

Analysis of Ethereum Ghost Protocol under Blockchain Framework

Baixi Wu

College of Science and Mathematics, University of Massachusetts Boston, Boston, United States

baixi.wu001@umb.edu

Abstract. This article discusses Ethereum Ghost Protocol, a technology that promises faster mining speeds. The Ghost protocol enables different crypto miners to create valid blocks concurrently. The article explains why the protocol reduces the delay in traditional blockchains through stale or uncle blocks. It explains why the Ghost Protocol is faster than Bitcoin. It also introduces areas in which Ethereum Ghost Protocol can work, such as insecure environments and Internet of Things (IoT). Besides, the paper defines centralization bias and explains how the Ghost Protocol solves the problem. Since the Ghost Protocol is decentralized and stores information in multiple nodes, it is more secure. Besides, it is scalable and saves storage space. Despite these benefits, this paper discusses two significant challenges, including slow transactions and difficulties in coding. However, the Ghost protocol will enhance cryptocurrency due to the ease of mining, enhanced security, and other benefits to miners. Overall, the paper suggests the need to embrace the Ghost protocol in the blockchain.

Keywords: Ethereum Ghost Protocol, centralization, centralization bias, blockchain, Ethereum.

1. Introduction

Distributed Ledger Technology has disrupted traditional transaction methods. It necessitates no central authority for sharing, synchronizing, and registering digital transactions [1]. Blockchain technology, notably Ethereum's Ghost Protocol, has changed many application domains. The Ghost Protocol is a decentralized and open platform that leads various blockchains [2, 3]. In this protocol, transactions are more accessible and transparent due to increased mining power when someone creates blocks with links to the primary chain [3]. In this system, the stale blocks are known as uncle blocks [4].

Ethereum introduced the Ghost protocol in 2013 to address the problem of blockchains suffering from many stale blocks. This platform eventually casts off the stale blocks based on their importance. Besides, the Ghost protocol addresses centralization bias, which results from the inability to choose faster blocks. These promises created an interest in exploring the Ghost protocol. Therefore, this paper seeks to understand whether the promised benefits are realistic and whether miners should trust the platform. It looks at how the Ghost protocol facilitates crypto mining. It explores the different ways that the framework reduces the delay in traditional blockchains. It compares Ethereum under this protocol with other cryptocurrencies, notably Bitcoin. It looks at how the GHOST protocol addresses the network security problem due to faster block generation time. It describes the different applications of the Ghost protocol and how the technology solves the centralization bias. It also examines the current challenges of Ethereum, including being slow in transactions and coding challenges. It evaluates the contributions and impact of the Ghost protocol on cryptocurrency. Overall, the paper provides insight into the Ghost protocol and why one might choose Ethereum as the most preferred option. Furthermore, the paper helps potential miners make an informed decision regarding the protocol.

2. Definition of Ethereum Ghost Protocol

In Ethereum's Greedy Heaviest Observed Subtree (Ghost) protocol, all the involved fork blocks ensure the system is more secure. However, the protocol does not consider all the info in the block

tree [5]. This makes retrieval and finalization of transactions faster. Making a chain block takes about fourteen seconds, implying that many different crypto miners can create valid blocks concurrently. This potentially leaves many stale blocks. The GHOST rules help select the most significant subtree as the primary tree, increasing the cumulative block difficulty. The main chain contains no stale blocks. However, Ethereum rewards them with the regular ones [2, 6]. This has an advantage for all crypto miners.

3. Transactions executed by Ghost Protocol based on blockchain

The GHOST protocol allows faster processing of transactions through the blockchain. The mining rate increases to one block per 15 seconds from one block per 10 minutes that was the case in conventional blockchains. This framework reduces the delay in traditional blockchains using references to uncles or orphan blocks. The uncle blocks are valid but do not become part of the main chain to eliminate delays caused by the longest chain's weight. Consequently, every new block links to previous uncles, creating an incentive for all crypto miners in the chain due to references' rewards. In this sense, faulty miners are discouraged from making long-range attacks or mining on forked chains [1].

4. Speed comparison between Ghost Protocol and Bitcoin

Unlike in the Ghost protocol, where minors greedily follow the heavier or most significant subtree, Bitcoin miner often choose a complex chain as the primary chain. This implies that a GHOST and a Bitcoin miner may follow an entirely different primary chain for the same subtree. Besides, it implies less difficulty in the case of Ghost protocol to mine [7].

