Application of game theory in Bitcoin mining to prevent selfish mining using Fair Evolutionary Multi-objective Optimizer (FEMO)

June 27, 2022

Nguyen Duc Trung - 1901040231
Nguyen Tran Tu - 1901040187
Nguyen Manh Hung - 1901040103
Nguyen Hong Thai - 1901040199
Hoang Tien Quyet - 1901040170

Contents

Abstract

A blockchain data system needs reversion resistance and censorship resistance, which are crucial elements in data security, this can only be maintained when the majority of the miners contributing to the system are performing honest mining. But a miner can also use selfish mining trick in order to prevent other miners from gaining any benefit using his calculation and selfishly gain all benefit for themselves, this will affect the whole system in a bad way. The answer for this problem is using game theory to form a Nash equilibrium where the honest behavior of all miners becomes the dominant strategy. Which gives them the largest payoff regardless of how other miners behave in the system, as long as they themselves are being honest, thus miners no longer want to perform selfish mining. To actualize this scenario, we use Fair Evolutionary Multi-objective Optimizer (FEMO) because Evolutionary algorithms are well known for the ability of solving multi-objective optimization problems. This research explains in detail both the problem and the algorithm used to solve it, the result presented here strongly indicate the suitability of using Fair Evolutionary Multi-objective Optimizer in solving selfish mining behavior.

1 Introduction:

In a world that is always changing and developing day by day, information security is always a topic of research investment, through which blockchain was born. Stuart Haber and W. Scott Stornetta conceived the idea of introducing a computationally realistic solution to timestamp digital documents [1]. This is the forerunner of Blockchain technology. Over time, many scientists have relied on this idea to do other research related to cryptocurrencies. In 2008, Bitcoin - the first form of Blockchain technology was born. A year later, the first Bitcoin transaction successfully took place between two computer scientists Hal Finney and Satoshi Nakamoto [2].

In a blockchain, by connecting blocks, miners will receive rewards in crypto-coins. Therefore, it is inevitable for the miners to cheat for their own benefit, in this paper, we focus on "selfish mining". Selfish mining renders the calculations of honest miners useless, instead their private blocks are accepted into the blockchain chain, thereby receiving greater rewards.

Selfish mining was first proposed by Cornell researchers Emin Gün Sirer and Ittay Eyal in 2013 [3]. They demonstrated that miners can earn more bitcoins by hiding blocks. newly created from the main blockchain and create a fork of its own.

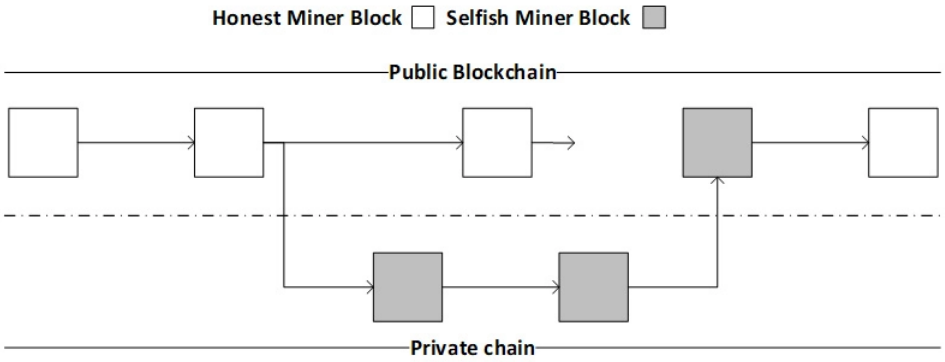

Figure 1: Selfish mining [3]

In their 2013 paper, Sirer and Eyal disclosed that miners could increase their share of the overall revenue by hiding new blocks and making them accessible to systems in their private network. This behavior quickens discovery and resolution of mining-related infrastructure issues such as network latency and power costs [3]. Nevertheless, this action will essentially cause damage to all participants. Selfish mining generates a lot of leftover, but it is important to note that those involved in this activity maintain a strategic benefit over other network partakers. As a result, the attacker will likely attract miners. In their paper, Eyal and Sirer highlighted this as a major jeopardy: selfish mining can lead to mining pools increasing in hashrate, as parties will collaborate with other selfish miners entities to maximize their income [3]. Ren Zhang and Bart Preneel also pointed out that selfish mining not only disrupts the fairness of the designer's original intent, but also presents potential threats to the distributed structure of Bitcoin.[5]

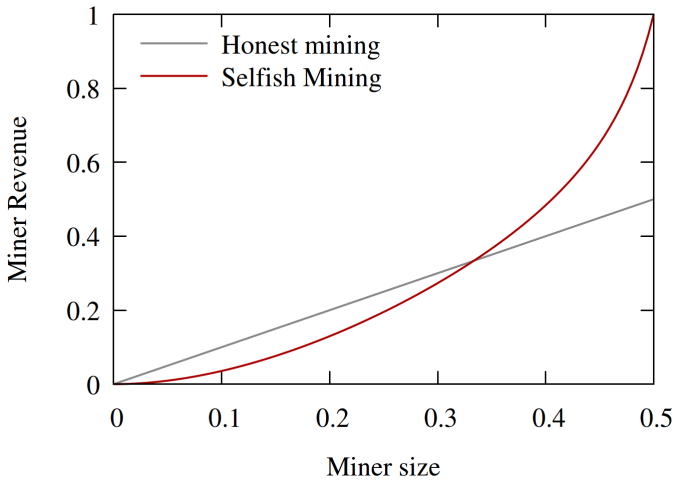

Figure 2: Miner gain from mining power [3]

Game theory is an approach to understanding and analyzing the behavior or decisions of individuals and groups of individuals in a conflicting situation. Game Theory pursues two basic assumptions. First, it assumes that each individual or group of individuals is a participant in a game and their goal is how to gain benefits (be it winning or reducing losses). Second, it considers each human action to be guided by the principle of reason in the sense that before each decision, individuals try to calculate their own benefits or disadvantages [6]. This study can be applied for many categories, one of which is decision making between miners and the blockchain.

In game theory, Nash equilibrium is a notion in which each player in a noncooperative game may optimize their result depending on the actions of the other players. In a game, Nash equilibrium is reached when no player, even if they know the other players' tactics, has any motivation to deviate from their own strategy. The hypothesis of the Nash equilibrium is that the players make decisions independently, without collusion. Rely on math and logic to determine the actions that game participants should take to ensure the best outcome for themselves[6]. Thus, Nash equilibrium is one of the most used concepts in applications of game theory when it comes to studying the interacting behaviors of agents with conflicting goals. It is the central concept of game theory that does not cooperate with perfect information.

In the papers we have introduced, almost all authors do not explain clearly about the cons of selfish mining in blockchain and have given unsatisfactory answers for the problem. In order to solve these shortcomings, we show a new form of selfish mining attack and how it affects blockchain. We empirically build a game model to solve the problem above and apply the Fair Evolutionary Multi-Objective Optimizer algorithm to find Nash equilibrium then explain how to solve the problems. This study applies a game theory approach to decision making and analysis of selfish mining behavior. In other words, this research can be used to prevent selfish mining and offer options to protect the interests of honest miners.

