A Game Theoretical Approach to Proofs of Useful Work

Alireza Nikpoosh

Iran University of Science and Technology

Abstract

Proof-of-Work (PoW) is a popular blockchain consensus algorithm that is used in cryptocurrencies like Bitcoin. This consensus uses lots of computational power and energy just for securing the blockchain. In order to not waste energy on hashing operations that do not have any other purpose than enabling consensus be tween nodes, Proof-of-Useful-Work (PoUW) is introduced which aims to replace excessive usage of hash functions with tasks that bring additional real-world benefit. This report tries to discuss such proofs, discuss how they can be modeled using game theory on a high level and consider some novel and some previously talked about attacks and threates that protocols using these proofs might face with the level of detail that is expected from a student report.

Contents

1 Introduction **2**
- 1.1 Primecoin . . . 2
- 1.2 Coinami . . . 2
- 1.3 Gridcoin . . . 3
- 1.4 PoDL . . . 3

2 Overview of Game Theory in PoW and PoUW **4**
- 2.1 Terminology . . . 4
- 2.2 Important Games . . . 5
  - 2.2.1 Non-Cooperative Game . . . 5
  - 2.2.2 Stackleberg Game . . . 6

3 Attacks and Challenges **6**
- 3.1 What if the task distributor is also the miner? . . . 6
- 3.2 Sybil Attacks . . . 7
- 3.3 What if miners stick to classical mining? . . . 7
- 3.4 Gradient poisoning attack in PoDLs . . . 7

4 Conclusion **7**

5 Refrences **7**

1 Introduction

Blockchain technology has found successful applications in various fields in recent years and shows potential for even broader use. However, the current mechanism used in blockchain consumes a significant amount of energy to maintain system security, raising concerns about its environmental impact. The Guardian has reported that "The cryptocurrency uses as much CO2 a year as 1 million transatlantic flights," emphasizing the need to address its climate impact. Forbes has also stated that "Bitcoin's need for electricity is its Achilles Heel". According to research, the energy consumption of Bitcoin has steadily increased, even though there was a sudden drop in Bitcoin's price in late November 2018 and a lesser one in May 2021. Currently, more than 50 TWh per year is consumed solely for maintaining the Bitcoin blockchain, and the total energy consumption of all blockchain applications is expected to be much higher. This amount is more than 170 times the consumption by traditional credit cards which can further complicate the wide integration of such networks. The main issue lies in the wastefulness of energy, particularly in the hash calculation process of Proof-of-Work (PoW) based blockchains. Although alternatives like Proof-of-Capacity (PoC), seen in cryptocurrencies like Burstcoin, aim to address the problem, they still result in resource wastage, such as storage. To this day, Proof-of-Useful-Work might be the best alternative consensus to traditional POWs. In the following paragraphs, we will discuss some notable examples of PoUWs.

1.1 Primecoin

Primecoin is a PoUW cryptocurrency that was launched in 2013 by Sunny King. Its PoUW consists of finding certain types of prime number chains, so-called Cunningham and bi-twin chains. Cunningham chains are a series of prime numbers that nearly double each time. In mathematical terms, a prime chain of length $n \in \mathbb{N}$ must fulfill

$$p_i + 1 = 2p_i + 1$$

to be considered a first-order chain or

$$p_i + 1 = 2p_i - 1$$

to be considered a second-order chain for all $1 \leq i < n$. For instance, $\{41, 83, 167\}$ is a first-order chain of length $n = 3$ and $\{7, 13\}$ is a second-order chain of length $n = 2$. In addition to Cunningham chains, the third type of chain that Primecoin allows as proof-of-work are bi-twin chains. These are prime chains that consist of a strict combination of first and second-order Cunningham primes. The mathematical definition of a bi-twin chain of length $k + 1$ is the sequence $\{n - 1, n + 1, 2n - 1, 2n + 1, 2^2n - 1, 2^2n + 1, ..., 2^kn - 1, 2^kn + 1\}$. For instance, choosing n = 6 leads to $\{5, 7, 11, 13\}$ which is a bi-twin chain of length 2 that consists of 4 prime numbers.

