, "Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work", *arXiv:1806.05477*, 2018, [online] Available: http://arxiv.org/abs/1806.05477.

[7] H. Chen, M. Pendleton, L. Njilla, and S. Xu, “A survey on Ethereum Systems Security,” *ACM Computing Surveys*, vol. 53, no. 3, pp. 1–43, 2020.

[8] R. Zhang, R. Xue, and L. Liu, “Security and privacy on Blockchain,” ACM Computing Surveys, vol. 52, no. 3, pp. 1–34, 2019.

[9] I.C. Lin and T.C. Liao, “A Survey of Blockchain Security Issues and Challenges,” International Journal of Network Security, vol. 19, no. 5, pp. 653–659, Sep. 2017.

[10] J. Park and J. Park, “Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions,” Symmetry, vol. 9, no. 8, p. 164, Aug. 2017.

[11] X. Yang, Y. Chen and X. Chen, "Effective scheme against 51% attack on proof-of-work blockchain with history weighted information", Proc. IEEE Int. Conf. Blockchain (Blockchain), pp. 261-265, Jul. 2019.

[12] A. Garoffolo, P. Stabilini, R. Vigliano and U. Stav, Proposal to Modify Satoshi Consensus to Enhance Protection Against 51% Attack, 2018, [online] Available: https://www.horizen.global/assets/files/A-Penalty-System-for-Delayed-Block-Submission-by-Horizen.pdf.

[13] Blockchain Security and How to Mitigate, Feb. 2021, [online] Available: https://medium.com/chainzilla/solutions-to-51-attacks-and-double-spending-71526be4bb86.

[14] R. Minchev, PirlGuard—Innovative Solution Against 51% Attacks, 2018, [online] Available: https://medium.com/pirl/pirlguard-innovative-solution-against-51-attacks-87dd45aa1109.

[15] A. Block, Mitigating 51% Attacks With LLMQ-Based Chainlocks | by Alexander Block | Dash Blog, Nov. 2018, [online] Available: https://blog.dash.org/mitigating-51-attacks-with-llmq-based-chainlocks-7266aa648ec9.

[16] What is Merged Mining—Bitcoin & Namecoin—Litecoin & Dogecoin?, 2015, [online] Available: https://www.cryptocompare.com/mining/guides/what-is-merged-mining-bitcoin-namecoin-litecoin-dogecoin/.