Block Rewards, Not Transaction Fees Keep Miners FaithfulIn Blockchain Protocols

by

Anurag Jain, Sujit Prakash Gujar

Report No: IIIT/TR/2021/-1

Centre for Visual Information Technology
International Institute of Information Technology
Hyderabad - 500 032, INDIA
January 2021

Block Rewards, Not Transaction Fees Keep Miners Faithful In Blockchain Protocols

Anurag Jain[0000−0002−4637−4708] and Sujit Gujar[0000−0003−4634−7862]

Machine Learning Lab,
International Institute of Information Technology, Hyderabad, India
anurag.jain@research.iiit.ac.in , sujit.gujar@iiit.ac.in

Abstract. Blockchain is a distributed system that achieves distributed consensus even in the presence of Byzantine adversaries as long as the majority of the nodes are honest. It is able to ensure this majority with the help of game theory by rewarding miners that behave honestly. These miners are either rewarded via block rewards for each block they mine or transaction fees for every transaction they include in their block.
However, it is difficult to ensure that a blockchain protocol is incentive-compatible which is highlighted by the discovery of multiple incentive-driven deviations such as selfish-mining and undercutting that not only yield more reward but are also a threat to the security of the blockchain. Since miners are themselves invested in the cryptocurrency, we make the hypothesis that they would not collude in a manner that could hurt the security and value of the cryptocurrency. Under this hypothesis, we call a protocol a *faithful implementation* if following the protocol is a Nash Equilibrium if all other miners also follow the protocol.
We then show that Bitcoin is a faithful implementation only with block rewards and not with transaction fees. We also extend our results for a general blockchain protocol and show that not only can no protocol be a faithful implementation in a setting with transaction fees but we also show that any blockchain protocol is a faithful implementation in a setting with block rewards if it provides sufficient block rewards.

Keywords: Game Theory · Blockchain Mining Games · Faithful Implementation

1 Introduction

Blockchain is a system that allows nodes to achieve distributed consensus in an environment with Byzantine adversaries with the help of incentive engineering, i.e., game theory. In a blockchain protocol, the participating users are provided with an incentive to behave honestly via mining rewards. Hence, a blockchain protocol must be incentive compatible in order to ensure that all miners behave honestly, i.e., in an ideal blockchain protocol, following the protocol must be the equilibrium strategy among all possible strategies to guarantee safe operation and discourage the miners from adopting any other strategy that could yield them a greater reward.

In this paper, we describe the conditions under which a protocol is able to provide an appropriate incentive to the participating miners to not only act honestly but also to prevent them from leaving the system. Researchers try to ensure that in the blockchain protocol that they design, following the protocol is the equilibrium strategy for the miners. However, a complete analysis of all possible mining strategies is often intractable, which could lead to the possibility of incentive-driven deviations in the blockchain protocol. Many researchers have explored both attacks on Bitcoin's incentive mechanism [4, 7, 12, 15, 22] as well as other cryptocurrencies [11, 17]. However, we remark that no such deviation has been observed in the wild despite being widely known for a few years.

We make the Anti-Collusion Hypothesis in which we claim that the miners do not collectively deviate via collusion since it could lead to a loss of trust in the system, reducing the value of the cryptocurrency itself. Making this assumption, we significantly reduce the set of possible strategies that the miners would practically consider for deviation. Hence, we could do a complete game theoretic analysis of mining strategies to discover any incentive-driven deviations. Thus, a blockchain protocol is practically safe against incentive-driven deviations by miners if following the protocol is the best response if all other miners are following the protocol. We call such a protocol in which following the protocol is the Nash Equilibrium for all miners as a *faithful implementation*.

We analyze the Bitcoin protocol and show that it is a faithful implementation only in the case where the miners draw their reward from block rewards but not in the case where the miners draw their reward from the transaction fees. Next, we show that it is not a mere coincidence and analyze both the sources of reward for a general blockchain protocol to show that a blockchain protocol cannot be a faithful implementation if the rewards are drawn from transaction fees. In contrast, a protocol in which the miners draw reward from block rewards is a faithful implementation if it provides sufficient block reward. Thus, blockchain protocols should reward miners via block rewards instead of transaction fees.