2 Literature review:

Cryptocurrency is one of the areas of great interest and focus. With that comes the need for research knowledge of the promise of the field. Along with the great potential for growth comes security risks, one of which is selfish mining. The first foundation of this research was laid by Ittay Eyal and Emin Gun Sirer [3] with the publication of selfish mining. They showed a new method of cryptocurrency mining and their impact on Bitcoin. Henceforth, topics around selfish mining are expanded. Regarding the hazard analysis, Dr Craig S Wright[9] argues that selfish mining will not generate additional blocks, and the profits will not be superior to that of miners participating in the work honestly. Jake Gober [10] proposed a hypothesis, in which, if selfish mining is more profitable, most people will choose selfish mining over honest mining, and point out that selfish mining is more profitable than mining. honestly, but multiple groups of miners on a network will create a race between the groups, thereby reducing profits. After clearly analyzing the situation of the risk of selfish mining, the reports aimed at giving solutions to the selfish mining attack were born.

Zhaojie Wang [11] and co-researchers proposed a system to detect selfish exploit attacks, based on a machine learning classification model for intelligent detection of attacks. Michal Kedziora, Patryk Kozlowski, Michal Szczepanik & Piotr Jozwiak[12] an algorithm of persistent mining in the pursuit of a longer chain with a modified selfish extraction algorithm to analyze what extent these risks may affect the fairness of the cryptocurrency extraction process.Shiquan Zhang; Kaiwen Zhang; Bettina Kemme[13] found out research gap in mainstream blockchain systems,

hence analyzing selfish mining scenarios with multiple independent attackers. Hamid Azimy; Ali Ghorbani[14] created a Bitcoin network simulator and used it to simulate different configurations of miners to analyze selfish mining in a competitive environment, with more than one selfish miners in play. Muhammad Saad, Laurent Njilla, Charles Kamhoua, Aziz Mohaisen said that selfish mining is a well known vulnerability in blockchains exploited by miners to steal block rewards. In this paper, Muhammad Saad, Laurent Njilla, Charles Kamhoua and Aziz Mohaisen explored [15] a new form of selfish mining attack that guarantees high rewards with low cost. Qianlan Bai; Xinyan Zhou; Xing Wang; Yuedong Xu; Xin Wang; Qingsheng Kong[16]show in their paper studies a fundamental problem regarding the security of blockchain on how the existence of multiple misbehaving pools influences the profitability of selfish mining.

Each selfish miner maintains a private chain and makes it public opportunistically for the purpose of acquiring more rewards incommensurate to the Hashrate. Chen Feng; Jianyu Niu[17] show Ethereum has received much attention from both academia and industry. Nevertheless, there exist very few studies about the security of its mining strategies. In this paper, Chen Feng and Jianyu Niu filled this research gap by analyzing selfish mining in Ethereum and understanding its potential threat. Tao Li,Zhaojie Wang,Yuling Chen,Chunmei Li,Yanling Jia,Yixian Yang Selfish mining attacks get a high prize due to the additional rewards unproportionate to their mining power (mining pools have particular advantages)[18]. Generally, this category of attacks stresses decreasing the threshold to maximize the rewards toward the view of attackers. Bitcoin is a well-known cryptocurrency in which records of transactions are maintained by a P2P network to create a distributed ledger. Due to the complex nature of maintaining highly efficient, transparent and speed transactions between nodes, security is one of the primary concerns of this system [19]. Kervins Nicolas; Yi Wang; George C. Giakos aim to identify implications of these countermeasures to address vulnerabilities in the blockchain network for future research on this topic. The paper presents vector of attack on the mechanism of achieving a proof of work consensus, such as the application of selfish mining strategy. The aim of the work was to analyze to what extent these risks may affect the balance of the cryptocurrency extraction process [20].

Michal Kedziora, Patryk Kozlowski, Michal Szczepanik & Piotr Jozwiak use an algorithm of persistent mining in the pursuit of a longer chain with a modified selfish extraction algorithm. Many current

mainstream blockchain systems, including Bitcoin, adopt Proof-of-Work (PoW) as their consensus protocol. Such a system faces various crypto economic attacks, such as selfish mining. In this paper, Shiquan Zhang; Kaiwen Zhang and Bettina Kemme addressed this research gap by analyzing selfish mining scenarios with multiple independent attackers[21]. Bitcoin mining is the process of generating new blocks in Bitcoin blockchain. This process is vulnerable to different types of attacks. One of the most famous attacks in this category is Selfish Mining, introduced by Eyal and Sirer in 2014. To address the problem, Hamid Azimy and Ali Ghorbani created a Bitcoin network simulator and used it to simulate different configurations of miners[22]. The Bitcoin cryptocurrency records transactions in a public log called the blockchain and its security critically depends on the distributed protocol that maintains it, run by participants called miners. Dr. Craig S.Wright showed that the Bitcoin mining protocol is in fact incentive-compatible and that the proposed attack with which colluding miners obtain a revenue larger than their fair share is flawed[23].

Bitcoin, still the most widely used cryptocurrency maintains a distributed ledger for transactions known as the blockchain. Eyal and Sirer introduced seflish mining, a strategy gives a significant edge in profits [24]. Dennis Eijkel & Ansgar Fehnker compared the analysis results to known results from literature and real-world data. The longest chain rule has been widely applied in blockchain systems to reach consensus on the distributed ledger. As an alternative solution to the longest chain rule, GHOST is proposed as a safer consensus rule. In this paper, Qing Xia; Wensheng Dou; Fengjun Zhang and Geng Liang explored the performance of selfish mining on GHOST[25]. Selfish mining attacks prove that Bitcoin's incentive mechanism is not incentive-compatible, which is contrary to traditional views. Selfish mining attacks may cause the loss of mining power, especially honest participants, which brings great security challenges to the Bitcoin system[26]. Zhaojie Wang , Qingzhe Lv, Zhaobo Lu, Yilei Wang and Shengjie Yue demonstrate that ForkDec has certain application value and excellent research prospects.

ID	Name of publishcation	Factor
1	Majority is not Enough: Bitcoin Mining is Vulnerable [reference][9]	New method of cryptocurrency mining
2	The Dynamics of a "Selfish Mining" Infested Bitcoin Network: How the Presence of Adversaries Can Alter the Profitability Framework of Bitcoin Mining.[10]	Show the profit of selfish-mining ,analyze the risk of selfish mining and show us some solution to prevent selfish mining
3	ForkDec: Accurate Detection for Selfish Mining Attacks[11]	Base on machine-learning, author use intelligent classification model to detect selfish exploit attacks
4	Analysis of Blockchain Selfish Mining Attacks[12]	Authors use extraction algorithm to modify and analyze selfish mining
5	Analyzing the Benefit of Selfish Mining with Multiple Players[13]	Analyzing selfish mining scenarios with multiple independent attackers
6	Competitive Selfish Mining[14]	Created a Bitcoin network simulator for miners and analyzed behaviors of players
7	Countering Selfish Mining in Blockchains[15]	Authors use the expected transaction confirmation height and block publishing to detect selfish mining behavior
8	A Deep Dive Into Selfish Mining Blockchain[16]	The security of blockchain was analyzed and showed how it work
9	Selfish Mining in Ethereum[17]	The paper analyzed selfish mining in Ethereum and understanding its potential threat
10	Is semi-selfish mining available without being detected?[18]	mining attacks get a high prize and mining pools have particular advantages

