RESEARCH ARTICLE OPEN ACCESS

Distributed Cryptocurrency Mining Framework for Enterprise Data Centers

Rahul R. Sharma

ABSTRACT
There is a pressing need to reduce processing power clustering by powerful mining farms for mining cryptocurrencies to prevent monopoly and bias in blockchain networks. Technology-based enterprises could play a major role in bringing this transformation. Most of the servers used by medium-scale and large-scale technology-based enterprises do not receive consistent traffic and therefore do not utilize their processing power completely. This paper presents the Distributed Cryptocurrency Mining Framework, a system that can utilize the remaining processing power in enterprise data centers by running a distributed, scalable, modular, and enterprise-safe cryptocurrency mining framework that allows mining for different cryptocurrencies. Enterprises can run their servers in hybrid modes where cryptocurrency mining is stopped or performed at much lower priority during periods of regular or higher main application traffic. During off-peak hours and low-traffic periods, the servers can perform cryptocurrency mining at much higher rates to better utilize the processing power available on their data centers.

Keywords —cryptocurrency attacks, cryptocurrency mining framework, enterprise cryptocurrency mining, mining profitability.

I. INTRODUCTION

In the recent years, there has been a steady surge in cryptocurrencies that utilize proof-of-work based algorithms. Most of the cryptocurrency mining is performed at dedicated cryptocurrency mining farms that utilize specialized hardware such as application-specific integrated circuit (ASIC) miners to perform mining at much higher rates than traditional processors and GPUs. According to [1], with the advent of these mining farms, most of the cryptocurrency mining is performed by a handful of powerful mining farms and very less mining is performed by other smaller miners in the network. If these trends continue, these powerful mining farms could dominate or even alter the future development of the cryptocurrencies in a manner that would directly benefit them. Several such incidents are discussed in [2], [3] and [4], where when miners attained control of more than 50 percent of the mining hash rate of the network, they acquired the privilege to halt or even reverse transactions. Such scenarios are known as the *51 percent* attack and are discussed further in [4] and [5]. Addition of a large number of smaller and mid-sized cryptocurrency mining farms to the network could counter their dominance, ensure that cryptocurrencies mined are less clustered towards a smaller set of powerful mining farms and prevent bias & network takeovers. Technology-based enterprises could play a major role in bringing this transformation.

Most medium-scale and large-scale technology-based enterprises make use of data centers that run hundreds or thousands of servers. Most of the servers do not receive consistent traffic and therefore cannot utilize their processing power completely. The demand for data center processing power experiences peaks only at certain periods of the day, and it remains much lower at other periods. These drastic demand variations for computing power in data centers are discussed further in [6]. With the prevalence of restful services and microservice based architectures, even more servers are handling IO intensive traffic and do not completely utilize their computing power. Servers that perform batch processing also receive traffic only at specific intervals and are generally idle at other times.

These observations present an interesting opportunity and potential for further utilization of thousands of servers owned by an enterprise to perform alternate non-invasive background tasks that can further generate revenue. One such non-invasive operation is cryptocurrency mining. By acting as smaller or mid-sized cryptocurrency mining farms, there enterprises would not only better utilize the processing power of their data centers but also contribute towards making the cryptocurrency network less clustered towards a few powerful mining farms.

This paper presents DCMF (Distributed Cryptocurrency Mining Framework), a system that can utilize the remaining processing power in enterprise data centers by running a distributed, scalable, modular, and enterprise-safe cryptocurrency mining framework that allows mining for different types of cryptocurrencies. Cryptocurrencies are also experiencing exponential growth in the recent years, which could add to the net earnings for the enterprises.

II. SYSTEM DETAILS

DCMF allows picking up a group of computing nodes from an enterprise's data centers and converting them into a full-fledged mining farm with one or more mining pools. DCMF's architecture consists of several mining nodes that perform cryptocurrency mining, and a group of one or more mining servers that handle the configuration of all the mining nodes. All cryptocurrency mining computations are performed only at the mining nodes. A system with a group of mining servers and several mining nodes forms a mining pool. Several such

mining pools could be run in an enterprise's data centers to utilize all the unused processing power for performing cryptocurrency mining.