1.2 Coinami

In 2016, a theoretical proposal of a mediator interface for a volunteer was published and named Coinami. The PoUW of Coinami is built on DNA sequence alignment (High Throughput Sequencing read mapping in particular) and aims to generate and analyze

huge datasets of disease signatures which can help us to gain a better understanding of diseases such as different cancer variants. The authors of Coinami describe their approach as a three-level multi-centric system that consists of a root authority, sub-authorities, and miners. Miners download problem sets from sub-authorities, map HTS reads to a reference genome and send the results back to sub-authorities for verification. Sub-authorities are certified by the root authority. As a result, this approach can be seen as a hybrid of Proof-of-Authority (PoA) and Proof-of-Useful-Work (PoUW) consensus algorithms. there currently exists no cryptocurrency that is connected to this academic proposal.

1.3 Gridcoin

Gridcoin is an open-source multi-incentive permissionless blockchain that mints and distributes cryptocurrency to various contribution-based and point-accruing systems. It currently distributes currency according to the relative processing power a network participant directs toward data-driven analysis and scientific discovery across the Berkeley Open Infrastructure for Networked Computing and Folding@Home. The Gridcoin blockchain is secured through the proof-of-stake v2 protocol and utilizes several mechanisms to assure network, data, identity, and economic security.

1.4 PoDL

Hoffmann presented a proof-of-concept design of an energy recycling blockchain with its novel PoDL mechanism. Miners perform training tasks of deep learning instead of hash calculation, and they present trained DL models as their proof of deep learning. Model stealing and overfitting are prevented by their block acceptance policy with separated phases. Without a majority of DL training power, double spending is hard even if the majority of full nodes are malicious. In Figure 1 a toy example of such a network is illustrated. PoDL and similar optimization proofs are the main focus of this report.

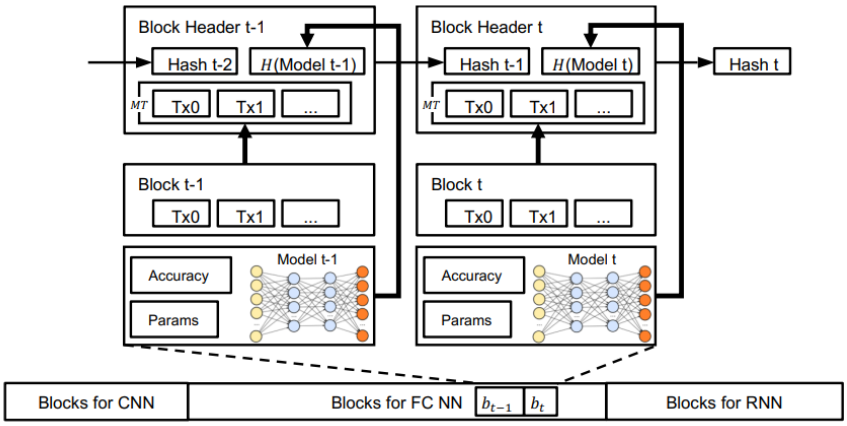

Figure 1: A toy example that trains CNN, Fully Connected NN, and RNN. (MT stands for the root of the Merkle tree)

2 Overview of Game Theory in PoW and PoUW

In a blockchain network, achieving consensus among nodes is a fundamental requirement, and a reliable consensus protocol should possess three certain properties: correctness, consistency, and traceability. Correctness ensures that nodes adopt the content and order of transactions in the confirmed canonical blockchain structure. Consistency guarantees that nodes update their local blockchain structures when a new block header is confirmed. Traceability ensures that all transactions can be traced back to the genesis block for confirmation.

However, disagreements can arise among nodes in certain cases, such as when the local blockchain replicas of nodes cannot be synchronized simultaneously due to network delays. This can result in different blockchain ledgers and the formation of fork chains, deviating from the protocol of maintaining the longest chain. To address this, the blockchain consensus protocol should be incentive-compatible. This means that any node that deviates from the protocol will suffer financial loss, such as a waste of investment in computing power. In other words, **it should be economically disadvantageous for nodes to deviate from the protocol**.

The mining mechanism in the Nakamoto protocol relies on both cryptography and game theory. While the PoW protocol is widely adopted, its incentive compatibility has been openly questioned from a game theoretical perspective. This is because achieving Nakamoto consensus involves nodes joining the network, executing the protocol, and maintaining the ledger. Nodes may be incentivized to deviate from the protocol to increase their own utilities. e.g. The Selfish Miner attack.
The same is also true for PoUW protocols. In the following pages, we will try to examine these protocols by considering two important games; but first, we need to review some terminology and define what exactly a "game" is.

