Stevens Institute Of Technology

The Front-running Game Between Miners and Traders in Blockchain

Seminar in Information Economics Research Paper
Author: Ruming L*
Advisor: Anand Goel

December 10, 2022

1 Abstract

Blockchain is a decentralized ledger which can let traders trade cryptocurrency through the network without a centralized intermediary. There are decentralized record-keepers called 'miners' in blockchain. They are randomly chosed by the blockchain protocol, they will help to verify the transactions happened in the blockchain and record those transactions to the new block for miners' reward.

For the miners, there exists conflicts of interest. A miner can not only record others' transactions, but also his own transactions, he can even arrange the order of those transactions and becomme a front-runner. So miners are natural insider traders in the blockchain, they may steal others trading profit for own interests. The traders also have their way to 'defend' their profit, because they are validator of the new block, they have options to disapprove the new block, or the traders can do some compromise and send some profit as the tips for the miners' ethical behavior.

In this paper we will consider a simplified situation where there are only one miner and one trader and form a game between these two players. Our conclusion is: In some situations especially the unethical miners are greedy, the equilibrium shows Delegdated Proof-of-Stake blockchain may fail. In some situations especially the block reward is enough high, all miners will keep being honest within equilibriums. And in some situations, blockchain works under the collaboration.

*rliu38@stevens.edu

2 Backgroud

2.1 Blockchain

A blockchain is a virtual chain of ordered blocks. Each block contains transactions and a reference to the previous block. All transactions can be easily verified by public due to zero knowledge proof mechanism. The blockchain updates once a new block is appended, new transactions are confirmed by consensus only by being included in a block that enters the blockchain.

Different blockchains use different protocols to generate a new block. Both almost all blockchains need the participation of miners. Miners are regarded as the record keepers in blockchains.

2.2 Proof-of-Work Protocol

In Bitcoin (BTC)[1] blockchain Proof-of-Work (PoS) protocol, miners are randomly chosen by solving a cryptography puzzle. Then the chosen miner can record some transactions in the new block and append to the chain. The probability of receiving the opportunity depends on the computation resource the miner have, which consumes a lot electricity power. Bitcoin, the most prominent PoW blockchain, consumes electricity at a level comparable with countries such as Austria and Ireland. [2]

2.3 Proof-of-Stake Protocol

Ethereum (ETH) used to use similar PoW protocol like Bitcoin, but for the sustainability. In 2022, From ETH 2.0, the ETH blockchain started to apply a protocol 'Casper' which is based on Proof-of-Stake (PoS) protocol[3]. PoS attempts to solve the energy consumption caused by PoW. The simpliest form of PoW is known as the Follow-the-Satoshi (FTS) algortithm[4], involves each blockchain branch selecting uniformly and randomly from the universe of native coins, e.g. BTC in bitcoin blockchain. The owner of the selected coin receives the opportunity to append to the branch that selected her coin and simultaneously collect a block reward. This protocol succeeds in reducing energy expenditure because miners no longer need to upgrade their computation resource for meaningless puzzles racing. The loyal holder of the naive coins are more likely become the miner for a new block.

Besides the FTS PoW, Delegated Proof-of-Stake (DPoS)[5] is a consensus mechanism that is a variation of the classic PoS system. DPoS evolved from PoS and allows users of the network to vote in delegates who then validate blocks. In DPoS, users vote in delegates, also known as validators, to verify and produce blocks. After they successfully produce a block,

[1] Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system.

[2] de Vries, A. 2018. Bitcoin's growing energy problem. Joule 2:801–5.

[3] Zamfir,V. 2017. Casper the Friendly Ghost: A correct-by-construction blockchain consensus protocol. Report, Ethereum Foundation, Zug, Switzerland. https://github.com/ethereum/research/blob/master/papers/ CasperTFG/CasperTFG.pdf.

[4] Xiao et al. (2020) survey distributed consensus protocols and discuss the FTS algorithm within the PoS section.

[5] Delegated Proof-of Stake Explained

these validators may then distribute their block rewards to those who voted for them. The DPoS will be our focused protocol for modelling.