In contrast to traditional cryptocurrency mining farms where mining is performed on dedicated nodes, DCMF is designed to run in parallel with an existing application as a non-invasive background process such that it does not have a significant impact on the performance of the existing application running on the servers. This is achieved by varying the configuration of the mining process running on the mining nodes, which includes adjusting the number of threads performing mining and the thread priority of the mining threads.

In most real-world web applications, the traffic varies throughout the day such that the traffic peak is anywhere between 1.5 and 5 times the average traffic. This allows significant amount of processing power to be reused for cryptocurrency mining, especially in applications where pool resizing strategies to add or remove new servers are discouraged for their inability to support sudden surge in application traffic.

the pool. The configuration for each mining node consists of details such as whether mining is enabled or disabled, number of mining threads for a specific mining node, the thread priority for the threads performing mining and other necessary configuration specific to the host. This allows modify the configuration for one or more mining nodes directly from the mining server to perform cryptocurrency mining aggressively during off-hours and low traffic periods, or to perform mining less aggressively during regular and high traffic periods.

The mining servers store shared data and pool statistics for the mining pool. The system also consists of a global shared repository for storing any global system parameters shared across all mining servers. The mining servers can access data from the global shared repository and provide them along with the pool shared data to the mining nodes.

Mining servers run a restful service that allows mining nodes to fetch their active configuration and data useful for the mining algorithms. For the purpose of maintaining enough mining nodes in a mining pool, the mining servers also maintain a list of backup hosts where they can start mining if the number of active mining nodes drop below a specific threshold. If a mining node comes back online, it is added to the backup hosts list and stops all mining activity.

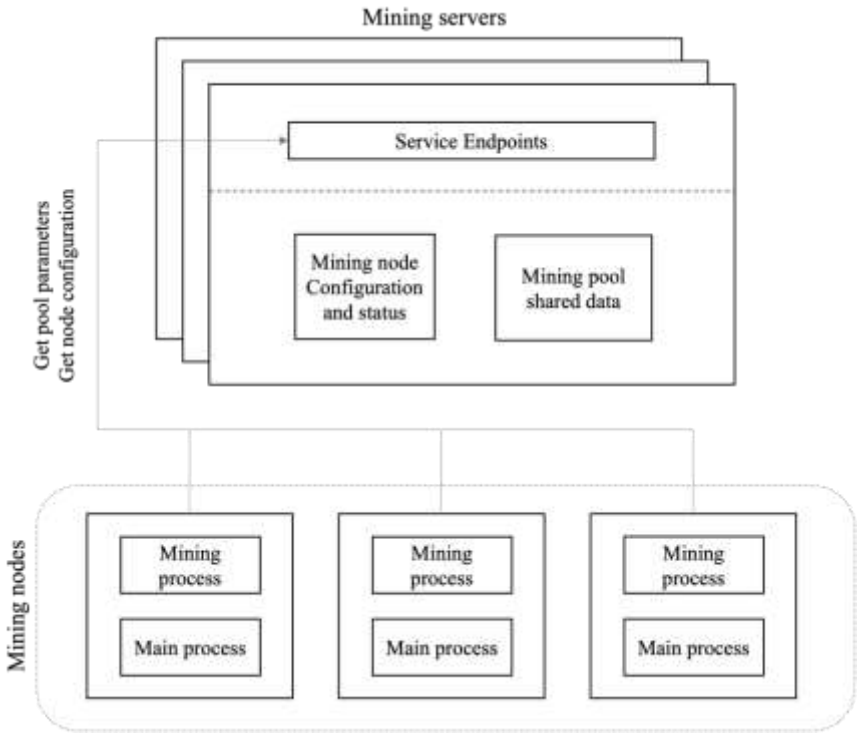

Fig. 1 presents the structure of a typical DCMF mining pool with one or more mining servers and the mining nodes. The mining servers store configuration for all the mining nodes in