5. Ethereum Ghost Protocol Usage

5.1. High-risk Situations

Several uncle blocks are maintained in the primary chain in the GHOST protocol, but they become stale. This is a mechanism to reduce the time spent in creating a block. The protocol is similar to a tree. The GHOST protocol eliminates the network security problem because of quicker block generation time [8]. It improves the bitcoin protocol that reduces confirmation time, slowing down the transactions [9]. Besides, the system maintains a higher security threshold than older blockchain protocols. The speed is higher even in network delays. It is possible to create new blocks faster without fear of attacks. This ensures high and more secure transaction rates [10].

5.2. Internet of Things

Due to its efficiency, the Ghost protocol can be used on the IoT. This can achieve faster results in manufacturing and industrial applications, such as supply chain management, remote machine diagnostics, manufacturing automation, and industrial machines' prognostic health management. One can also use the protocol in cloud-based manufacturing that leverages IoT technologies. It allows access to manufacturing resources on demand. It facilitates transactions between the manufacturing service users [11].

6. Centralization Bias and Examples

It is often difficult to maintain a blockchain with a standardized protocol. Whenever there are changes in the blockchain's operation, most crypto miners in the network must adhere to the newly proposed protocol, which does not always happen [12]. Centralization often occurs in a network initially intended to be decentralized. The crypto miners trust the network pool operators and expect honest returns after mining a block. However, the network operator might behave dishonestly,

creating a bias in centralization [13]. Centralized blockchain nodes have shorter propagation times for created blocks. However, a larger hash rate increases the time spent, making the mining process on the primary chain difficult [13]. According to the study of Neitz in 2020 [14], blockchain centralization leaves crucial decision-making to a small number of corporations or people. These agents might influence the blockchain, creating a bias.

7. Advantages of Ghost Protocol in Solving Centralization Bias

7.1. Added Security Linked to Trust Levels

The GHOST protocol uses Coordination Blockchain to enable crypto miners to locate information using domain names. This system creates different trust relationships and levels. Additionally, it provides a decentralized and secure means for storing information that is accessible and categorizable through the use of domains, trust levels, and relationships. This helps overcome the problems with the previous technologies that did not have measures to ensure censorship resistance and security [4].

7.2. Ghost Protocol is difficult to exploit

Since the Ghost Protocol's information remains in multiple nodes and is not centralized, it is not vulnerable to exploitation, making it more difficult for the attackers to exploit the system. Even though the uncle blocks do not contribute to this security, crypto miners who create them get rewarded, further discouraging centralization. Besides, Ethereum accepts only seven uncle block generations, preventing numerous calculations. This increases the importance of the primary chain [15, 16]. The more a miner moves from the main chain, the more difficult it becomes to find a valid block. This encourages minors to stick to essential blocks [13].

7.3. Ability to account for the blocks quickly

The GHOST protocol offers forty times more superior performance than Bitcoin [7]. It is also more secure because it accounts for all the blocks in multiple subtrees. Thus, attackers cannot penetrate the network quickly. Cases of double-spend attacks also reduce in this network [17, 18].

8. Other Advantages of Ethereum Ghost Protocol

8.1. Scalability

Crypto miners on the Ghost network stick to the sub tree with the most blocks rather than the highest branch. However, the network must confirm and accept new blocks. Scalability occurs because the system categorizes the blocks for approval, which offers an advantage over the Bitcoin blockchain that adds new transaction blocks after nearly every ten minutes [19]. GHOST makes mainchain determination faster by permitting block parallelism, scaling up the network [18].

8.2. Reduced Storage

Since the Ghost protocol keeps track of essential blocks, the entire blockchain is not needed for validation. Ghost keeps track of only the reasonable blocks, unlike the Bitcoin blockchain, reducing the need to store the whole blockchain. State Tree Pruning allows partial storage, saving on storage [13].

9. The Positive Impact of Ethereum Ghost Protocol on Cryptocurrency

The Ghost protocol ensures efficiency in cryptocurrency use. It rewards crypto miners more and puts them in more control. It saves time and hassle associated with considering the entire blockchain. It is more secure, reducing the risk of losses. Thus, Ethereum has become more secure, efficient, and accessible owing to this protocol.