2.4 Literature Review

A large literature now is studying blockchain economics, our seminar is about the information economics, I list some related research about the blockchain.

Recall that blockchain is a decentralized ledger, so it is crucial to make sure the ledger is unique in the whole system, there will exist 'double spending' problem if there are two different ledgers in blockchain in long run. It is called 'fork', the fork happened in ETH in 2016, which caused a permanent disagreement so that the ETH protocol fork to two protocols, ETH and ETC. Biais et al. (2019) demonstrate existence of both an equilibrium in which PoW induces consensus and an equilibrium in which PoW generates persistent disagreement.[6] Fahad (2021) provides formal economic model to solve the fork problem under PoS protocol, a sufficiently modest reward schedule not only implies the existence of an equilibrium in which consensus obtains as soon as possible but also precludes a persistent forking equilibrium.[7] Cong, He, and Li (2020) discuss staking pools problem for miners.[8] Emiliano (2021) claims the equilibrium between blockchain users and miners and impossible triangle for blockchain security.[9]

3 Model

3.1 Delegated Proof-of-Stake

As we mentioned before, our model will focus on the DPoS protocol, and this protocol has not been talked too much in other researchers' paper. Generally speaking, the DPoS is a game between miners and blockchain users. The miners propose some candidate blocks, and the users (also the validators) will vote a candidate block they like. If the candidate block is voted by the majority, it will become a new block and be appended to the blockchain. Every voters of this candidate can share the rewards of this new block.

We should also note that the users may have extra benefit from the new block except the sharing rewards. For instance, a trader who is doing a profitable trade in blockchain will very likely to vote for the candidate block which includes her profitable trade inside.

3.2 Front-runner

A very tricky rule in the blockchain protocol is that miners are not prohibited from trading in the blockchain. A miner can not only play as a record keeper but also an insider trader. There is a possible situation that, a miner's algorithm find the trader's profitable trade in blockchain, then the miner copy the trader's strategy to steal part of the trader's profit, or

[6] Biais, B., C. Bisière, M. Bouvard, and C. Casamatta. 2019. The blockchain folk theorem. Review of Financial Studies 32:1662–715.

[7] Fahad, S 2021. Blockchain without Waste: Proof-of-Stake.

[8] Cong, L. W., Z. He, and J. Li. 2020. Decentralized mining in centralized pools.

[9] Emiliano, P 2021. Decentralizing Money: Bitcoin Prices and Blockchain Security.

even make trader loss. These front-runners are threats to users' voting decision.[10] Some protocols like ETH calls this stolen profit 'Miner extractable value'. (MEV)[11]

In our model setting, we will consider front-running as an unethical behavior of miners, An ethical miner should not add her trade which comes from the information she got from others' trade in the same block. If she break this ethic, she becomes a front-runner and will be regarded as a unethical miner.

3.3 Signalling Game Model

In line with the previous description of DPoS and front-running. We consider a simplified model in which there are only two players, one miner and one trader. We ignore the reward sharing to trader (also the validator). But we do consider the transfer from miner to trader ('Bribes'). We also consider the transfer from trader to miner ('Tips'). Below is our definition for this signalling game, Fig 1 is our model tree and Fig 2 is our payoff matrix:

1. There are two types of miners. An ethical miner will never be a front-runnner, an unethical miner will always be a front-runner.

2. Nature decides the type of miner, she could be unethical $\boxed{\text{U}}$ miner with probability $\boxed{q}$ or ethical $\boxed{\text{E}}$ miner with probability $\boxed{1-q}$. And the miner knows her own type.

3. The miner can show a signal to the trader, the miner's action set is $\boxed{\{B, B'\}}$, where $\boxed{B \geq 0, B' < 0}$. The signal $B \geq 0$ means the miner guarantee "bribes" to the miner if the miner approve the candidate block. The signal $B' < 0$ means the miner will extract some "tips" from the trader, if trader's trade is included in the candidate block and trader accept the candidate block.

4. The trader can not see the type of miner, she only knows the signal from the miner, she knows her original profit of the trade $\boxed{P}$, which is a common knowledge to the miner, because the miner can see the trade and calculate the profit. The trader will decide to accept (A) or not accept (NA) the block, so the traders action set is $\boxed{\{A, NA\}}$.