Fig. 1. Mining pool structure

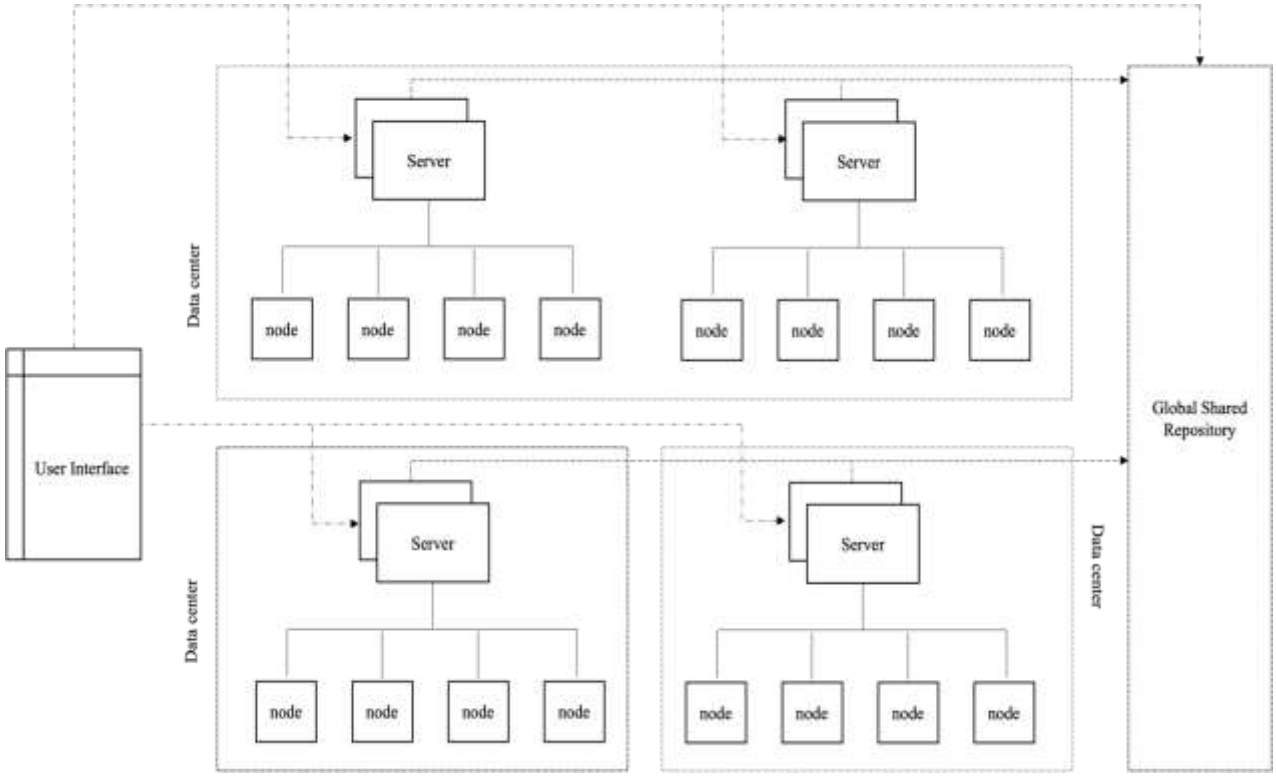

Fig. 2. DCMF components in a mining farm

The mining nodes periodically synchronize their configuration with the mining server. This process also enables the mining servers to track heartbeat of the mining nodes which facilitates monitoring the system health. Since the mining nodes only call the servers periodically, a group of one or more mining servers can scale to thousands of mining nodes in a pool. To ensure fault tolerance, the group of mining servers consist of multiple server nodes where all mining servers store a replica of the client configurations, pool data and system health details. All pool data and system health details are replicated periodically between the mining servers. The structural units of a mining farm are presented in Fig. 2.