11	Comprehensive Overview of Selfish Mining and Double Spending Attack Countermeasures[19]	The complex nature of maintaining highly efficient, transparent and speed transactions between nodes, security
12	Analysis of Blockchain Selfish Mining Attacks[20]	The paper presents vector of attack on the mechanism of achieving a proof of work consensus, such as the application of selfish mining strategy
13	Analyzing the Benefit of Selfish Mining with Multiple Players[21]	Many current mainstream blockchain systems, including Bitcoin, adopt Proof-of-Work (PoW) as their consensus protocol
14	The Fallacy of Selfish Mining in Bitcoin: A Mathematical Critique[23]	the blockchain and its security critically depends on the distributed protocol
15	A Distributed Blockchain Model of Selfish Mining[24]	introduced selfish mining, a strategy gives a significant edge in profits
16	The Performance of Selfish Mining in GHOST[25]	In this papers the authors explored the performance of selfish mining on GHOST
17	Advances in Security and Performance of Blockchain Systems[26]	Selfish mining attacks may cause the loss of mining power, especially honest participants, which brings great security challenges to the Bitcoin system

Table 1: Review summary

After evaluating all articles above, we confirm that the above researches have many weaknesses that make the article not convince readers. In the article [9], [10], [12] the authors did not show the solutions for the problem they mentioned before. Shiquan Zhang; Kaiwen Zhang; Bettina Kemme and Hamid Azimy; Ali Ghorbani analyzed how the system of selfish mining works in article [13], [14]. However they have used the old extraction algorithm which is out of date today. Theory of [15], [16] just focuses on single objectives which is not suitable for reality today. In conclusion, all papers above did not apply the Game theory and FEMO to solve the problem for multiple objectives.

For that reason, this paper proposes an improved model of FEMO, the Fair Evolutionary Multi-objective Optimizer (FEMO). The major weakness of FEMO for the target function under consideration lies in the fact that a large number of mutations are distributed to parental pairs whose neighborhoods are already fully covered. Otherwise, the optimal sampling algorithm will always use the most promising origin at the border of the current population. Of course, this information is not available in the black-box optimization scenario. Homogeneous sampling leads to a situation where optimal Pareto individuals are unequally sampled depending on when each individual joins the population. The following fair sampling strategy ensures that all individuals receive the same number of samples in the end.

The FEMO algorithm is an improvement of SEMO. The problem is that some individuals are chosen more often than others to become parents. As a result, some individuals will mutate more often simply because they were added to the population earlier in history. As a result, the neighborhoods of these individuals will be over explored while others will not. The FEMO algorithm tries to avoid this situation by counting the number of offspring that each individual produces. When selecting parents, the selection algorithm determines the individual with the smallest number of children. If more than one individual with the same number of children is found, the parent is randomly selected from among these individuals.

3 Problem description:

3.1 Description of problem:

Cryptocurrency mining in general and bitcoin in particular is a complicated topic[27]. The conflict and balance between private interest and security has always been a backlog in any discussion of cryptocurrencies. Besides honest miners who always make their calculations public to build blockchain chains, thereby profiting through transactions, another mining method is potentially risky and profitable for miners, and sometimes the whole system - selfish mining. The goal of selfish miners is to stay ahead of the rest of the network by at least one block. The nodes that accept the most accumulated chain are valid blockchains. At any time, selfish miners may reveal their chain. If it is longer than the block followed by the rest of the network, the existing blocks will be dropped and the transactions reversed, their block will become part of the blockchain while the other block becomes an orphan

block. they will collect all the rewards from these blocks and cause other parties to waste resources[28]. Furthermore, if the parties cooperate to maximize their revenue, and when they have the most power, they can effectuate a 51% attack. Selfish mining brings a lot of opportunities, at the same time brings great challenges for miners and the whole system. If selfish mining can be successfully done by a pool of miners, it could indeed be an attractive strategy for other miners to join in order to increase their own revenue. In the worst case, the disadvantage will be for the whole system.

Some iconic events of selfish mining can be represented by a 51% attack on Krypton in 2016, a blockchain on the Ethereum network [7]. Selfish mining can lead to mining pools increasing in hashrate, and once the majority of the hash rate is obtained, the attacker will be able to intervene such as excluding or modifying the order of transactions. In 2018, a Japanese cryptocurrency Monacoin suffered a selfish mining attack which caused approximately $90,000 in damages[8].In this case, Monacoin was sent to abroad exchanges to swap them for other currencies before the hidden chains were revealed. These attacks pose an unavoidable threat in the immediate future that needs to be changed and upgraded in response to similar attacks aimed at promised targets, causing a dangerous impact for the virtual currency market.

3.2 Problem example:

For example, the following is an emulated game conducted by three miners, they will go through four rounds with different strategies. In this game, all three players – miners will have equal hash power at about 33% of total 100% system hash power. Which means they all have one third chance of winning each round, starting when they begin to mine a block until that block with the correct hashcode founded by any players, the miners who found the block win the round. Three miners are A, B and C, miners A and B are honest miners following bitcoin protocol while C is the selfish miner harming the system and other miners.

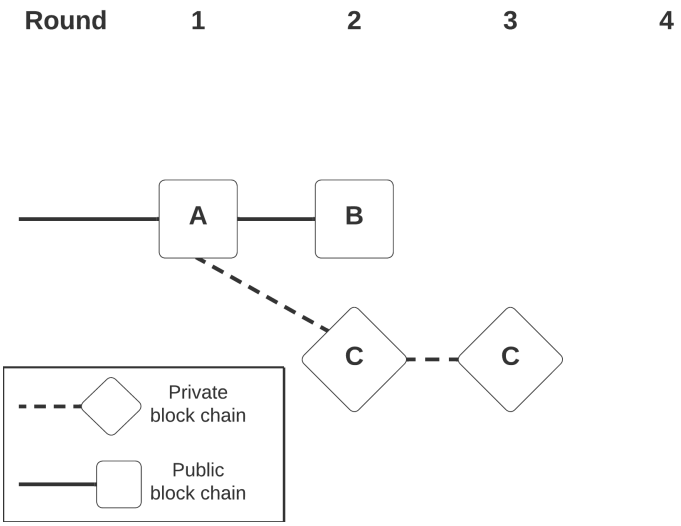

Figure 3: The first two round

All three miners started at the same time, competing with each other, racing to find out the next valid block. In this scenario, miner A got lucky and became the first one to win this one third chance. As an honest miner, he published his block immediately and got recognized by the system, his block surely participated in the final chain.

The second round began and this time, miner C found the correct hashcode first, but instead of publishing his result, he kept it privately and used it to calculate the next block for himself. And he actually got lucky the second time, found out the third block before anyone published the second block, this selfish miner is two steps ahead of everyone else already. The chance for this to happen are extremely low, just to find two continuous blocks are only at about 11%. Not to mention it has to be done before anyone else finds the second block, which lowers the chance to about 5%.