5. The mining reward for the miner if the candidate block is accepted is $\boxed{T}$, this is also common knowledge.

6. The miner doesn't have some many cryptocurrencies like the trader. The miner will can only try to steal $\boxed{0.6P}$ profit from the trader and leave $\boxed{0.4P}$ to the trader.

7. If the trader not accept the candidate block, she has to wait until next block, an the profit will shrink to $\boxed{0.8P}$.

■ Explanation for the payoff 1: The miner is a front runner and she guarantee some 'bribes' $B \leq 0$ to the trader, the trader also accept the candidate block. The miner will get the block reward T plus part of the profit $0.6P$ minus the 'bribes' to the trader.

[10] Depth learning about front-running is discussed by Dan B, Bart T, 2008. Front-running dynamics.
[11] Ethereum Miner Extracted Value (MEV)

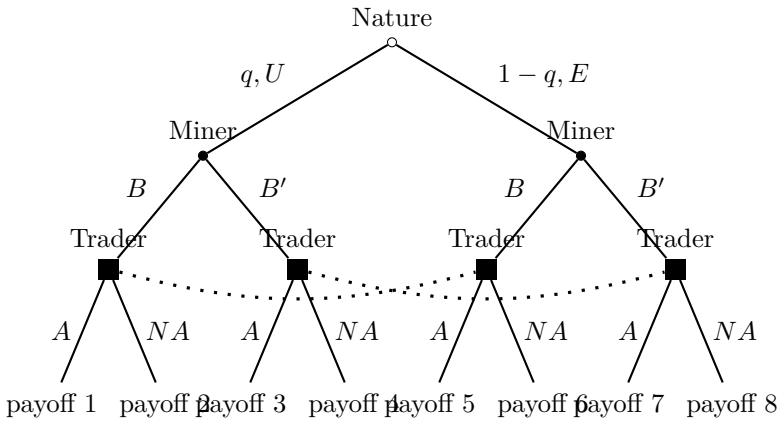
The miner's total payoff is $T + 0.6P - B$. Similarly, the trader only receive the rest profit $0.4P$ plus the 'bribes' B, which is $0.4P + B$.

- Explanation for the payoff 2: The miner is a front runner and she guarantee some 'bribes' $B \leq 0$ to the trader, however, the trader doesn't accept the candidate block. The miner get nothing (0) in this block, the trader will wait until next block but the profit will shrink to $0.8P$.

- Explanation for the payoff 3: The miner is a front runner and she asks for some 'tips' $B < 0$ from the trader, the trader accept the candidate block. The miner will get the block reward T plus part of the profit $0.6P$ plus the 'tips' $-B'$ from the trader. The miner's total payoff is $T + 0.6P - B'$. Similarly, the trader only receive the rest profit $0.4P$ minus 'tips' B', which is $0.4P + B'$.

- Explanation for the payoff 7: The miner is honest and she asks for some 'tips' $B < 0$ from the trader, the trader accept the candidate block. The miner will get the block reward T plus the 'tips' $-B'$ from the trader. The miner's total payoff is $T - B'$. Similarly, the trader get all profit P minus 'tips' B', which is $P + B'$.

Figure 1: An incomplete information game between Miner and Trader



Note: The dotted lines are the information sets for the trader

Now that we have completed the extensive-form representation of this game. we can turn to its normal form. In the normal form , the miner will know her type, miner must have 4 pure strategies. We define a strategy for miner as $a_1 = a_1^U a_1^E$, where $a_1^{\theta_1} \in \{B, B'\}$ is what a type θ_1 of miner chooses. So the pure strategy set of miner is

$$a_1 \in A_1 = \{BB, BB', B'B, B'B'\}.$$

For instance, $a_1 = BB'$ means the miner will choose B if she knows her type is U and choose B' if her type is E. The trader can't figure out the type of the miner, she can only observe the move of the miner, she has two information sets, so she also has 4 pure strategies

$$a_2 \in A_2 = \{AA, ANA, NAA, NANA\}.$$

Figure 2: Payoff matrix

	Miner	Trader
payoff 1	$T + 0.6P - B$	$0.4P + B$
payoff 2	0	$0.8P$
payoff 3	$T + 0.6P - B'$	$0.4P + B'$
payoff 4	0	$0.8P$
payoff 5	$T - B$	$P + B$
payoff 6	0	$0.8P$
payoff 7	$T - B'$	$P + B'$
payoff 8	0	$0.8P$