Hence, in this work, we:

1. Introduce the Anti-Collusion Hypothesis in Section 3.1, followed by the formal definition of faithful implementation in Section 3.2.
2. Analyze the Bitcoin protocol in Section 4, first in a setting with block rewards and then in a setting with transaction fees.
3. Show that any blockchain protocol can be a faithful implementation in a setting with only block rewards (Theorem 3).
4. Show that no blockchain protocol can be a faithful implementation in a setting with only transaction fees (Theorem 4).

2 Related Work

Amoussou-Gueno et al. [3] analyze the game-theoretic equilibrium between rational and Byzantine players in a consensus-based blockchain, whereas we consider only rational miners in a proof-of-work based blockchains. Our result from Theorem 1 matches with Kroll et al. and Ewerhart [6, 13] since we find that Bitcoin Mining is indeed a Nash Equilibrium in a setting where miners have perfect information about all mined blocks.

Eyal et al. and Sapirshtein et al. [8,22] prove very pessimistic thresholds on the fraction of honest nodes needed to guarantee security properties due to the presence of incentive-driven deviations. We assume that such deviations are not practical since the miners are also invested in the cryptocurrency (Anti-Collusion Hypothesis).

Siddiqui et al. [23] propose BitcoinF, a modification to the Bitcoin protocol that ensures a minimum transaction fee in a transaction fee-only model, but they assume a constant influx of transactions. With this, this is same as having some minimum block reward. We show that in case the number of unconfirmed transactions declines, it would not be feasible to continue mining in Bitcoin, or BitcoinF or any blockchain protocol. Pass et al. [18] describe a fair protocol in which miners are not only incentivized to append blocks to the blockchain but also confirm transactions independently in the form of "fruits". They use a reward scheme in which the transaction fees is averaged over blocks, and we show that due to Theorem 4, their protocol is not a faithful implementation.

3 Definitions

Definition 1 (Miner's Utility). *The miner's utility for mining a block could be defined as* $u(\sigma) = P(\text{the block is accepted}) \times r_{block} - C_{mining}$ *where* $P(\text{the block is accepted})$ *is the probability of a block being accepted in the main chain in a given time period,* r_{block} *is the reward earned by the miner for the block, and* C_{mining} *is the cost of mining in a given time period.*

3.1 Anti-Collusion Hypothesis

It is well-known that the value of a blockchain-based cryptocurrency is derived from the fact that the cryptocurrency is safe against malicious adversaries [2, 10, 20]. A blockchain that is vulnerable to a double-spend attack by an adversary would not be able to provide any value to the cryptocurrency since no merchant would be willing to exchange goods for the cryptocurrency fearing a double-spend attack rendering the cryptocurrency worthless. If some miners collectively deviate from the blockchain protocol, it may lead to a reduction in the resilience of the protocol against Byzantine adversaries, consequently reducing the perceived value of the reward (i.e., real-world value of the reward, for instance, the price of Bitcoin in US Dollar). In a blockchain, the participating miners are provided with rewards in the same cryptocurrency as an incentive to act honestly. Hence, miners collectively try to maintain the security of the cryptocurrency to protect the perceived value of the reward, which implies that rational miners at least would not collude to deviate from the honest strategy.

Definition 2 (Anti-Collusion Hypothesis). *Bitcoin miners would not collectively deviate from following the protocol if their collusion could hurt the perceived value of the cryptocurrency. Hence,*

$$u_i(\sigma_i, \sigma_{-i}) = -C_{mining} \quad \forall \sigma_{-i} \neq \pi_{-i}$$

where π_i *is the strategy played by the player* i *in which he/she is following the protocol,* $u_i(\sigma_i, \sigma_{-i})$ *utility of player* i *when he/she plays* σ_i *while all other players play* σ_{-i}*, and* C_{mining} *is the mining cost associated with mining in an epoch (introduced in Section 3.4).*

3.2 Faithful Implementation

A protocol Π is said to be *faithful implementation* if the revenue yielded by a miner to follow the protocol honestly is not less than the optimal revenue, if all others are following the protocol honestly as well.