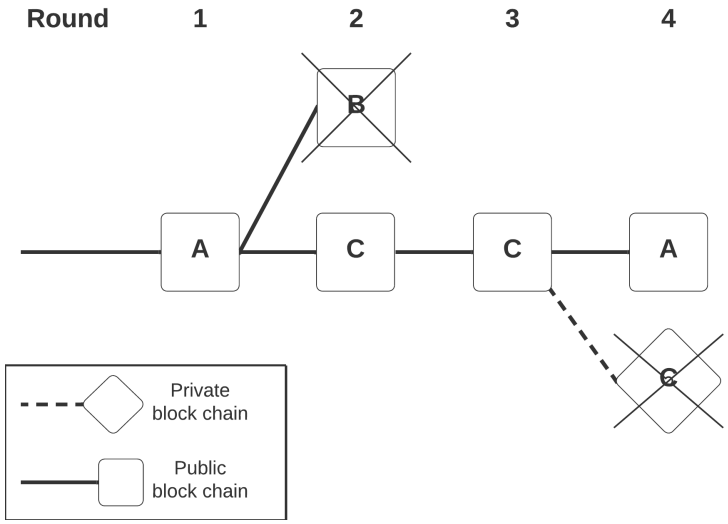

Figure 4: A completed game

The figure above describes how selfish mining attacks other miners financially. In this case, after miner B successfully found the second block and honestly published it. But when C saw it, he immediately published both his two blocks that he kept private. The system now sees miner C's chain is the longest blockchain and recognizes it instead of miner B's block, so C still got his two blocks at the end but B has wasted all of his money and effort for nothing.

The same strategy is applied, C kept on selfish mining but this time he did not get lucky because miner A found the fourth block right after him. Miner A is an honest miner so he published his block without hesitation and the system recognized immediately. Since C has not got the next block yet, he can not trick the system to make it reject miner A's publication. As a result, the private block of C is wasted.

3.3 Properties characteristics:

In the game of bitcoin mining, the players who participated and contributed to the blockchain system are called miners. These miners have some crucial characteristics that define their mining process and can change their strategies in making decisions. Each miner has their own:
- **Hash power**: also known as **mining hash rate**, the higher the rate, the higher the chance they can propose the next valid block and add it to the final chain. In order to obtain more hash power, miners need to invest in special devices specialized for computing hash code.
- **Hardware**: consumes an enormous amount of **electricity**, at industrial level, so the miner's financial upkeep plays an important role in this process as well.
- **Network speed**: is also a game changer to the block's upload speed or the time required to receive system changes since this computer race goes down to millisecond.

Using their hardware, miners can start computing and competing with each other, trying to be the first one who found the next valid hash code. And if a miner did find the valid block before others, he can choose to adapt one of two strategies:
- **Honest mining**: to follow the blockchain protocol and immediately publish it to the system for everyone else. If the miner performs honest mining, his block will be immediately recognized by the system and likely be paid at the end, but there are small chances that if someone else are selfish mining and already going far ahead, that person chain will be the longest chain, as the result, the honest miner's block is rejected and all the cost for computing process will be in vain. So honest mining only benefits the most if other miners are also doing it, remaining the major honest assumption of the whole system.
- **Selfish mining**: to keep the block privately and singly continue mining on that. The miner did not share his block and used it to compute the next block for himself. It heavily depends on luck since the chances of successfully finding two or three continuous blocks is amazingly low. Or if the selfish miner does not want to depend on luck, he has to increase his hash power by buying more hardware which is very costly.

Property	Characteristics
Player: Miners	- Mining hash rate(%). - Hardware: specialize computing devices, electricity. - Network speed. - Chosen block: block difficulty, block value.
Strategy	Honest mining: - Payoff: hardware prices + electric and network bill + selfish miners' financial attack. - Winning chance: equal to Mining hash rate. - Calculating time: Block difficulty / Mining hash rate. - Publish moment: right after successfully calculating a block. - Profit: Total block value - Payoff.
	Selfish mining: - Payoff: hardware prices + electric and network bill. - Winning chance: (Mining hash rate r̂ounds) x other miners' lose chances. - Calculating time: (Block difficulty / Mining hash rate) x rounds. - Publish moment: wait until other mines reach one block behind. - Profit: Total block value - Payoff.

Table 2: Summarize Properties characteristics

3.4 Example with sampled data set:

To better understand all strategies and to find Nash equilibria, we provide a sampled data set for the previous game introduced in part 3.2, and then use those data to simplify the calculating process. This time, miner A has a 30% mining hash rate, miner B has 25% and miner C owns up to 45%, all together contributing 100% hash power to the system. The larger the mining hash rate, the larger the amount of investment in hardware and also the electricity needed to operate them. In this case A used a total of 3000 dollars for buying hardware and B spent 2500 dollars, C heavily invested 4500 dollars to acquire the most mining hash rate.

All miners aiming to get as many blocks as possible, each completed block will give the one who calculated it and published it first some bitcoin worth 2000 dollars, the block itself also contains extra prize based on its

difficulty. So miners must choose a mining strategy of their own in order to maximize the profit. A and B decided to become an honest miner while C is a selfish miner. Then the game - mining process begins.

At the first round, miner A chose a fairly simple block that required less calculation corresponding to its low value. But since it is suitable to the 30% mining hash rate of A, he successfully calculated the first block and published it to the system. Miner A gained 2000 dollars for completing a block and 100 dollars as that block value, but he also lost 500 dollars because of electricity cost.

In the second round, Miner C with his high hash power found the second block first, but he decided to keep it privately, then use the information of that second block to calculate the continuous third block selfishly, he actually got lucky and achieved it before anyone else figured out the second block. Until that point, C has lost 1000 dollars of electricity to calculate two blocks.

Miner B did not know about the selfish mining strategy of C, so he was still calculating his own second block at that time, and after a while he finished his work, immediately publishing to the system. Seeing that B is catching up, miner C now publishes both his two private blocks. And since it forms a chain containing three blocks (A, C, C) which is longer than the two-blocked chain (A, B), the system automatically recognizes the longest block. As a result, C gained 4000 dollars for his two blocks along with blocks worth 800 dollars. While miner B lost 500 dollars electricity bill for nothing, he has been financially attacked by the selfish minner.

In the final round, C still got the block first thanks to his enormous investment at the beginning, then C still performed selfish mining but this time luck is not on his side, miner A published the fourth block before miner C succeeded in finding the next one by himself. The system recognize A's result because it will form a new longest chain, thus making the block that C keep private wasted, miner C has lost 500 dollars for nothing.

At the end, miner A gained 400 dollars profit as a normal honest miner, miner B lost a total 3000 dollars since he was attacked by the selfish miner. The selfish miner C himself also lost 1200 dollars. As the result shows, A is the only miner who gains profit because he is honest and has not been attacked by another selfish miner. In case of B and C, both lost money as the victim and the attacker in a selfish mining action. So as long as all miners remain honest, they will gain the most profit based on their investment no matter what others have done, this no doubt is the nash equilibria of the problem.

4 Models:

4.1 Introduction to Unified Game-based model:

The model is represented by the Fair Evolutionary Multi-objective Optimizer(FEMO). FEMO is the MOEA proposed by Laumann et al. [29]. It's a replacement for their previously released SEMO (Simple Evolutionary Multi-Objective Optimizer). It was first introduced in 2002 as a new black box multi-objective optimization approach. This chapter highlights and describes the key components of the FEMO algorithm. Finally, some of the findings from past studies are provided.