For instance, $a_2 = ANA$ means the trader will choose A if she observed miner moves B, and will choose NA if she observed miner moves B'.

To convert the extensive-form game to a normal-form matrix game, we are now computing the expected payoffs for each pair of pure strategies. Miner and traders both have 4 pure strategies, there will be a 4×4 matrix to represent the game. For instance, consider the pair of strategies $(a_1, a_2) = (BB', ANA)$. The payoffs of the game will be determined by below:

- Nature chooses $\theta_1 = U$ with probability q, in which case miner plays B and trader plays A, the payoffs are $(T + 0.6P - B, 0.4P + B)$.
- Nature chooses $\theta_1 = E$ with probability $1 - q$, in which case miner plays B' and trader plays NA, the payoffs are $(0, 0.8P)$.

Based on above possible outcomes we can compute the expected payoffs for miner and trader with $(a_1, a_2) = (BB', ANA)$:

$$E[V_{miner}] = q \times (T + 0.6P - B) + (1 - q) \times 0 = qT + 0.6qP - qB$$
$$E[V_{trader}] = q \times (0.4P + B) + (1 - q) \times 0.8P = 0.8P - 0.4qP + qB$$

Similarly, we can compute the expected payoffs for miner and trader with $(a_1, a_2) = (BB', AA)$:

$$E[V_{miner}] = q \times (T + 0.6P - B) + (1 - q) \times (T - B') = T - B' + 0.6qP + qB' - qB$$
$$E[V_{trader}] = q \times (0.4P + B) + (1 - q) \times (P + B') = P + B' - 0.6qP - qB' + qB$$

The total normal form matrix is shown in Fig 3.

3.4 Scenario 1: High block reward can prevent the front-running

Consider below situation: the probability of unethical miner is $q = 1/4$, the trading profit is $P = 100$, trader doesn't consider to give miner tips, $B' = 0$. The mining block reward is $\boxed{\text{much larger}}$ than the trading profit $T = 10P$, the bribes from miner is $B = 0.6P$. The matrix representation is Fig 4.

Figure 3: Normal form matrix

Miner, Trader	A A	A NA	NA A	NA NA
B B	$(T-B+0.6qP, P+B-0.6qP)$	$(T-B+0.6qP, P+B-0.6qP)$	$(0, 0.8P)$	$(0, 0.8P)$
B B'	$(T-B'+0.6qP+qB'-qB, P+B'-0.6qP-qB'+qB)$	$(qT+0.6qP-qB, 0.8P-0.4qP+qB)$	$(T-B'-qT+qB', P+B'-0.2qP-qB')$	$(0, 0.8P)$
B' B	$(T-B+0.6qP+qB-qB', P+B-0.6qP-qB+qB')$	$(T-B-qT+qB, P+B-0.2qP-qB)$	$(qT+0.6qP-qB', qB'+0.8P-0.4qP)$	$(0, 0.8P)$
B' B'	$(T-B'+0.6qP, P+B'-0.6qP)$	$(0, 0.8P)$	$(T-B'+0.6qP, P+B'-0.6qP')$	$(0, 0.8P)$

Figure 4: Normal form matrix of Scenario 1

Miner, Trader	A A	A NA	NA A	NA NA
B B	$(955, \underline{145})$	$(\underline{955}, \underline{145})$	$(0, 80)$	$(\underline{0}, 80)$
B B'	$(1000, \underline{100})$	$(250, 85)$	$750, 95)$	$(\underline{0}, 80)$
B' B	$(970, 130)$	$(705, \underline{140})$	$(265, 70)$	$(\underline{0}, 80)$
B' B'	$(\underline{1015}, \underline{85})$	$(0, 80)$	$(\underline{1015}, \underline{85})$	$(\underline{0}, 80)$

If we follow the method of underlining miner's best responses for each column, also underlining trader's best responses for each row, we immediately find three pure-strategy Bayesian Nash equilibrium (BNE): $\boxed{(BB, ANA), (B'B', AA) \text{ and } (B'B', NAA)}$. Next steps we will see whether these can be perfect Bayesian equilibrium (PBE).