10. Current challenges of Ethereum

Many people have experienced the challenge of a slow Ethereum network. Recently, crypto miners have complained about the Ethereum network because transactions take hours or days to complete. The network often jams up with transactions, disappointing many users. Reportedly, the problem originates from the Ethereum Tether version (USDT-ETH), which accounts for 25 to 50 percent of the network's usage. In September 2019, the blockchain received at least 100,000 Tether transactions in seven hours. Regrettably, Ethereum has not enhanced its "gas limit" to help increase the block size. Compared to Bitcoin that has a block size of between 1 and 2MB every 10 minutes, Ethereum has an 800kb block size for the same time. Gas is a measuring unit of the blockchain's work per transaction [20].

Ethereum transactions have become very slow. Ethereum reportedly carries out thirteen transactions every second. Meanwhile, the daily estimated demand for transactions nears 1.355 million transactions per second. Compared to other payment processors like Mastercard Incorporated and Visa Inc, Ethereum is slow. It is also slower than many other cryptocurrencies, particularly the new ones. According to The Value Trend in 2021, the people managing Ethereum have been trying to create solutions to this problem through updates [21]. However, Ethereum can only opt for Proof-of-Stake in place of Proof-of-Work, a challenging approach. Prove-of-work consumes massive electricity units, which makes it unfriendly to the environment. Proof-of-Stake is costly but would help address this challenge.

Another challenge with Ethereum relates to coding. According to The Value Trend in 2021, Ethereum consists of newly introduced intelligent contracts running on the network [22]. This introduction implies the ability to program virtually anything in Ethereum, from video games to finance applications. Different applications running on the Ethereum Virtual Machine imply that developers must use the Solidity language, its limitations. For instance, Solidity has intrinsic security issues, and only a few programmers are familiar with it.

Micky News in 2021 explains that many developers experience challenges with Ethereum's congestion, particularly for those engaged in cutting-edge applications or projects whose services are time-sensitive [23]. The developers have to pay exorbitant gas fees or wait for other transactions to complete. This delay results from different apps having a different number of users. Ethereum creators and other team members have opted for second-layer solutions, such as Ethereum 2.0, to deal with scalability and speed issues. However, the optimism in these solutions is still low. Another problem with Ethereum coding relates to the Ethereum protocol being still under development [24]. This challenge necessitates developers to spend much time learning the coding process. Until Ethereum has matured as a blockchain network, developers will continue to face coding challenges. Building and deploying applications are still challenging, for the system is still new and may undergo changes in the future [24]. Understanding Ethereum's infrastructure requires learning the different platforms, security protocols, networking, programming languages, and tools. Not many developers are familiar with these areas, and most of them have to learn to set up quality development environments.

11. Case study of Ghost algorithm

In the study of Kiayais and Panagiotakos [25], they showed a lower constraint on the likelihood of uniquely successful rounds in this section. This constraint enables to debate the security of GHOST even when f is larger than 1.

The second inequality has been extensively explored and is true for $r < 0.1$. We can be obtained through $a \leq c \frac{\ln(1-r)}{1+\frac{\ln(1-r)}{r}}$, which holds true for $r < 0.1$ and $a \in (r, 2k)$.

Assume that γ is a lower constraint on the likelihood of a round being uniquely successful. (a round where only one block is found). From an occurrence in which $(m - \gamma)$ players each throw q

coins and precisely one coin toss results in heads, the likelihood of a round being uniquely successful can be described as Formula 1 as below:

$$(m - y)tr(1 - r)^{t(m-y)-1} \geq \alpha e^{-\alpha - hl} \quad (1)$$

We define $\gamma = \alpha e^{-\alpha - hl}$ as the smallest k that fulfills the relation $\alpha \in (l, 2c)$. This is a significantly better bound than u and also a lower bound in the event of a successful round. Fig 1 illustrates the relationship between the two boundaries [25].

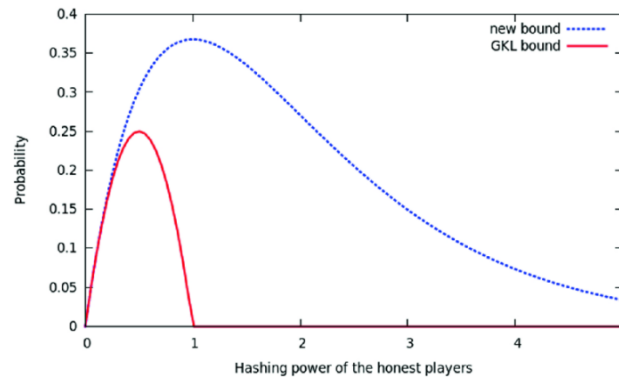


Figure 1. Hashing power of the honest players

Comparing the lower limits on the likelihood of a round being uniquely successful, γ and γ_u utilized this section. Notice that when f is more significant than 1, γ permits us to debate security.