FEMO was created as a better version of SEMO. The fact that a substantial proportion of mutations occur in parents whose surroundings have been thoroughly researched is SEMO's main flaw. Furthermore, when uniform sampling is utilized, populations are sampled unevenly depending on the length of time an individual has been in the population [29]. This difficulty is solved by using a rational sample, which ensures that everyone receives roughly the same number of samples.

Laumanns et al. [30] proposed the FEMO algorithm after arguing that it would be beneficial if all individuals in the population generated nearly the same number of children. This algorithm employs the local mutation operator and a counter for each person in the population to count the number of children produced by that individual. We look into more generalized FEMO variants. Our techniques use the global mutation operator to accept more individuals with the same target vector as a population member. Because the ability to flip two or more bits in a single mutation step is required to escape the local optimum, the usage of the global mutation operator appears to be desirable. The flexible acceptance rule aids optimization by allowing for the exploration of plateaus and regions in decision space where decision vectors are mapped to the same goal vector.

4.2 Mathematical model:

In the above parts, we have researched all the factors that can affect the profits and the consequences of many players in the game, combined with the application of game theory to the mining process. We offer a **Unified**

Game-base model:

G = ({ P0,P }, Si, Ui , Rc)

In which:

- P0: is the data owners who need the blockchain system to secure their data.
- N: number of miners competing in finding the hash code of one or more blocks.
- P = { p1, . . . , pi, . . . , pN } set of miners.
- Si = {Si1, . . . , Sij, . . . , SiMi } set of miner's strategy, i

$$1 \leq i \leq N$$

- ui: is the payoff function of player i, reference the strategy of player i to a real numeric value.

$$Si \rightarrow R$$

- Rc: is the vector indicating the direction of solving the problem's contradiction. In which, c is the set representing the conflicts between miners in the problem.

Parameters of the model:

- Strategy of miners: - Si = {Si1, . . . , Sij, . . . , SiMi } set of miner's strategy, i

$$1 \leq i \leq N$$

in which

+ Mi: is the amount of blocks that player i competing in.
+ Sij: is the strategy of player i, including: winning chance, calculating time, publish moment.

- Payoff function of each miner:

ui = Vj - Hi - $Ei + Ni$ x Dj x $\frac{Si}{Ri}$ x Wi - Vj x SR

In which:

- Hi: hardware prices that the miner i invested in.
- Ei: electricity price in the region that miner i lived in.
- Ni: network price in the region that miner i lived in.
- Dj: block difficulty of the chosen block j.
- Vj: block value of the chosen block j.
- Ri: mining hash rate (hash power) of miner i.
- Ni: network speed of miner i.
- SR: Selfish miner's mining hash rate in the whole system other than

miner i.

4.3 Nash Equilibria formula and its application:

Nash equilibrium is one of the most used concepts in applications of game theory in economics when it comes to studying the interacting behaviors of agents with conflicting goals. It is the central concept of game theory that does not cooperate with perfect information. The concept was proposed by J. Nash (1951) as a formalization of the date, but A. A. Cournot a century and a half ago anticipated the idea in his analysis of a two-man monopoly.

When we say that a physical system is in equilibrium we mean that it is in a steady state, which is a state where all the causal forces within the system are in balance, equal to the outside and so leaves it at "at rest" until and unless it is disturbed by the intervention of some exogenous force. That is what economists have traditionally conceived of as "equilibrium"; they read economic systems as networks of cause-and-effect relationships, just as material systems and the equilibria of such systems are endogenously stable states. As we shall see after discussing evolutionary game theory in the following section, we can reserve the same understanding of equilibrium in the case of game theory. Some have interpreted game theory as an interpretive theory of strategic reasoning. For them, a solution to a game must be an outcome that a rational agent must predict using only rational computational mechanisms. Such theorists face a number of dilemmas about solution concepts that are not so important to behaviorists. We will look at such problems and possible solutions throughout the rest of this article.

We consider a population of M ESPs and a collection of K cryptocurrencies, where each cryptocurrency is associated with its blockchain. We indicate by N(N=1,2,3,..N) the set of miners. There is a finite population of miners, and if a minor changes his strategy this can cause a change within the strategy of other miners. Let K (K=1,2,3..K) be the set of puzzles, each of which related to a special cryptocurrency that the miners are attempting to unravel. Suppose that one cryptocurrency corresponds to precisely one puzzle. Let M (M=1,2,3...M) indicate the ESPs, also mentioned as mining servers, that miners can depend on. A special virtual ESP with index 0 corresponds to an always idle ESP, whose service rate is zero. Miners join ESP 0 after they decide to not join the

mining game.

Notation [31]

Variable

K: Number of blockchains (cryptocurrencies)
M: Number of edge service providers (ESPs)
N: Number of miners (willing to mine using ESPs)
$U_{k,m}$(l): Utility of user mining blockchain k at ESP m
$\gamma_{k,m}$: Mining cost associated to blockchain k at ESP m
$\mu_{k,m}$: Service rate from ESP m requested by each miner to solve puzzle k
Action space and corresponding variables
Si $\subset$ K x M: Corresponding to ESPs that miner i Can use to mine k
$l_{k,m}$: Number of users mining blockchain k at ESP m
l: Strategy profile, l = (l11, l22,...$l_{k,m}$)

Control Variable
Si: si = (k, m) if user i mine blockchain k at ESP m
x_m:Amount bid by ESP m, proportional to the load invested by ESP m for mining

Metrics
$P_{k,m}$: Probability that user is first to mine a block

Strategies. Set **Si $\subset$ K x M**indicates the set of ordered pairs (puzzle, ESP), corresponding to ESPs that miner i can rely on to solve puzzles of a given type. The set Si can differ across miners due to political or economic restrictions. For instance, certain countries do not allow investment in certain cryptocurrencies. Alternatively, the set of available ESPs for two different miners may not be the same. A strategy for miner i is denoted by **si ϵ Si** , corresponding to the puzzle (cryptocurrency) which the miner intends to solve using a given infrastructure. Strategy **si = (k, m)** corresponds to user i using ESP infrastructure m to mine cryptocurrency k. A strategy vector **s=(si)i ϵ N** produces a load vector **l** = $l_{k,m}$**,k,m,** where $l_{k,m}$ denotes the number of miners using ESP m to mine cryptocurrency k. [31]

Mining complexity: We denote by μk,m,i the service rate from ESP m requested by miner i to solve puzzle k. We assume μk,m,i > 0 when m

$\neq 0$, and μk,0,i = 0, for k = 1, ..., K and i = 1, ..., N. For convenience, the service rate is measured:

• In rate of hashes computed per time unit (trials to solve the puzzle per time unit), when accounting for the fine grained adjustment of mining complexity, wherein the average number of puzzles solved per time unit for the whole population is fixed and given, and

• In rate of puzzles successfully solved per time unit, when accounting for the coarse grained adjustment, so as to simplify notation (1).