Let's consider the BNE (BB, ANA). The model tree is in Fig 5, the information set I_B is reached with positive probability, so that a unique belief is derived from Bayesian formula: $\mu_B = 1/4$, under this belief, we calculate the average payoff of A and NA,

$$E[A|\mu_B = 1/4] = \mu_B \times 100 + (1 - \mu_B) \times 160 = 1/4 \times 100 + 3/4 \times 160 = 145$$
$$E[NA|\mu_B = 1/4] = \mu_B \times 80 + (1 - \mu_B) \times 80 = 1/4 \times 80 + 3/4 \times 80 = 80.$$

$E[A|\mu_B = 1/4] > E[NA|\mu_B = 1/4]$, so we have proved A is the best response in information set I_B. Because information set $I_{B'}$ is reached with zero probability, we can assign a belief $\mu_{B'} = 1/10$, in that case, the average payoff of A and NA,

$$E[A|\mu_{B'} = 1/10] = \mu_B \times 40 + (1 - \mu_B) \times 100 = 1/10 \times 40 + 9/10 \times 100 = 94$$
$$E[NA|\mu_{B'} = 1/10] = \mu_B \times 80 + (1 - \mu_B) \times 80 = 1/10 \times 80 + 9/10 \times 80 = 80.$$

$E[A|\mu_{B'} = 1/10] > E[NA|\mu_{B'} = 1/10]$, so we have proved A is the also the best response in information set I_B given belief $\mu_{B'} = 1/10$. Therefore, the $\boxed{\text{BNE } (BB, ANA) \text{ under the belief } \mu_B = 1/4, \mu_{B'} = 1/10 \text{ is also a PBE}}$.

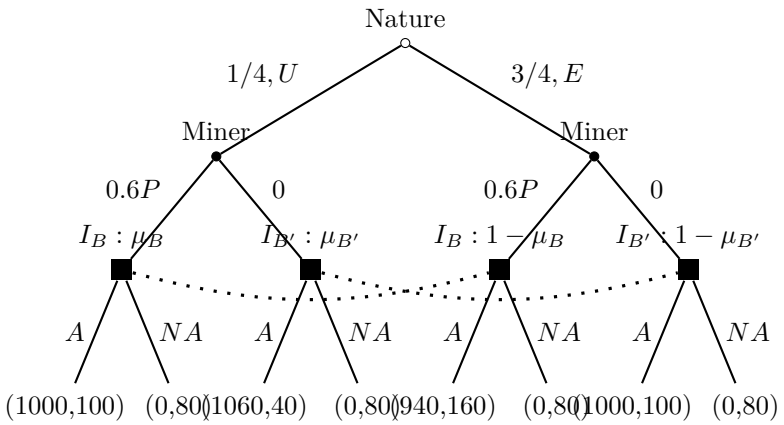
Under the same technique, we can also prove $\boxed{(B'B', AA) \text{ is a PBE}}$. Finally, let's consider the BNE $(B'B', NAA)$, note that in off equilibrium information set I_B, A is a strictly dominant strategy, it's unreasonable to choose NA under any belief. $\boxed{(B'B', NAA) \text{ is not a PBE}}$.

Notice that both PBEs (BB, ANA) and $(B'B', AA)$ are pooling equilibriums, the trader can not infer the miner's type from the signal. Now the question is how to explain these two equilibriums?