Mining pools can run one or more mining algorithms but running a single mining algorithm for a pool makes them simpler. An enterprise can run multiple mining pools, each using a specific mining algorithm. This also allows the pools to mine different type of cryptocurrency that use the same mining algorithm. The nodes can be part of a particular mining pool based on different criteria suitable for the enterprise, such as combining computing resources located at a particular geographical location into a mining pool or combining resources from a particular department into a mining pool.

The pool status and mining statistics can be monitored via a user interface that retrieves mining statistics from the mining servers from all mining pools. The system also supports configuration of policies for the mining pools to control mining schedule and activity. This allows pre-configuration of aggressive mining activities during planned maintenance, known low traffic periods and other special occasions.

III. FEATURES OF DCMF

The DCMF abstractions allows programmers to use any of the existing mining algorithms or add their own by extending the base miner class to provide their mining algorithm that could be run in parallel on several mining nodes. The mining nodes can either work together mining for the same block by mining on different nonce ranges, or they can mine their own blocks independent of the other nodes, depending on the algorithm and configuration. This allows the ability to plug-and-play any existing and upcoming crypto-mining algorithms used by hundreds of proof-of-work based cryptocurrency mining algorithms to mine different cryptocurrencies.

Some of the most important features and characteristics of DCMF are discussed below.

A. Hybrid-mode mining support

DCMF is designed to run along with an existing application in the form of a non-invasive background process without significantly impacting the performance of the existing application. This enables enterprises to enter the cryptocurrency domain without making any significant

investment on the infrastructure needed for performing cryptocurrency mining, and at the same time allows them to utilize their existing infrastructure more efficiently and enhance further their income. Enterprises could also add more hardware that are initially utilized for cryptocurrency mining and can later be used for serving the main application traffic incrementally. Some of the most rewarding use cases for DCMF adaptation includes applications with larger differences between peak traffic and average traffic, batch applications that are idle for a significant portion of the day and newer applications that are expected to grow rapidly in the near future where resources need to be allocated in advance to support the rapid growth and ramp-up.

B. Scalability

Scaling the mining capacity of a data center is as simple as identifying new nodes from the data center that are under-utilized and adding them to either an existing or a brand-new mining pool to start mining cryptocurrencies.

The mining servers in the DCMF structure are also easy to scale. The DCMF mining servers receive traffic only periodically from the mining nodes for configuration synchronization and health reporting. This allows one server to handle thousands of mining nodes in a single pool without acting as a bottleneck. A mining farm can consist of thousands of such mining servers from an enterprise, making the whole system highly scalable. The structure of the mining server and the mining nodes are also very simple.

C. Fault Tolerance

The system is fault-tolerant in terms of mining server failures. The mining server group consists of one or more mining servers that replicate all pool data and configuration. Therefore, if one or more servers fail, the remaining servers serve the mining nodes. Since the mining nodes perform the actual mining operation, complete failure of the mining servers or their unavailability for a short duration may not affect the mining operation, but it might delay mining activity scheduling. In the worst case, the mining nodes that are unable to synchronize their configuration with the mining server may keep performing mining aggressively which could impact the performance of the main application running on the same servers.

The mining performance can degrade if multiple mining nodes fail. To prevent this scenario and to always ensure enough mining nodes, the mining servers maintain a list of backup hosts where they can start mining if the number of active mining nodes drop below a specific threshold for the pool.

D. Modularity and Extensibility

The mining nodes could run any of the standard mining algorithms. New mining algorithms could be added very easily by extending the base miner class to accommodate any new and upcoming mining algorithms. The modular design and ease of onboarding future cryptocurrency algorithms could mean that enterprises that adopt DCMF could keep utilizing it for much longer by just adding newer algorithms or fine-tuning the existing algorithms.