Let ηk be the load of miners across all ESPs toward cryptocurrency k. Then,

$$\eta\mathbf{k} = \sum\mathbf{m'}\epsilon\mathbf{M}\sum\mathbf{i'}\epsilon\eta\mathbf{k,m',i'}. \quad \mathbf{(1)}$$

In the remainder of this paper, except otherwise noted, we assume that a user who selects a given (ESP, cryptocurrency) pair is allocated a given hash power by the ESP2. Figure 2 illustrates the considered setup. Then, (1) simplifies to:

$$\eta\mathbf{k} = \sum\mathbf{m'}\epsilon\mathbf{Mlk,m'}\eta\mathbf{k,m'}. \quad \mathbf{(2)}$$

Note that (2) is obtained from (1) by lumping the state space: for symmetric users it suffices to track the number of users selecting each of the available (ESP, cryptocurrency) pairs rather than their identities. [31]

For a best understanding about Nash equilibrium point in game theory, we suggest reader to learn [6]. Our main theorem give Nash equilibrium points of this model and our approach to prove the Nash's equilibrium points of this game is to use optimization techniques by doing cumbersome calculations. First, we summarize here the main hypotheses used in this model before announcing the main theorem associated to it. We consider in this paper the following assumptions:

(H) {
- The block's size is not limited ([2]).
- All transactions have fees.
- Miners can not detect the creation of blocks by their opponents (no spy mining).
- There is no protocole changes to delay the transmission of block like in [8] (i.e there is no selfish-mine attack in the network, all miners are honest and follow the protocole)

Figure 5: Hypotheses of Nash equilibrium in mining

Theorem Nash equilibrium point: [32]
1. If c = 0, then the mining game has a unique Nash equilibrium point $x^* = (x1^*, x2^*, \ldots, xn^*)(R^+)^n$with $x1^* = x2^* = \ldots = xn^* = 0$. Moreover,$\forall i \epsilon M \Theta i x^* = \alpha_i.R$.
2.If c > 0 and $\alpha_1 = \alpha_2 = \alpha_3 = .. = \alpha_n = \frac{1}{n}$ then the mining game has a unique Nash equilibrium point$(x^*)^{\rightarrow}$.
More clearly, if$\frac{1}{\lambda.k(1-\alpha_n)} > 0, (x^*)^{\rightarrow} = (\frac{1}{\lambda.k(1-\alpha_n)} else (x^*)^{\rightarrow} = 0^{\rightarrow}$
3. if c > 0, then the mining game has a Nash equilibrium point $x^* = ((x_i)^*)_{i=1,..,n} \epsilon (R^+)^n$. Value of $((x_i)^*)_{i=1,..,n}$ are not explicitly given in this paper. However we will give, for all miner Mi for all fixed profile strategic $x_{-i}^{\rightarrow}$, an interval in which the point x_i^0 which maximizes its reward function, is located.

Our first result is trivial. It signifies that including transactions in a block has the only consequence of extending the period needed for a miner's block to reach consensus. The marginal reward associated with this inclusion is null. Hence, there are only negative incentives for miners to include transactions in blocks. The second result means that the Nash equilibrium points are symmetric. This situation is in line with the idea that when including transactions in 120 blocks, a miner has positive externalities on other miners.

In the third case, there is a large set of parameters for which the only Nash equilibrium of the Bitcoin mining game occurs when no miners include any transactions in their blocks. It is crucial to check for the plausibility of such a set of parameters because when all miners do not include transactions in their blocks, Bitcoin cannot be used for its intended purpose as a payment system. This rationale is one motivation for studying the mining environment.

4.4 Nikaido Isoda function:

The equilibrium problem was first introduced by H. Nikaido, K. Isoda in 1955 with the aim of generalizing the Nash equilibrium problem in non-cooperative games [33]. Specifically, the Nikaido-Isoda function defines the Nash equilibrium of the project management conflict problem described by the Unified Game-based model, which has the following form:

$$f(x^*, x) = \sum_{i=1}^{n} (f_i(x) - f_i(x[y_i]) \qquad [34]$$

Where vector $(x[y_i])$ is the vector obtained by replacing the component xi by yi from the vector x. The notation Ki $\subset$ R is the strategy set of player i. Then the strategy set of the game is: K = K1 x...x Kn. A point $x^*\epsilon$ is called the Nash equilibrium of the game play if:

$$f_i(x^*) = max f_i(x^*[y_i]), \forall y_i \epsilon K i, \forall i \qquad [34]$$

So according to the Nikaido-Isoda bi-function in Nash equilibrium [35], applied to the Unified Game-based model, when finding the value:

$$f(x^*, x) = f(S^*, S) = \sum_{i=1}^{n} (u_i(S_i^*), (S_{-i}^*) - (u_i(S_i), (S_{-i}^*)) \geq 0, \forall S_i \epsilon S_i \qquad [34]$$

In fact, the Nash equilibrium needs to satisfy other constraints and the calculation is based on many factors and data of the problem, so we have things to prove about the existence of Nash equilibrium in project management conflict problems: It can be asserted that if multi-objective evolutionary optimization algorithms converge in the case when the fitness value of the algorithm after a finite number of iterations changes only varies within less than a predefined value of ξ; Project management conflict problems are suitable for linear programming problems with many objective functions (multi-objectives). From there, it is shown that the conflict problems in project management are convergent and both exist in Nash equilibrium.

5 Algorithm with NE:

5.1 Reason to use FEMO algorithm to solve the problem:

Blockchain is a new technology whose purpose is to improve the authenticity of information. The technology is proposed to solve the shortcomings in the business process in the process of asset securities investment. At present, there are many intelligent optimization algorithms, such as non-dominated sorting genetic algorithm (NSGA-II), Pareto envelope-based selection algorithm (PESA-II), strength Pareto evolutionary algorithm (SPEA2), multi-objective particle swarm optimization (MOPSO), and multi-objective artificial bee colony algorithm (MOABC). They have been applied to portfolio optimization. [35]

In terms of MOEAs, fairness relies on the fact that every individual of a population should have the same possibility of being mutated [20]. Compared to other MOEAs, FEMO does not prefer an individual over another one by how close it is to others, like NSGA-II; or any other preference mechanism. This way, the descendants are generated by fairly chosen individuals. This fairness could be good when all the individuals of a population have created approximately the same amount of descendants [36].

5.2 How this algorithm can find Nash equilibria:

Fair evolutionary multiobjective (FEMO) methods employ stochastic operators to a parent population in order to evolve a fitter population. Solving vector valued optimization problems with a child population Given that identifying the whole Pareto frontier [36] is one of the tasks in FEMO, fitness is assigned via Pareto Domination(PD) x If x is strictly no worse off than y in all objectives and x is better, Pareto dominates. ([36], Definition 2.5, pp. 28) than yin at least one objective [36] define Nash Domination as a term akin to PD for the NE problem. The strategies of all N players are concatenated into a chromosome here. A vector Consider two strategy $a, b \epsilon S, (a \equiv (a1, ..., an), b \equiv (b1, ..., bn))$and define an operator k: S x S $\rightarrow$ associating the cardinality of a set defined by $2i \epsilon (1, ..., n) and Ui(bi, a - i) \geq Ui(a), bi = ai(2)$.This set defined by (2) comprises the players that would benefit by playing bi when everyone else plays a-i. The total number of players in this set is given by k(a,b). A similar interpretation applies, mutandis, for k(b,a). Note that to evaluate

k(a,b)and k(b,a), the payoff to each player, individually, from deviating has to be computed. Then in a pairwise comparison of two strategy profile, either one of the following must be true: ([36], Remark 4, pp. 365)
1. k(a,b)¡k(b,a)→a Nash Dominates b or
2. k(b,a)¡k(a,b)→b Nash Dominates a or
3. k(a,b)=k(b,a)→a and bare Nash Non Dominated (NND) with respect to each other.