2.1 Terminology

To analyze the interactions among consensus nodes in blockchain networks, game theoretical models are employed. These models aim to study the strategic behaviors and incentives of nodes in the consensus process. They help in understanding the dynamics and outcomes of the interactions among nodes and provide insights into the incentive compatibility and stability of the consensus protocol. Game theory provides mathematical tools for analyzing the interactions among rational decision-makers. In a game, each player chooses a strategy to maximize their utility, considering the strategies chosen by other players. In the context of blockchain networks, game theory has been widely applied to analyze interactions and decision-making processes. Here are some important terminologies related to game theory that will come in handy:

Player: A player refers to a decision-maker in the game. In the blockchain context, players can be miners, mining pools, or blockchain users.

Utility: Utility represents a player's expected outcome, payoff, interest, or revenue. It reflects the player's assessment of the value or benefit they derive from a particular strategy.

Strategy: A player's strategy comprises a set of actions, choices, or decisions that they can make to achieve their expected outcome. The player's utility is determined based on their own strategy as well as the strategies chosen by other players.

Rationality: A player is considered rational if they always act in a self-interested manner, aiming to maximize their own payoff. Rationality assumes that players make decisions based on their perceived self-benefit.

2.2 Important Games

2.2.1 Non-Cooperative Game

In non-cooperative game models, players determine strategies independently without coordination. While considering others' probable actions, players have no means to communicate or jointly plan strategies. Each player autonomously chooses actions solely based on individual incentives within gameplay confines. While interaction occurs naturally as players anticipate the consequences of uncoordinated choices, the "non-cooperative" label stems from the lack of cooperation on agreed strategies.
Consider a blockchain network in which miners as the players invest strategically in computational power to compete for a reward from mining successfully. The miners are rational and the non-cooperative game can be used to model the interaction among the miners. Assume that there are N miners, i.e., players, and M_i is a set of strategies of miner i, where $M = M_1 \times M_2 \times \ldots \times M_N$ is the Cartesian product of the sets of individual strategies. Let $m_i \in M_i$ be the strategy of miner i. A vector of strategies of N miner can be defined as $m = (m_1, \ldots, m_N)$ and a vector of corresponding payoffs can be defined by $\boldsymbol{u} = (u_1(m), ..., u_N(m)) \in \mathbb{R}^N$, where $u_i(p)$ is the utility of player i, for example, mining rewards or the transaction fees, given the miner's chosen strategy and the strategies of the others. Each miner chooses its best strategy m^* to maximize its utility. A set of strategies $m^* = (m_1^*, \ldots, m_N^*) \in m$ is the Nash equilibrium if no miner can gain higher utility by changing its own strategy when the strategies of the other miners remain unchanged, that is:

$$\forall i, m_i \in M_i : u_i(m_i^*, \bar{\mathbf{m}}_i^*) \geq u_i(m_i, \bar{\mathbf{m}}_i^*)$$

where $\bar{\mathbf{m}}_i = (m_1, ..., m_i - 1, m_i + 1, ..., m_N)$ is a vector of the strategy of all miners except miner i. This inequality demonstrates the equilibrium state of the game. At the Nash equilibrium, the players have no incentive to deviate from their current strategies. However, there may exist no Nash equilibrium in some cases, or multiple equilibria in other cases. Thus, it is important to check the existence and uniqueness of the Nash equilibrium to analyze a non-cooperative game. The existence and uniqueness of equilibrium theory demonstrates that the strictly concave game can achieve the unique equilibrium asymptotically. Here, the concave game means that the utility functions of players are concave, and this can be proved by computing the second-order derivative of the utility function. The non-cooperative theory can be applied to a broad range of blockchain-based scenarios.
In the case of PoDLs, Game models could analyze how miners allocate computing resources between training different machine learning models. Also, interactions where miners choose between different ML training pools can be modeled considering that factors like hardware resources, model types supported, and reward structures impact optimal pool selection strategies. Furthermore, Scenarios can be discussed where miners selectively validate only certain trained models that might require less computing power.