E. Enterprise-safe Algorithms Support

The safety of the source code running on the data centers is a top concern for enterprises to prevent malware, ransomware, or other potentially harmful code from running on their data centers. DCMF facilitates this process by exposing the mining algorithms as an independent entity of the system that could be reviewed and certified separately. The mining nodes would run the mining algorithms reviewed and certified by an enterprise making it safer to run these algorithms and perform mining.

F. Security

In most cases, since the mining nodes are located within a data center safeguarded by the enterprise's firewalls and access control policies, the system is secure against most unauthorized external access. Furthermore, the mining servers utilize authentication and authorization for the restful services to ensure that only authorized users could add new mining nodes to the mining pool, remove mining nodes from existing mining pools or reconfigure the mining activity for a pool. The restful services perform authentication and authorization via OAuth 2.0 standard by using bearer tokens. The restful services rely on transport layer security (TLS) version 1.3 to protect the data while in transit. [7] and [8] provides more details on the OAuth 2.0 standard, bearer token usage details and security analysis of the OAuth 2.0 standard. DCMF is also compatible with blockchain-based tokens discussed in [9]. Further details on the TLS protocol version 1.3 and its security and privacy aspects are discussed in [10], [11], [12] and [13].

IV. DISCUSSION

DCMF does not aim to replace traditional mining farms. It is an attempt to facilitate the introduction of large number of smaller mining farms that can perform cryptocurrency mining by utilizing the existing infrastructure more efficiently rather than introducing new dedicated computing resources. Since a large number of these computing resources are used by technology-based enterprises, they could be an immediate benefactor of this technology. Most of the features and characteristics of DCMF are designed around making it easier for enterprises to adopt and utilize the system on their data centers. Moreover, if enough number of such smaller mining farms get added to the network, they could together make up a significant portion of the net processing power. This would not only reduce bias but also make the cryptocurrency networks more stable in terms of changes in the net processing power in case some of the mining farms decide to leave the network.

A. Mining profitability

A major factor that dictates whether utilizing DCMF is economically feasible or not is the profitability of the mining operation. DCMF can enable enterprises to utilize their

unused processing power and perform cryptocurrency mining, but the enterprises need to evaluate a few parameters themselves to evaluate the potential gains from the mining process. This profitability analysis is similar in nature to the evaluation process employed by the traditional cryptocurrency mining farms.

The profitability in performing cryptocurrency mining is dependent on several factors which include the electricity rate at a particular geographical location, the cost of purchasing and maintaining the mining infrastructure, the cost for cooling the hardware, the real-estate costs for the facility which hosts the mining hardware, and the increase in value of the cryptocurrency mined over time.

Several factors that affect mining profitability are discussed in detail in [14], [15], [16] and [17]. The energy consumed during the proof-of-work based cryptocurrency mining process, especially for Bitcoin production is discussed in detail in [14]. It is important to note that energy consumption would be lower for proof-of-work based cryptocurrencies with lower mining difficulty. [15] compares the cost of mining Bitcoin in relation to the volume of transactions processed and suggests that the relative cost of mining Bitcoin has remained relatively constant. [16] presents a study on the profitability of the Bitcoin mining operation in a span of four years between 2012 and 2016 to suggest that Bitcoin mining has become less profitable over time when the hardware investments and energy costs are considered. [17] also presents a similar picture for Bitcoin miners where the mining profitability has been falling for existing mining farms due to the increasing difficulty of the mining process. These results suggest that alternative cryptocurrencies with lower mining difficulty could be more profitable from cryptocurrency mining perspective for smaller mining farms.