Definition 3 (Faithful Implementation). *A protocol* Π *is said to be* Faithful Implementation *if* $\forall i$

$$u_i(\pi_i, \pi_{-i}) \geq u_i(\sigma_i, \pi_{-i}) \quad \forall \sigma_i \in \Delta(S_i)$$

where $\Delta(S_i)$ *is the set of strategies that the player* i *can take.*

Remark 1 Since the miners can possibly shut down their mining operation if $u_i(\pi_i, \pi_{-i}) < 0$, quitting $\in \Delta(S_i)$ where $u_i(\text{quitting}, \pi_{-i}) = 0$. The resilience of the blockchain against a Byzantine adversary is proportional to the computational power invested by the miners, hence if the miners leave the system, the security of the blockchain is negatively impacted. Therefore,
Π is faithful implementation $\implies u_i(\pi_i, \pi_{-i}) \geq 0$.
Notice that a protocol in faithful implementation not only incentivizes them to act honestly but also motivates them to join the mining ecosystem in the first place.

Definition 4 (Rational Agent). *An agent is said to be a* rational player *if it may strategically deviate from the protocol rules if the deviation is expected to yield a higher reward.*

Definition 5 (Adversarial Agent). *An agent is said to be an* adversarial player *(and sometimes also known as "Byzantine" in the literature) may also strategically deviate from the protocol. However, the adversary's goal is to disrupt the operation of the protocol, and it does* ***not*** *try to maximize its reward.*

3.3 Blockchain

A blockchain $\mathbb{B}$ can be defined by the tuple $(B, \prec, M)$ where B is the set of blocks, $\prec$ is the parent-child relation, M is the mapping of miners to the blocks. This general definition allows us to include all DAG-based blockchain protocols such as IOTA [21], SPECTRE [24], Mneme [5], etc. Formally,

- $B = \{b_0, b_1, \ldots, b_n\}$ where each block is said to be valid *iff* it has a hash value less than the target.
- $\prec$ is a relation over B that defines the ordering of the blocks. $\prec$ is defined as follows: (i) $x \prec y$ if y contains a hash pointer to x, and (ii) $x \prec y$ and $y \prec z \implies x \prec z$, i.e., $\prec$ is a transitive relation.
- $M : B \to \mathcal{N}$ is the function that maps blocks to miners.

Garay et al. [9] show that any system that satisfies the Persistence and Liveness properties can be used to build a distributed ledger. Hence, a blockchain could be used to build a distributed ledger as follows:

- A transaction is said to be valid *iff* (i) it is included in a block $b_o \in B$, (ii) the inputs to the transaction are included in a block b_i precedes b_o ($b_i \prec b_o$) (iii) All other transactions that refer to the same inputs are present in blocks that follow b_o. Hence, only the first transaction is considered valid.
- Majority of the miners should mine on the maximal block, to ensure the *liveness* and *persistence* properties.
- In case two valid transactions are in that are in blocks b and b' such that they are not comparable, there must be a conflict resolution rule that should "pick" the transaction that appeared earlier in time. This is the most challenging part in designing a blockchain protocol, and many protocol designers take different approaches in specifying this rule. We would assume a general conflict resolution rule $\mathcal{C}(x, y)$ exists that returns the block that appeared earlier between x or y.

3.4 Reward Model

There are two principal ways of rewarding the nodes participating in a blockchain system:

1. *Block Reward* - The reward miners can assign to themselves for mining a block. This reward mints new currency, adding to the total amount of currency in circulation. This reward can be fixed by the protocol designers, which would allow them to pick a suitable value that could offset the mining costs borne by the miner.
2. *Transaction Fees* - This is the fee offered by the users for miners' services by providing incentives to include their transactions in the blocks. Typically, the users are allowed to decide the transaction fees they wish to offer while creating a transaction. Although protocol designers may enforce a minimum transaction fee (e.g. BitcoinF [23]), they cannot ensure that there are enough unconfirmed transactions to include in a new block.

We assume that the blockchain protocol additionally specifies a reward function $R : B \to \mathbb{R}$ that specifies the reward assigned to the miners.