- Equilibrium $(B'B', AA)$ means both unethical and ethical miners choose not to ask for 'tips' from trader. If the miner is unethical, the miner will steal some profit, the trader (or the validator) should not approve the candidate block. But because the probability of unethical miner is low $q = 0.25$, and the signal is pooling, $\boxed{\text{trader believes she is more likely faced to an ethical miner}}$, that's why she choose to accept the candidate block.
- Equilibrium (BB, ANA) means both unethical and ethical miners choose not to give trader bribes $0.6P$. Remember that in our scenario, the block reward is quite high $T = 10P$. There is an incentive for miner to persuade the trader agree with the candidate block. So the miner gives the validator some bribes $0.6P$ for earning the block reward. One interesting thing is that, for the unethical miner, she stole $0.6P$ profit by being a front-runner, now she gives bribes $0.6P$ to the miner, which means she compensate the loss of the trader. In other words, $\boxed{\text{an unethical miner will not become a front-runner if the block reward is high}}$.[12]

[12] We may find the margin condition for this assert in future study.

Figure 5: An incomplete information game of scenario 1



Note: The dotted lines are the information sets for the trader

Figure 6: Normal form matrix of Scenario 2

Miner, Trader	A A	A NA	NA A	NA NA
B B	$(14, \underline{96})$	$(14, \underline{96})$	$(0, 80)$	$(\underline{0}, 80)$
B B'	$(21, \underline{89})$	$(\underline{18}, \underline{89})$	$(3, 80)$	$(\underline{0}, 80)$
B' B	$(77, 33)$	$(-4, \underline{87})$	$(81, 26)$	$(\underline{0}, 80)$
B' B'	$(\underline{84}, 26)$	$(0, \underline{80})$	$(\underline{84}, 26)$	$(\underline{0}, \underline{80})$

3.5 Scenario 2: Trader collaborate if unethical miner is majority

Consider below situation: the probability of unethical miner is $q = 9/10$, the trading profit is $P = 100$, trader consider to give miner tips, $B' = -0.2P$. The mining block reward is much smaller than the trading profit $T = 0.1P$, the bribes from miner is $B = 0.5P$. The matrix representation is Fig 6.

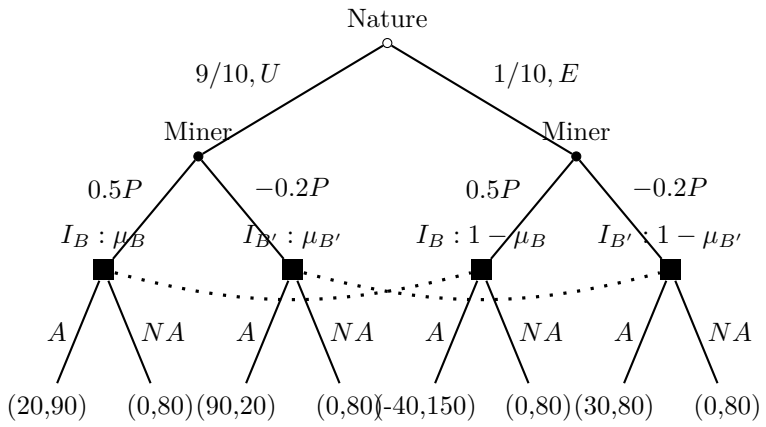
And the model tree is in Fig 7.

If we follow the method of underlining miner's best responses for each column, also underlining trader's best responses for each row, we immediately find two pure-strategy Bayesian Nash equilibrium (BNE): (BB', ANA), and $(B'B', NANA)$. Next steps we will see whether these can be perfect Bayesian equilibrium (PBE). Before that, we recall a proposition of perfect Bayesian equilibrium.

Remark. *If a strategy $\sigma^* = (\sigma_1^*, ..., \sigma_n^*)$ is a Bayesian Nash equilibrium of a Bayesian game τ, and if σ^* induces all the information sets to be reached with positive probability, then σ^*, together with the belief system μ^* uniquely derived from σ^* and the distribution of types, constitutes a perfect Bayesian equilibrium for τ.*

From this proposition it follows that (BB', ANA) can be part of a perfect Bayesian equilibrium because both of the information sets I_B and $I_{B'}$ are reached with positive probability.