Technology-based enterprises own an inherent advantage in the mining process when compared with traditional cryptocurrency mining farms since they already own or rent the data centers that host the hardware, and they already pay for the cooling, maintenance, and real-estate costs. The only extra expense incurred would be for the extra power utilized for performing mining. Selecting a location with better electricity rates and the right cryptocurrency could enhance the long-term mining profit. The enterprise could also selectively mine the cryptocurrencies that are expected to appreciate the most or can exchange the easy-to-mine cryptocurrencies mined by their pools for more desirable cryptocurrencies suitable for long-term holding.

Despite these advantages, the mining hash rate from a hybrid approach would be significantly lower than the hash rates achieved by powerful ASIC miners and other specialized hardware employed by traditional mining farms. The profitable approach for smaller standalone DCMF based miners could be to focus on cryptocurrencies with lower and medium mining difficulty. Smaller DCMF mining enterprises could also collaborate with other smaller DCMF mining enterprises by pooling their resources to form large powerful mining pools. There large mining pools could not only compete in processing power with traditional mining farms with specialized hardware but would also increase the chances of mining a block for the smaller enterprises. In a globally distributed configuration with multiple smaller enterprises, each mining farm within an enterprise would act as a mining node that performs mining for the same block, and the profits from mined blocks are split based on the portion of the processing power contributed by the individual nodes. This resource pooling approach is similar to the one discussed in [18], [19] and [20] for Bitcoin mining pools, but in this case, each node is a DCMF mining farm.

V. CONCLUSION

There is a pressing need to reduce processing power clustering by powerful mining farms for mining cryptocurrencies to prevent monopoly and bias in blockchain networks. Technology-based enterprises could play a major role in transforming cryptocurrency networks to become even more unbiased and de-centralized in nature. With its capability to convert a traditional data center into a full-fledged mining farm, DCMF can play a major role in bringing this transformation.

DCMF provides a powerful, scalable, fault-tolerant, modular, easily extensible, and secure cryptocurrency mining framework. Enterprises can utilize DCMF to run their servers in hybrid mode where unutilized processing power is utilized for performing cryptocurrency mining. During off-peak hours and low-traffic periods, the servers can perform cryptocurrency mining at much higher rates, whereas cryptocurrency mining could be stopped or performed at much lower priority during periods of regular or higher main application traffic.

DCMF does not aim to replace traditional mining farms with enterprise servers performing cryptocurrency mining as a background non-invasive operation. Rather, it strives to introduce large number of smaller mining farms that can perform cryptocurrency mining by utilizing the existing infrastructure more efficiently.

REFERENCES

[1] Khairuddin, Irni Eliana and Sas, Corina, “An Exploration of Bitcoin Mining Practices: Miners’ Trust Challenges and Motivations”, In Proceedings of CHI '19: CHI Conference on Human Factors in Computing Systems (CHI '19), May 04, 2019, Glasgow, Scotland UK. (https://doi.org/10.1145/3290605.3300859)

[2] Bambrough, Billy, “Bitcoin Rival Suffers Devastating Attack”, Forbes, Jan 28, 2020. (https://www.forbes.com/sites/billybambrough/2020/01/28/bitcoin-rival-suffers-devastating-attack/?sh=53c254a1cb73)

[3] Ghosh, Monika, “Understanding 51% Attacks On Blockchains”, Jumpstart, Sep 14, 2020. (https://www.jumpstartmag.com/51-attacks-on-blockchains/)

[4] “51% Attacks”, Digital Currency Initiative, MIT Media Lab, Retrieved Nov 6, 2021. (https://dci.mit.edu/51-attacks)

[5] Frankenfield, Jake, “51% Attack”, Investopedia, Aug 25, 2021. (https://www.investopedia.com/terms/1/51-attack.asp)

[6] Liu, Jie, Zhao, Feng, Liu, Xue and He, Wenbo, "Challenges Towards Elastic Power Management in Internet Data Centers", 29th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS 2009 Workshops), 22-26 June 2009, Montreal, Québec, Canada. (http://dx.doi.org/10.1109/ICDCSW.2009.44)