The cost associated with mining a block, C_{mining} is assumed to be proportional to the computational power δ. Thus, we say $C_{\text{mining}} = \alpha\delta$. This cost is assumed to remain same irrespective of the strategy adopted by the miner, however, a miner that does not mine or shuts down the mining operation does not bear this cost.

4 Bitcoin Results

Bitcoin is a cryptocurrency protocol [16] that is arguably the most successful in terms of market capitalization and mass adoption. Bitcoin miners are rewarded via block rewards which halve every 210,000 blocks. Once the block rewards become negligible, it is expected that the miners would be rewarded by Transaction Fees instead. Currently, miners draw a fraction of their reward from the transaction fees, but the majority of the reward comes in the form of Block Rewards.

We show that Bitcoin is a faithful implementation in the setting where miners draw a majority of their reward from block rewards but we cannot say the same about the setting where miners draw a majority of their reward from the transaction fees. Bitcoin is a blockchain protocol Π_{Bitcoin} which specifies the conflict resolution rule $\mathcal{C}_{\text{longest\_chain}}$ in which the block which is the part of the longer chain is picked over other blocks. We consider two reward schemes in Bitcoin, block rewards only ($R(b) = r\ \forall b$), and transaction fees only ($R(b) = \text{TxFees}(b)$ where $\text{TxFees}(b)$ is the cumulative transaction fees of the transactions included in the block b). Initially, Bitcoin was "bootstrapped" via block rewards but it will eventually converge to a transaction fees only model.

Theorem 1 (Bitcoin in Block Rewards). *In a setting in which the miners derive their reward from Block Rewards, Bitcoin is a faithful implementation if $r \geq \alpha$ where r is the fixed block reward and α is the coefficient of mining cost ($C_{mining} = \alpha\delta$).*

A formal proof for Theorem 1 is provided in Appendix A.

Notice that a rational miner will only participate in the system if the expected reward is greater than the cost of mining a block, which implies that if the block reward is reduced, some miners will quit mining. This result is consistent with the observation that we always observe a sharp drop in the network hash rate in Bitcoin each time the block reward is halved [14]. In the most recent example, when the Bitcoin block reward was halved on 11^{th} May 2020, the estimated network hash rate declined by about 25%[1]. However, since Bitcoin readjusts the mining cost after every two weeks, the network hash rate started to recover after 26^{th} May 2020 when Bitcoin reduced the difficulty of mining [1].

Theorem 2 (Bitcoin in Transaction Fees). *In a setting in which the miners derive majority of their reward from transaction fees, Bitcoin is not be a faithful implementation.*

A formal proof for Theorem 2 is provided in Appendix B.

5 Universal Results

Theorem 3 (Block Rewards Faithfulness). *Any blockchain protocol where the miner derives majority of revenue only from block rewards is a faithful implementation if $r \geq \alpha$ where r is the fixed block reward and α is the coefficient of mining cost ($C_{mining} = \alpha\delta$).*

[1] This observation prompted the authors to write this paper.

In case of fixed block rewards, no matter where the miner mines the block, he receives the same reward. Therefore, mining the maximal block is the best response strategy. Formal proof for Theorem 3 is provided in Appendix C.

Notice that a protocol designer could always pick suitable block reward r that exceeds α.

Theorem 4 (Transaction Fees Impossibility). *Any blockchain protocol where the miner derives majority of revenue only from transaction fees can not be a faithful implementation.*

Theorem 4 assumes a general blockchain protocol in which the transaction fees may not only come from the transactions included in the newly mined block but also from previously mined blocks. This includes some protocols such as FruitChain [19] that average the miner's reward over multiple blocks. A formal proof is provided in Appendix D. The intuition for the proof lies in the fact that no matter how to protocol rewards the miners, it would have a fixed pool of rewards accumulated throughout the execution of the protocol most of which would have already been distributed to the miners of existing blocks. If the total transaction fees accumulated by the miners is lesser than the reward offered to the miners, this pool of reward would keep on reducing until it exhausted. Once the pool of rewards is exhausted, no further reward can be distributed to the miners who still need to pay their mining costs. Hence, their utility becomes negative.