Figure 7: An incomplete information game of scenario 2



Note: The dotted lines are the information sets for the trader

In particular the derived beliefs based on Bayesian formula from (BB', ANA) are $\mu_B = 1$ and $\mu_{B'} = 0$. It follows from the Bayesian game matrix that trader is playing a best response to these beliefs in each of his information sets, and that miner is playing a best response in each of his. So $\boxed{(BB', ANA) \text{ together with } \mu_B = 1 \text{ and } \mu_{B'} = 0 \text{ constitute a PBE}}$.

Now let's check the BNE $(B'B', NANA)$, we focus on the off-path information set I_B. To prove $(B'B', NANA)$ is a PBE, we need to find a belief μ_B such that, NA is the best response under this belief. But notice that under information set I_B, $\{A\}$ is a strictly dominant strategy to the trader, in other words,

$$\begin{aligned} E[A|\mu_B] &= \mu_B \times 90 + (1 - \mu_B) \times 150 \\ E[NA|\mu_B] &= \mu_B \times 80 + (1 - \mu_B) \times 80 \\ E[A|\mu_B] &> E[NA|\mu_B], \forall \mu_B \in [0, 1], \end{aligned}$$

BNE $\boxed{(B'B', NANA) \text{ fails to be a PBE under any belief}}$.

- Equilibrium (BB', ANA) is a $\boxed{\text{seperating equilibrium}}$ which means the trader can infer the type of the miner based on the signal. If the miner choose $\{B\}$, the trader will realize the miner is unethical front-runner. If the miner choose B', the trader will know the miner is ethical.

- In this scenario, the block reward is very low $T = 0.1P$, the $\boxed{\text{minority ethical miners}}$ $\boxed{\text{ask for some extra 'tips'}}$ from the trader, $B' = -0.2P$. The unethical miner knows that 'unethical miners are majority' is a common knowledge to the trader, if he just be a front-runner and do nothing else, the trader will very likely not approve the candidate block. So the $\boxed{\text{unethical miner shows a signal (bribes)}}$ to the trader $B = 0.5P$.

- Question 1: Why the trader don't approve the candidate block if she knows the miner is ethical when observing the signal $\{B'\}$?
  If the miner approve the block, she earn the profit P and subtract the 'tips' to the

Figure 8: Normal form matrix of Scenario 3

Miner, Trader	A A	A NA	NA A	NA NA
B B	$(64, 46)$	$(\underline{64}, 46)$	$(0, \underline{80})$	$(\underline{0}, 80)$
B B'	$(64, 44)$	$(63, 44)$	$(3, \underline{80})$	$(\underline{0}, \underline{80})$
B' B	$(82, 28)$	$(1, \underline{82})$	$(81, 26)$	$(\underline{0}, 80)$
B' B'	$(\underline{84}, 26)$	$(0, \underline{80})$	$(\underline{84}, 26)$	$(\underline{0}, \underline{80})$

miner $B' = -0.2P$, the trader's final payoff is $0.8P$, which is the same with the payoff if she not approve this candidate block and wait until next block. However, the trade is afraid of some unethical miner showing this signal to pretend they are ethical. In that situation, if the trader approve the block, her profit will be $0.4P$ subtract the tips $B' = -0.2P$, the final payoff is $0.2P$ which is much worse than waiting until next block. That's why the trader plays $\{NA\}$ when she observes signal $\{B'\}$, she behaves tough to prevent unethical miner pretending as an ethical miner.

- Question 2: Why there exists collaboration between trader and unethical miner?
  The trader will infer miner's type from the signal B and there will be front-running trade, the trader seems likely to reject the block. To invade nothing from this block, the unethical miner put forward a plan: the miner will return part of the front-running profit back to the trader (bribes) B. After seeing this plan, the trader will get final payoff $0.9P$ which is better than waiting until next block $0.8P$, the trader will accept it even though she know there is front-running. In summary, when the unethical miners are majority, they are hard to hide their type, then the miner can only do a modest front-running, and leave some cake to the trader.