From the proof ([14], Proposition 9, pp. 366) that all NND chromosomes are NE, all that is required now is to use an EMO algorithm to check for Nash Domination rather than PD. Instead of locating the Pareto Front, the approach would converge to the NE. Approach 1 presents a proposed Nash Domination Evolutionary Multiplayer Optimization (FEMO) algorithm. The approach of [36], which depends on Differential Evolution (DE) [27], is the foundation of FEMO. It should be noted that any alternative FEMO method can be employed. EPECs' Nash Dominance.

5.3 Algorithm, code and diagram of FEMO:

Algorithm:
Input: h, Maxit ,ε , DE Control Parameters, payoff functions
it ←0
Randomly initialize parent strategy profiles P
Evaluate payoff to players with P
Check convergence P

Output: Non-Dominated Nash Solutions The following is how NDFEMO works: The user selects the maximum number of generations Maxit, the population size h, the convergence conditions (> 0), control parameters necessary in DE [37], and a mechanism for computing payoffs. Pare's initial parent strategy profiles were created at random. Then, as stated in [37], child strategy profiles Care are constructed by applying the DE operators to a stochastic combination of randomly chosen parents. Following the Nash Domination technique, parent and child strategy profiles are compared one by one pairwise at each generation. Those that are NND have the potential to be parents for the future generation, therefore if the number of NND chromosomes reaches h, we cull them at random (R)such that only h parents remain. The method is then

continued until either 6 Andrew Koh Maxit is reached or convergence is obtained (as measured by the euclidean norm between a randomly picked chromosome tand the remainder of P). When convergence (measured by the euclidean norm between a randomly chosen chromosome tand the rest of P) is attained, or when Maxit is obtained. **Pseudo Code:**

While it<Maxit or P not converged do
Apply DE operators to create child strategy profile C: CDE←P
Evaluate payoff to miners with C
Perform Pairwise Nash Domination Comparison between P and C:
for j=1 to h **do**
a←Pitj
b←Citj
if $k(a, b) < k(b, a)$ **then**
reject b
R ← a
else if $k(a, b) < k(b, a)$ **then**
reject a
R ← b
else
R ← a
R ← b
end if
It ← It + 1
end for
if size of $R >$ then
Randomly cull R until h remain
P(It+1)←R
end if
Convergence Check:
Randomly choose a chromosome (t)from Pit+1
Compute norm between tand every other member in Pit+1
if norm $\leq \varepsilon$ then
Terminate
end if
it ←it +1
end while

Model:

Without loss of generality, it is hypothesized that all objectives of the problem should be minimized - a minimization type objective can be

converted to a maximization type by multiplying by -1. The K objective minimization problem is defined as follows: given a vector of n-dimensional decision variables **x=x1,. . . ,xn** in the solution space X, find the vector x^* that minimizes the set of K function functions. given target $z(x^*) = z1(x^*), \ldots, zK(x*)$.. The solution space X is generally limited by a series of constraints of the form $gj(x^*) = bj(j = 1, \ldots, m)$. [39]

A feasible solution x is said to dominate the solution y (x y), if and only if, **zi(x)** $\leq$ **zi(y) (i=1,. . . , K)** and **zj(x)** $<$ **zj(y)** in at least one objective j. A solution is said to be Pareto optimal if it is not outperformed by any other solution in the solution space. The set of all possible solutions that are not exceeded in X is called the Pareto optimal set. For a given Pareto optimal set, the corresponding objective function values in the objective space are called Pareto Front.

The goal of multi-objective optimization algorithms is to identify solutions in the Pareto optimal set. In fact, proving that a solution is optimal is often computationally infeasible. Therefore, a practical approach to the multi-objective optimization problem is to find the set of solutions that are the best possible representation of the Pareto optimal set (Best-known Pareto set).
With the above concerns in mind, the multi-objective optimization approach needs to fulfill the following three conflicting criteria well:

+ The Best-known Pareto set should be a subset of the optimal Pareto set.

+ The solutions in the Best-known Pareto set should be evenly and diversely distributed on the Pareto front to provide decision makers with a picture of the reciprocal trade-offs between objectives.

+ The Best-known Pareto front should represent the whole Pareto front.

Given the limited computational time, the first criterion is best accomplished by focusing (intensifying) the search on a particular region of the Pareto front. In contrast, the second criterion requires that the search process be evenly distributed on the Pareto front. The third criterion is aimed at extending the Pareto front at both ends to explore extreme solutions.[39]

Diagram:

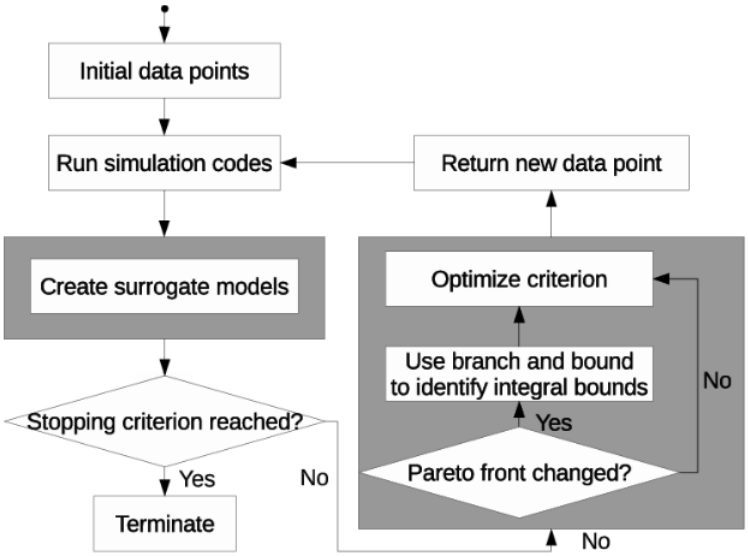

Figure 6: Flow chart of the FEMO algorithm [38]

6 Conclusion:

Cryptocurrency mining brings a huge impact in today's life, they are present everywhere in the market, promising a big step forward for all aspects of life. Over time, from the time it was first developed and conceived to the present time, Cryptocurrencies have proven the possibilities they bring and have gradually been applied in many economic, social, and political aspects,... Along with that development, attack methods to the blockchain are always present, making the issue of information protection always on the top, one of which is selfish mining. Selfish mining offers great potential and promises to improve the productivity and rewards of miners, but the consequences and dangers of selfish mining have been shown through studies and experiments, and they are inevitable. Therefore, through this research paper, we have carefully analyzed the possibilities and proposed specific solutions to bring about possible solutions to this problem.