6 Conclusion

In this paper, we introduced the notion of a faithful implementation and illustrated the conditions under which Bitcoin is a faithful implementation. Under a faithful implementation, a blockchain protocol incentivizes miners not only to behave honestly but also to keep participating in the system. We then proved that any blockchain protocol could be a faithful implementation in a setting where miners draw their reward from block rewards but not in a setting where miners draw their reward from transaction fees. Therefore we conclude that while designing blockchain protocols, researchers should preferably use block rewards for rewarding miners rather than transaction fees.

6.1 Future Work

Although we covered the analysis of Bitcoin protocol in a general setting with a fixed cost of mining C_{mining}, in practice it varies with the mining difficulty which is periodically readjusted. Therefore, if expected utility by mining Bitcoin is positive, more rational miners would join the mining ecosystem, which would increase the difficulty and consequently drive up the cost of mining. This could reduce the expected utility for all miners and prevent new miners from joining the system or cause some miners to leave the system. Since the reward is measured in terms of the cryptocurrency but the mining costs lie in terms of a real-world value, the utility would vary with the perceived value of the currency. We leave a more detailed analysis of the economics of Bitcoin mining for future work to explore.

We also introduced the hypothesis that claims blockchain miners would not collude if their collusion could hurt the perceived value of the cryptocurrency (Anti-Collusion Hypothesis). We leave future researchers to analyze this hypothesis in terms of behavioural economics and explore the relationship between the security of a cryptocurrency and its perceived value.

References

1. Blockchain Charts (2020 (accessed November 20, 2020)), https://www.blockchain.com/charts/hash-rate
2. Alabi, K.: Digital blockchain networks appear to be following metcalfe's law. Electronic Commerce Research and Applications **24**, 23 – 29 (2017). https://doi.org/https://doi.org/10.1016/j.elerap.2017.06.003, http://www.sciencedirect.com/science/article/pii/S1567422317300480
3. Amoussou-Guenou, Y., Biais, B., Potop-Butucaru, M., Tucci-Piergiovanni, S.: Rational vs byzantine players in consensus-based blockchains. In: Proceedings of the 19th International Conference on Autonomous Agents and MultiAgent Systems. p. 43–51. AAMAS '20, International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC (2020)
4. Carlsten, M., Kalodner, H., Weinberg, S.M., Narayanan, A.: On the instability of bitcoin without the block reward. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. pp. 154–167 (2016)
5. Chatzopoulos, D., Gujar, S., Faltings, B., Hui, P.: Mneme: A mobile distributed ledger. In: IEEE INFOCOM 2020 - IEEE Conference on Computer Communications. pp. 1897–1906 (2020). https://doi.org/10.1109/INFOCOM41043.2020.9155497
6. Ewerhart, C.: Finite blockchain games. Economics Letters **197**, 109614 (2020)
7. Eyal, I.: The miner's dilemma. In: 2015 IEEE Symposium on Security and Privacy. pp. 89–103. IEEE (2015)
8. Eyal, I., Sirer, E.G.: Majority is not enough: Bitcoin mining is vulnerable. In: International conference on financial cryptography and data security. pp. 436–454. Springer (2014)
9. Garay, J., Kiayias, A., Leonardos, N.: The bitcoin backbone protocol: Analysis and applications. Cryptology ePrint Archive, Report 2014/765 (2014), https://eprint.iacr.org/2014/765
10. He, J., Zhang, G., Zhang, J., Zhang, R.: An economic model of blockchain: The interplay between transaction fees and security. Available at SSRN 3616869 (2020)
11. Hou, C., Zhou, M., Ji, Y., Daian, P., Tramer, F., Fanti, G., Juels, A.: Squirrl: Automating attack discovery on blockchain incentive mechanisms with deep reinforcement learning. arXiv preprint arXiv:1912.01798 (2019)
12. Judmayer, A., Stifter, N., Zamyatin, A., Tsabary, I., Eyal, I., Gazi, P., Meiklejohn, S., Weippl, E.R.: Pay-to-win: Incentive attacks on proof-of-work cryptocurrencies. IACR Cryptol. ePrint Arch. **2019**, 775 (2019)
13. Kroll, J.A., Davey, I.C., Felten, E.: The economics of bitcoin mining, or bitcoin in the presence of adversaries (2013)
14. Lasi, D., Saul, L.: A system dynamics model of bitcoin: Mining as an efficient market and the possibility of "peak hash" (2020)
15. Liao, K., Katz, J.: Incentivizing blockchain forks via whale transactions. In: International Conference on Financial Cryptography and Data Security. pp. 264–279. Springer (2017)
16. Nakomoto, S.: Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf
17. Neuder, M., Moroz, D.J., Rao, R., Parkes, D.C.: Selfish behavior in the tezos proof-of-stake protocol. arXiv preprint arXiv:1912.02954 (2019)
18. Pass, R., Shi, E.: Fruitchains: A fair blockchain. In: Proceedings of the ACM Symposium on Principles of Distributed Computing. pp. 315–324 (2017)
19. Pass, R., Shi, E.: Fruitchains: A fair blockchain. In: Proceedings of the ACM Symposium on Principles of Distributed Computing. p. 315–324. PODC '17, Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3087801.3087809, https://doi.org/10.1145/3087801.3087809
20. Peterson, T.: Metcalfe's law as a model for bitcoin's value. Alternative Investment Analyst Review Q **2** (2018)
21. Popov, S.: The tangle