2.2.2 Stackleberg Game

the Stackelberg game is a game that involves a certain predefined ordered strategies by players. In the Stakelberg game, the players are divided into the leaders and the followers. The followers decide their strategies after observing the strategies of the leaders. Both the leaders and the followers are typically rational and aim to maximize their own utilities. You can see how this can be useful in modeling players of PoUW networks where pooling can be occur frequently due to the existence of ASICs. To understand how the Stackelberg game works, we consider a blockchain relying on edge computing network, which involves two players, i.e., the service provider and the miner. The service provider possesses the computational power which can be offered to the miner as service, and the provider can set the service price to charge the fee for profit. The miner optimizes its demand of computational power to the provider to maximize its utility, taking its cost into account. As such, the service provider sets the price first, and then the miner decides its demand. Thus, the Stackelberg game can be used to model the interaction between the service provider and the miner. Assume M_1 and M_2 are the sets of strategies of the service provider and the miner, respectively. The service provider chooses its strategy p1 from set P1 to maximize its utility $u_1(m_1, m_2)$, and the miner chooses its strategy m_2 from set m_2 to maximize its utility $u_2(m_1, m_2)$. The optimization problems of the leader and the follower together form the Stackelberg game. The objective of analyzing such a game is to find a Stackelberg equilibrium . Since the leader first takes its strategy and then the follower chooses its strategy, the Stackelberg strategy guarantees the service provider to achieve its payoff at least as much as the corresponding Nash equilibrium. The reason is that when choosing the Stackelberg strategy, the service provider actually optimizes its decision which will maximize its utility. This feature makes the Stackelberg game suitable for many scenarios in blockchain based applications. For example, the Stackelberg game is adopted for setting transaction fees and selection of miners for verification [43], determination of cyber-insurance price, and analyzing the supply-demand relationship in the blockchain based edge computing platform.

3 Attacks and Challenges

3.1 What if the task distributor is also the miner?

A novel threat that I thought of describes a scenario where the entity that requests a certain task in PoUW networks(where the task is not necessarily pre-determined) can also mine with its computing power in a certain pool to achieve the same task. It's clear that the client has an initial incentive to invest resourses on the achievement of it. The requester has every reason to take advantage of such a scenario to increase its chances of getting the block reward while essentially making everyone that doesn't have the same incentive do free labor.
increasing the number of clients would be one approach to make this less likely. Furthermore, in networks such as PoDL the training can be done with smaller models that will be combined by some method similar to Ensemble Learning.

3.2 Sybil Attacks

Bad actors can setup several Sybils on the network to collectively generate a bad model. They could also perform cheap work by replicating only one unit of work across all controlled nodes. To avert this attack, worker nodes are not allowed to pick tasks themselves, they only state their preferences. By doing so, they also cannot pick easy tasks.

3.3 What if miners stick to classical mining?

To avoid such a scenario, we can constrain the number of nonces to make classical mining insignificant. A miner that would do bogus work and focus only on mining would be unable to prove the validity of the produced blocks. Bogus work includes: echoing received weight updates, leaving the task before completion or not following the steps. It is economically damaging to the miners to engage in such behaviours because they would lose their stake and wouldn't receive any fee from the client anyway.

3.4 Gradient poisoning attack in PoDLs

Gradient poisoning is a type of attack in which a miner tries to skew the learning process by sending huge or fake gradients. Sending the same message multiple times is also a type of poisoning (spam). Supervisors can watch for this attack and add the malicious worker node to a blacklist which they expose publicly. Fellow nodes will ignore the gradient updates from the bad miners and evaluators will confiscate their stakes. Also, miners will not apply multiple IT RES messages corresponding to the same iteration. To turn away miners that do not make progress, validators require that a lucky miner must prove that his/her local model improved over previous iterations.

4 Conclusion

We have successfully demonstrated how PoUWs operate, how we can use game theory to model different aspects of such networks and how these proofs are still vulnerable in many ways to traditional and nontraditional attacks and threats. Although this report is conducted on a high-level, there is a room to investigate every discussed topic on a more detailed and mathematically sound way in a new paper without the constricted time.

5 Refrences

- A Proof of Useful Work for Artificial Intelligence on the Blockchain
- A Survey on Blockchain: A Game Theoretical Perspective
- Challenges of Proofs-of-Useful-Work
- Energy-recycling Blockchain with Proof-of-Deep-Learning
- Proof-of-Learning: a Blockchain Consensus Mechanism based on Machine Learning Competitions