From the shortcomings of all the papers we have introduced in this research, we solved the problems by empirically building a game model to solve the problem above. We applied the Fair Evolutionary Multi-Objective Optimizer algorithm to find Nash equilibrium and then explained how to solve the problems. Thereby, we showed a new form of selfish mining attack and how it affects blockchain. We also listed more the cons of selfish mining in blockchain, and finally gave satisfactory answers to the problems. The benefits of preventing selfish mining are quite noticeable, as it can bring millions, if not, billions of dollars to the ecosystem if done correctly. Also, preventing selfish mining can inhibit the loss of countless amount of money that has gone undetected by the system, therefore partially eliminate the act of selfish mining as a whole.

References

[1] Robert Sheldon: "A timeline and history of blockchain technology" (09 Aug 2021).

[2] Sharauya Malwa: "The First Bitcoin Transaction Was Sent to Hal Finey 12 Years Ago" (Jan 12, 2021).

[3] Ittay Eayal, Emin Gun Sirer: "Majority is not Enough: Bitcoin Mining is vulnerable" (15 Nov 2013).

[4] Eitan Altman, Daniel Menasché, Alexandre Reiffers, Mandar Datar, Swapnil Dhamal, Corinne Touati, Rachid El-Azouzi: "Blockchain competition between miners: a game theoretic perspective " (24 Jan 2020).

[5] Ren Zhang and Bart Preneel: "Publish or Perish: A Backward-Compatible Defense against Selfish Mining in Bitcoin" (14 February 2017).

[6] Adam Hayes: "Game Theory" (February 02, 2022)

[7] Rocky: "KRYPTON RECOVERS FROM A NEW TYPE OF 51% NETWORK ATTACK" (August 26, 2016)

[8] Dave Gutteridge: "Japanese Cryptocurrency Monacoin Hit by Selfish Mining Attack"(May 22, 2018)

[9] Dr Craig S Wright: "The Fallacy of the Selfish Miner in Bitcoin: An Economic Critique" (29 Apr 2018)

[10] Dash. Harvard. Edu. "The Dynamics of a "Selfish Mining" Infested Bitcoin Network: How the Presence of Adversaries Can Alter the Profitability Framework of Bitcoin Mining." (Feb. 4, 2022)

[11] Zhaojie Wang, Qingzhe Lv, Zhaobo Lu, Yilei Wang and Shengjie Yue: "ForkDec: Accurate Detection for Selfish Mining Attacks" (Feb. 4, 2021.)

[12] Michal Kedziora, Patryk Kozowski, Michal Szczepanik and Piotr Jóźwiak: "Analysis of Blockchain Selfish Mining Attacks" (05 September

2019)

[13] Shiquan Zhang; Kaiwen Zhang; Bettina Kemme : " Analyzing the Benefit of Selfish Mining with Multiple Players" (2-6 Nov. 2020)

[14] Hamid Azimy Ali Ghorbani : "Competitive Selfish Mining" (26-28 Aug. 2019)

[15] Muhammad Saad, Laurent Njilla, Charles Kamhoua, Aziz Mohaisen: "Countering Selfish Mining in Blockchains" (18-21 Feb. 2019)

[16] Qianlan Bai; Xinyan Zhou; Xing Wang; Yuedong Xu; Xin Wang; Qingsheng Kong: "A Deep Dive into Blockchain Selfish Mining" (20-24 May 2019)

[17] Chen Feng; Jianyu Niu : "Selfish Mining in Ethereum" (7-10 July 2019)

[18] Tao Li,Zhaojie Wang,Yuling Chen,Chunmei Li,Yanling Jia,Yixian Yang: "Is semi-selfish mining available without being detected?" (04 October 2021)

[19] Kervins Nicolas; Yi Wang; George C. Giakos: "Comprehensive Overview of Selfish Mining and Double Spending Attack Countermeasures" (23-24 Sept. 2019)

[20] Michal Kedziora, Patryk Kozlowski, Michal Szczepanik and Piotr Jozwiak: "Analysis of Blockchain Selfish Mining Attacks" (05 September 2019)

[21] Shiquan Zhang; Kaiwen Zhang; Bettina Kemme: "Analysing the Benefit of Selfish Mining with Multiple Players" (2-6 Nov. 2020)

[22] Hamid Azimy; Ali Ghorbani: "Competitive Selfish Mining" (26-28 Aug. 2019)

[23] Dr Craig S Wright: "The Fallacy of Selfish Mining in Bitcoin: A Mathematical Critique" (12 Apr 2018)

[24] Dennis Eijkel and Ansgar Fehnker: "A Distributed Blockchain

Model of Selfish Mining" (13 August 2020)

[25] Qing Xia; Wensheng Dou; Fengjun Zhang; Geng Lian: "The Performance of Selfish Mining in GHOST" (20-22 Oct. 2021)

[26] Zhaojie Wang , Qingzhe Lv, Zhaobo Lu, Yilei Wang and Shengjie Yue: "Advances in Security and Performance of Blockchain Systems" (30 Nov 2021)

[27] Euny Hong : " How does Bitcoin Mining work?" (May 05, 2022)

[28] Jake Frankenfield : " Selfish Mining" (February 04, 2022)

[29] M. Laumanns, L. Thiele, E. Zitzler, E. Welzl, and K. Deb, Running time analysis of multi-objective evolutionary algorithms on a simple discrete optimization problem. Springer, 2002.

[30] M. Laumanns, L. Thiele, and E. Zitzler. Running time analysis of multiobjective evolutionary algorithms on pseudo-boolean functions. IEEE Transactions on Evolutionary Computation, 8(2):170–182, 2004.

[31] Eitan Altman, Daniel Menasché, Alexandre Reiffers-Masson, Mandar Datar, Swapnil Dhamal, Corinne Touati and Rachid El-Azouzi : "Blockchain Competition Between Miners: A Game Theoretic Perspective" (17 January 2020)

[32] Moustapha Ba: "With a transaction fee market and without a block size limit in Bitcoin network; there exists a Nash equilibrium point of the mining game" (2020)

[33] Hukukane Nikaido, Kazuo Isoda (1955), "Note on non-cooperative convex game, Pacific Journal of Mathematics", Vol 5. No. 5; tr 907-815

[34] Trinh Bao Ngoc (2020), AP DUNG LY THUYET TRO CHOI VA CAN BANG NASH XAY DUNG PHUONG PHAP MO HINH HOA XUNG DOT TRONG QUAN LY DU AN DAU TU CONG NGHE THONG TIN VA THU NGHIEM TRONG MOT SO BAI TOAN DIEN HINH

[35] YulinDeng, HongfengXu, JieWu: "Optimization of blockchain

investment portfolio under artificial bee colony algorithm" (15 March 2021)

[36] Guillermo Lapuente Valea: "Multi-objective algorithms for the optimization of a sequence of generator matrices in topological quantum computing" (2015)

[37] Andrew Koh:"Nash Dominance with Applications to Equilibrium Problems with Equilibrium Constraints"(19-3-2009)

[38] Ivo Couckuyt, Dirk Deschrijver, Tom Dhaene: "Towards Efficient Multiobjective Optimization: Multiobjective statistical criterions" (Jun 2012)

[39] TOI UU DA MUC TIEU VÀ CAC GIAI THUAT TIEN HOA DA MUC TIEU (hocday.com, November 03, 2017)