[7] Jones, Michael B. and Hardt, Dick. "The OAuth 2.0 Authorization Framework: Bearer Token Usage." RFC 6750, p1-18, Oct 2012. (https://www.rfc-editor.org/info/rfc6750)

[8] Fett, Daniel, Küsters Ralf, and Schmitz Guido, "A Comprehensive Formal Security Analysis of OAuth 2.0". In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16). Association for Computing Machinery, New York, NY, USA, 1204–1215, 2016. (https://doi.org/10.1145/2976749.2978385)

[9] Fotiou, N., Pittaras, I., Siris, V.A., Voulgaris, S., & Polyzos, G.C., "OAuth 2.0 authorization using blockchain-based tokens". ArXiv, abs/2001.10461, 2020. (https://arxiv.org/pdf/2001.10461.pdf)

[10] Rescorla, Eric, "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, IETF, Aug 2018. (https://rfc-editor.org/rfc/rfc8446.txt)

[11] Arfaoui, Ghada, Bultel, Xavier, Fouque, Pierre-Alain, Nedelcu, Adina and Onete, Cristina, "The privacy of the TLS 1.3 protocol" Proceedings on Privacy Enhancing Technologies, vol.2019, no.4, 2019, pp.190-210. (https://doi.org/10.2478/popets-2019-0065)

[12] Lee, Hyunwoo, Kim, Doowon, and Kwon, Yonghwi, "TLS 1.3 in Practice: How TLS 1.3 Contributes to the Internet". In Proceedings of the Web Conference 2021 (WWW '21). Association for Computing Machinery, New York, NY, USA, 70–79, 2021. (https://doi.org/10.1145/3442381.3450057)

[13] Dowling, B., Fischlin, M., Günther, F. et al., "A Cryptographic Analysis of the TLS 1.3 Handshake Protocol", J Cryptol 34, 37, 2021. (https://doi.org/10.1007/s00145-021-09384-1)

[14] Küfeoğlu, Sinan and Özkuran, Mahmut, "Bitcoin mining: A global review of energy and power demand", Energy Research & Social Science, Volume 58, Dec 2019, 101273, ISSN 2214-6296. (https://doi.org/10.1016/j.erss.2019.101273)

[15] Song, Y-D and Aste, T, "The Cost of Bitcoin Mining Has Never Really Increased". Front. Blockchain 3:565497, Oct 2020. (https://doi.org/10.3389/fbloc.2020.565497)

[16] Derks, J., Gordijn, J. and Siegmann, A., "From chaining blocks to breaking even: A study on the profitability of bitcoin mining from 2012 to 2016". Electron Markets 28, 321–338, Aug 2018. (https://doi.org/10.1007/s12525-018-0308-3)

[17] Deutsch, Hans-Peter, "Bitcoin Mining Profitability – The Good, the Bad and the Ugly". SSRN, Jan 2018. (https://ssrn.com/abstract=3123543)

[18] Luu, L., Saha, R., Parameshwaran, I., Saxena, P. and Hobor, A., "On power splitting games in distributed computation: The case of bitcoin pooled mining". In Computer Security Foundations Symposium (CSF), 2015 IEEE 28th, pages 397–411. IEEE, 2015. (https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7243747)

[19] Romiti, M., Judmayer, A., Zamyatin, A., & Haslhofer, B., "A Deep Dive into Bitcoin Mining Pools: An Empirical Analysis of Mining Shares". ArXiv, abs/1905.05999, 2019. (https://arxiv.org/pdf/1905.05999.pdf)

[20] Ittay Eyal and Emin Gün Sirer, "Majority is not enough: bitcoin mining is vulnerable". Commun. ACM 61, 7, July 2018, 95–102. (https://doi.org/10.1145/3212998)

[21] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll and E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," 2015 IEEE Symposium on Security and Privacy, 2015, pp. 104-121, doi: 10.1109/SP.2015.14. (https://ieeexplore.ieee.org/document/7163021)