22. Sapirshtein, A., Sompolinsky, Y., Zohar, A.: Optimal selfish mining strategies in bitcoin. In: International Conference on Financial Cryptography and Data Security. pp. 515–532. Springer (2016)
23. Siddiqui, S., Vanahalli, G., Gujar, S.: Bitcoinf: Achieving fairness for bitcoin in transaction fee only model. In: Proceedings of the 19th International Conference on Autonomous Agents and MultiAgent Systems. p. 2008–2010. AAMAS '20, International Foundation for Autonomous Agents and Multiagent Systems, Richland, SC (2020)
24. Sompolinsky, Y., Lewenberg, Y., Zohar, A.: Spectre: A fast and scalable cryptocurrency protocol. IACR Cryptology ePrint Archive **2016**, 1159 (2016)

A Proof of Theorem 1

Theorem 1 (Bitcoin in Block Rewards). *In a setting in which the miners derive their reward from Block Rewards, Bitcoin is a faithful implementation if $r \geq \alpha$ where r is the fixed block reward and α is the coefficient of mining cost ($C_{mining} = \alpha\delta$).*

Proof. Consider the blockchain at time $T = 0$, we only have the genesis block so there is no other choice than mining on top of the genesis block.
Consider the blockchain at time $T = T_0$, we divide the execution of blockchain into time slots separated by events in which new blocks are mined. The probability of a miner being able to mine a block in a time slot would be δ
If a miner chooses to start mine a block at depth k while the rest of the users are mining at depth 0 (at the top of the longest chain). The ensuing mining race between the miner and the rest of the network can be modelled by a random walk in which the miner starts k steps towards the left of the origin. The miner gains a positive reward only if he/she manages to reach on the right side of the origin.
Let $P(x = i, t)$ denote the probability of the miner's chain exceed the network's chain by i blocks at time t. The expected utility after t time slots will be

$$\mathbb{E}[u(\text{miner mining at depth } k, \pi_{-i}) \text{ after time } t] = \left[\sum_{i=k}^{\infty} P(x = i, t)(k + i)\right] r - tC_{\text{mining}}$$

$$\mathbb{E}[u(\text{miner mining at depth } k, \pi_{-i}) \text{ after time } t] = \left[\sum_{i=k}^{t} \left(\frac{t!}{[(t+i)/2]![(t-i)/2]!}\delta^{(\frac{t+i}{2})}(1-\delta)^{(\frac{t+i}{2})}\right)(k+i)\right] r - tC_{\text{mining}}$$

For $\delta < 0.5$, the maximum expected reward is achieved when $k = 0$ and $t = 0$.