12. Discussion

The Ghost protocol has applications in different sectors, including cloud-based manufacturing that leverages IoT technologies. It overcomes the challenges of centralized blockchain nodes. The network enhances security by creating different trust relationships and levels. GHOST makes mainchain determination faster by permitting block parallelism. State Tree Pruning allows partial storage. Cryptocurrency miners should consider the Ghost protocol for these benefits.

13. Conclusion

Ethereum's Ghost Protocol does not consider the complete information in the block tree, making faster retrieval and finalization of transactions. GHOST rules help miners select the most significant subtree as the primary tree, increasing the cumulative block difficulty. It reduces the delay in traditional blockchains using references to uncles or orphan blocks. Due to references' rewards, the Ghost protocol creates an incentive for all crypto miners in the chain. The protocol implies less difficulty in mining and eliminates the network security problem because of quicker block generation time. Centralization often occurs in a network initially intended to be decentralized. The GHOST protocol uses Coordination Blockchain to enable crypto miners to locate information using domain names. It helps overcome the problems with the previous technologies that did not have measures to ensure censorship resistance and security. Ethereum accepts only seven uncle block generations, preventing numerous calculations. Recently, crypto miners have complained about the Ethereum network since transactions take hours or days to complete. Ethereum has not enhanced its "gas limit" to help increase the block size. Until Ethereum matures as a blockchain network, developers will continue to face coding challenges. However, the network enhances security by creating different trust relationships and levels, increasing the acceptability of Ethereum as a cryptocurrency.

References

- [1] Antal, C., Cioara, T., Anghel, I., Antal, M., & Salomie, I. (2021). Distributed Ledger Technology Review and Decentralized Applications Development Guidelines. *Future Internet*, 13(3), 62. <https://doi.org/10.3390/fi13030062>.