$$\begin{aligned}\max_k \mathbb{E}[u(\text{mining at depth } k) \text{ at time } t] &= \mathbb{E}[u(\pi_i, \pi_{-i}) \text{ after time } t] \\ &= t\delta r - C_{\text{mining}}\end{aligned}$$

Also,

$$\begin{aligned}\mathbb{E}[u(\pi_i, \pi_{-i}) \text{ after time } t] &= t\delta r - tC_{\text{mining}} \\ &= t\delta r - t\alpha\delta \\ &= t\delta(r - \alpha) \\ &\geq 0 \qquad (\because r \geq \alpha)\end{aligned} \tag{1}$$

Thus, mining on top of the longest chain ($\because k = 0$) and releasing the blocks as soon as they are mined ($\because t = 1$) is the equilibrium strategy.
Therefore, Π_{Bitcoin} is a faithful implementation with block rewards.

B Proof of Theorem 2

Theorem 2 (Bitcoin in Transaction Fees). *In a setting in which the miners derive majority of their reward from transaction fees, Bitcoin cannot be a faithful implementation.*

Proof. We show this via proof-by-contradiction in the worst case when the transaction volume drops and there is negligible transaction fees to be collected for a new block.
Reward obtained by mining the block on top of the longest chain $R(b_{\max}) = r_0$ assumed to be $< C_{\text{mining}}$ since there is almost no transaction fees available.
Since the mining would have a non-zero mining cost C_{mining} associated with it, the miner would either shut down the mining operation all together or mine at another position at depth $k > 0$.
Let us consider if a miner that mines at a depth k, i.e., it mines on top of a chain k blocks shorter than the longest chain. Let us define $\text{Shallow}(k) = \{b | b \text{ is at a depth less than } k\}$ then for the miner mining the block at depth k, $r_k = \sum_{b \in \text{Shallow}(k)} R(b)$ reward is available. Consider the blockchain at time $T = T_0$,
Similar to the proof of Theorem 1, if a miner chooses to start mine a block at depth k while the rest of the users are mining at depth 0 (at the top of the longest chain). The ensuing mining race between the miner and the rest of the network can be modelled by a random walk in which the miner starts k steps towards the left of the origin. The miner gains a positive reward only if he/she manages to reach on the right side of the origin.
Let $P(x = i, t)$ denote the probability of the miner's chain exceed the network's chain by i blocks at time t. The expected utility after t time slots will be

$$\mathbb{E}[u(\text{miner mining at depth } k, \pi_{-i}) \text{ after time } t] = \left[\sum_{i=k}^{\infty} P(x = i, t)\right] r_k - tC_{\text{mining}}$$

$$\mathbb{E}[u(\text{miner mining at depth } k, \pi_{-i}) \text{ after time } t] = \left[\sum_{i=k}^{t} \left(\frac{t!}{[(t+i)/2]![(t-i)/2]!} \delta^{(\frac{t+i}{2})} (1-\delta)^{(\frac{t+i}{2})}\right)\right] r_k - tC_{\text{mining}}$$

Notice that the expected utility obtained by mining on top of the longest chain would be negative if $r_0 < \frac{tC_{\text{mining}}}{\delta}$. Hence, the miners would shut down their mining operation, effectively quitting the game, which would yield 0 reward ($u(\text{quitting}) = 0$). However, they also have an alternative strategy to fork the chain k blocks deep. This strategy would yield positive expected utility if $\exists\ k$ such that $r_k > \frac{tC_{\text{mining}}}{\left[\sum_{i=k}^{\infty} \left(\frac{t!}{[(t+i)/2]![(t-i)/2]!} \delta^{(\frac{t+i}{2})} (1-\delta)^{(\frac{t+i}{2})}\right)\right]}$ for some time $t > 0$
However, both the strategies could dominate the strategy for mining on top of the longest chain.
Thus, Π_{Bitcoin} is not a faithful implementation with only transaction fees.