- [2] Chen, H., Pendleton, M., Njilla, L., & Xu, S. (2020). A Survey on Ethereum Systems Security. *ACM Computing Surveys*, 53(3), 1-43. <https://doi.org/10.1145/3391195>.
- [3] Bahga, A., & Madiseti, V. (2016). Blockchain Platform for Industrial Internet of Things. *Journal of Software Engineering and Applications*, 09(10), 533-546. <https://doi.org/10.4236/jsea.2016.910036>.
- [4] Ritz, F., & Zugenmaier, A. (2018). The Impact of Uncle Rewards on Selfish Mining in Ethereum. *IEEE European Symposium on Security and Privacy Workshops*, 2018, 50-57. <https://doi.org/10.1109/EuroSPW.2018.00013>.
- [5] Amores-Sesar, I., Cachin, C., & Parker, A. (2021). Generalizing Weighted Trees: A Bridge from Bitcoin to GHOST, 1-27. Retrieved 17 November 2021, from https://www.researchgate.net/publication/354268684_Generalizing_Weighted_Trees_A_Bridge_from_Bitcoin_to_GHOST.
- [6] Nguyen, G., & Kim, K. (2018). A Survey about Consensus Algorithms Used in Blockchain. *Journal Of Information Processing Systems*, 14(1), 101-128. <https://doi.org/10.3745/JIPS.01.0024>.
- [7] Gencer, A., Basu, S., Eyal, I., Renesse, R., & Sirer, E. (2018). Decentralization in Bitcoin and Ethereum Networks, 1, 1. Retrieved 17 November 2021, from https://www.researchgate.net/publication/322498293_Decentralization_in_Bitcoin_and_Ethereum_Networks.
- [8] Rudlang, M. (2017). Comparative Analysis of Bitcoin and Ethereum (Masters). Norwegian University of Science and Technology. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2451325/17050_FULLTEXT.pdf?sequence=1.
- [9] Natoli, C., & Gramoli, V. (2017). The Balance Attack or Why Forkable Blockchains Are Ill-Suited for Consortium. *Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, 47, 579-590. <https://doi.org/10.1109/DSN.2017.44>.
- [10] Robinson, P. (2020). The merits of using Ethereum MainNet as a Coordination Blockchain for Ethereum Private Sidechains. *The Knowledge Engineering Review*, 35(e30), 1-17. <https://doi.org/10.1017/s0269888920000296>.
- [11] Aguiar, L. (2019). Improve dissemination in the Ethereum Network (Masters). Instituto Superior Técnico. https://fenix.tecnico.ulisboa.pt/downloadFile/1689244997260379/80950_luis_aguiar_dissertacao.pdf.
- [12] Kiayias, A., & Panagiotakos, G. (2019). On Trees, Chains and Fast Transactions in the Blockchain. *Progress In Cryptology – LATINCRYPT 2017*, 1, 327-351. https://doi.org/10.1007/978-3-030-25283-0_18.
- [13] Ritz, F., & Zugenmaier, A. (2018). The Impact of Uncle Rewards on Selfish Mining in Ethereum. *IEEE European Symposium on Security and Privacy Workshops*, 2018, 50-57. <https://doi.org/10.1109/EuroSPW.2018.00013>.
- [14] Nawaz, A., Peña Queralta, J., Guan, J., Awais, M., Gia, T., & Bashir, A. et al. (2020). Edge Computing to Secure IoT Data Ownership and Trade with the Ethereum Blockchain. *Sensors*, 20(14), 3965. <https://doi.org/10.3390/s20143965>.
- [15] Parma, J., & Wassvik, C. (2018). Should well-diversified portfolios contain cryptocurrencies? (Masters). University of Agder. <https://oda.oslomet.no/oda-xmlui/bitstream/handle/10642/7076/Parma-Wassvik.pdf?sequence=2&isAllowed=y>.
- [16] Amores-Sesar, I., Cachin, C., & Parker, A. (2021). Generalizing Weighted Trees: A Bridge from Bitcoin to GHOST, 1-27. Retrieved 17 November 2021, from https://www.researchgate.net/publication/354268684_Generalizing_Weighted_Trees_A_Bridge_from_Bitcoin_to_GHOST.
- [17] Kolb, J., AbdelBaky, M., Katz, R., & Culler, D. (2020). Core Concepts, Challenges, and Future Directions in Blockchain. *ACM Computing Surveys*, 53(1), 1-39. <https://doi.org/10.1145/3366370>.
- [18] Neitz, M. (2020). Blockchains and the Ethical Considerations of Centralization. *Digital Commons*, 1, 1. <https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?article=1866&context=pubs>.
- [19] Sompolinsky, Y., & Zohar, A. (2021). Secure High-Rate Transaction Processing in Bitcoin. *The Hebrew University of Jerusalem, Israel*. <https://eprint.iacr.org/2013/881.pdf>.
- [20] Son, B., Lee, J., & Jang, H. (2020). A Scalable IoT Protocol via an Efficient DAG-Based Distributed Ledger Consensus. *Sustainability*, 12(4), 1529. <https://doi.org/10.3390/su12041529>.

- [21] Xu, Y., & Huang, Y. (2019). MWPoW: Multiple Winners Proof of Work Protocol, a Decentralisation Strengthened Fast-Confirm Blockchain Protocol. *Security And Communication Networks*, 2019, 1-13. <https://doi.org/10.1155/2019/3674274>.
- [22] Zambrano, R. (2017). Blockchain: Unpacking the disruptive potential of blockchain technology for human development, 1, 4-84. Retrieved 17 November 2021, from <https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56662/IDL-56662.pdf>.
- [23] Turcotte, C. (2019, September 13). Why did transactions on Ethereum become terribly slow? Retrieved from <https://hackernoon.com/explainer-why-is-my-ethereum-transaction-taking-so-long-qg1t632cz>.
- [24] The Value Trend. (2021, October 6). Ethereum: Death by 1000 paper cuts (Cryptocurrency: ETH-USD). Retrieved from <https://seekingalpha.com/article/4458739-ethereum-death-by-1000-paper-cuts>.
- [25] Kiayias A., Panagiotakos G. (2019) On Trees, Chains and Fast Transactions in the Blockchain. In: Lange T., Dunkelman O. (eds) *Progress in Cryptology – LATINCRYPT 2017*. LATINCRYPT 2017. Lecture Notes in Computer Science, vol 11368. Springer, Cham. https://doi.org/10.1007/978-3-030-25283-0_18.