C Proof of Theorem 3

Theorem 3 (Block Rewards Faithfulness). *Any blockchain protocol where the miner derives majority of revenue only from block rewards is a faithful implementation if $r \geq \alpha$ where r is the fixed block reward and α is the coefficient of mining cost ($C_{mining} = \alpha\delta$).*

Proof. Consider a scheme with a fixed block reward $R(b) = r \quad \forall\ b$.

$$\mathbb{E}[u(\sigma_i, \pi_{-i}) \text{ after time } t] = P(\text{b is accepted after time } t)r - tC_{\text{mining}} \tag{2}$$
$$\mathbb{E}[u(\pi_i, \pi_{-i}) \text{ after time } t] = t[P(b_{\max} \text{ is accepted after slot in which it is mined})r - C_{\text{mining}}] \tag{3}$$

Since $P(\text{b is accepted after time } t)$ requires a block to be mined in an epoch,
$P(\text{b is accepted after time } t) \leq \delta t$.

$$\begin{aligned} \mathbb{E}[u(\pi_i, \pi_{-i}) \text{ after time } t] &= t[P(b_{\max} \text{ is accepted after first epoch})r - C_{\text{mining}}] \\ &= t\delta r - tC_{\text{mining}} \\ &\geq P(\text{b is accepted after time } t)r - tC_{\text{mining}} \\ &\geq \mathbb{E}[u(\sigma_i, \pi_{-i}) \text{ after time } t] \qquad \forall \sigma_i \end{aligned} \tag{4}$$
$$\because \quad \mathbb{E}[u(\pi_i, \pi_{-i}) \text{ after time } t] \geq \mathbb{E}[u(\sigma_i, \pi_{-i}) \text{ after time } t] \qquad \forall \sigma_i$$

Also,

$$\begin{aligned} \mathbb{E}[u(\pi_i, \pi_{-i}) \text{ after time } t] &= t\delta r - tC_{\text{mining}} \\ &= t\delta r - t\alpha\delta \\ &= t\delta(r - \alpha) \\ &\geq 0 \qquad (\because r \geq \alpha) \end{aligned} \tag{5}$$

The blockchain protocol is a faithful implementation.

D Proof of Theorem 4

Theorem 4 (Transaction Fees Impossibility). *Any blockchain protocol where the miner derives majority of revenue only from transaction fees can not be a faithful implementation.*

Proof. We define $\text{Ancestors}(b) = \{x \mid x \prec b \ \forall\ x \in B\}$ as the set of all blocks that precede b.
Let us assume there exists a reward function $R()$ such that $R(b) = \sum_{x \in \text{Ancestors}(b)} f(b, x)$ where $f : B \times B \to \mathbb{R}$ is a function that takes in transaction fees in block x and returns the corresponding contribution to the reward for the block b.
Since no new currency can be minted via block rewards, the miner's reward cannot exceed the total transaction fees collected in the blockchain till now less the reward already distributed to the miners, i.e., $\sum_{b \in B} f(b, x) \leq \text{TxFees}(x)\ \forall\ x$. Total reward available to the miner mining the maximal block $b_{\max}$ would be $(\sum_{b \in B} TxFees(b)) + TxFees(b_{\max}) - |B|C_{\text{mining}}$. If similar to the Bitcoin's worst case, there were negligible transaction fees available due to a dearth of available transactions. Hence, $TxFees(b_{\max}) = 0$.
Let us assume that the blockchain protocol is a faithful implementation,

$$\implies \mathbb{E}[u(\pi_i, \pi_{-i}) \text{ after time } 0] \geq 0 \tag{6}$$
$$\implies \delta R(b_{\max}) - C_{\text{mining}} \geq 0 \tag{7}$$
$$\implies \delta R(b_{\max}) \geq C_{\text{mining}} \tag{8}$$

Thus, total available reward for the next miner would be
$R(b'_{\max}) \geq \sum_{b \in B} TxFees(b) - (|B|+1)C_{\text{mining}}$. If mining is continued without new transaction fees,

soon there will not be any available reward to be offered to the miners. At this point, $R(b_{\max})$ must be < 0.
At this time, $\mathbb{E}[u(\pi_i, \pi_{-i})] < 0$.
Thus, we reach a contradiction to Remark 1, the blockchain protocol Π is not a faithful implementation.