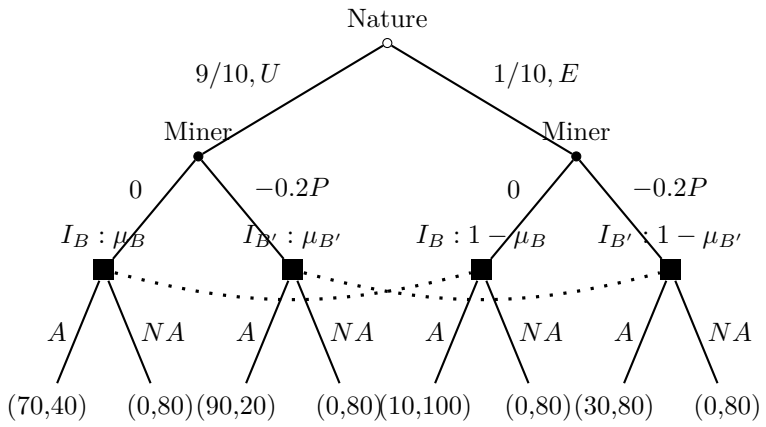
As we have shown above, under some conditions and the unethical miners are majority, there exists a equilibrium that miner will collaborate with unethical miner, and ethical miner's candidate block can never be approved. If that is the situation, in the long run, ethical miners will leave the mining pool because they have no chance to get the block reward. Finally, each block will be created under the collaboration between traders and miners, every transactions will be affected by front-running more or less.

3.6 Scenario 3: Blockchain may failure if miner is greedy

Consider below situation: the probability of unethical miner is $q = 9/10$, the trading profit is $P = 100$, trader consider to give miner tips, $B' = -0.2P$. The mining block reward is much smaller than the trading profit $T = 0.1P$, there is no bribe from miner, $B = 0$. The matrix representation is Fig 8. The model tree is in Fig 9.

If we follow the method of underlining miner's best responses for each column, also underlining trader's best responses for each row, we immediately find three pure-strategy BNE: $(BB, NANA)$, $(BB', NANA)$ and $(B'B', NANA)$. By using the techniques in Section

Figure 9: An incomplete information game of scenario 3



Note: The dotted lines are the information sets for the trader

3.4, we can see all these 3 equilibriums $\boxed{(BB, NANA)}$, $\boxed{(BB', NANA) \text{ and } (B'B', NANA)}$ are also perfect Bayesa=ian equilibriums.

- Equilibriums $(BB, NANA)$ and $(B'B', NANA)$ are both pooling equilibriums, the trader can not infer any information from the signal, and the probability of unethical miner is high q = 0.9, also notice that $B = 0$ means there is no bribe from miner to trader, the trader have no incentive to approve the candidate block. That's the reason leads these two PBE.

- Equilibrium $(BB', NANA)$ is a separating equilibrium. The unethical miner chooses no bribe with $B = 0$, the trader realizes that she is faced with an unethical miner and her profit will be taken away without any compensation (bribe), the trader's best response is $\{NA\}$. An ethical miner asks for some tips with $B' = -0.2P$, trader knows she is faced with an ethical miner and in $\boxed{\text{Section 3.5 Question 2}}$, we have explained why the trader doesn't approve the block even though she knows the miner is ethical.

According to the analysis above, under some conditions and especially the $\boxed{\text{unethical miner is greedy}}$, she never compensates the trader for her unethical front-running, all these 3 equilibriums will cause the $\boxed{\text{trader never approving the candidate block}}$, the blockchain system can not generate new block and become failure.

4 Further Research in this Game

In our model, we simplify the DPoS protocol to a two players' signalling game between miner and trader. We simulate some scenarios and explain the equilibriums. In the future research,

- We may find the marginal condition for this scenario, e.g. what scale of the block reward can prevent the unethical miners' front-running?

- We may consider the game contains more than one validator. In that case, the trader is not the only voter, she may need to consider other validtors actions.
- Miner's past behavior can be partially revealed in the blockchain, we may somehow find a way to build the miner's reputation in the game.

5 Conclusion

In this paper, we are focusing on a blockchain protocol DPoS, which has not been talked too much compared with other protocols like PoW and PoS. We form a signalling game between the miners and traders. We analyzes some situations especially the unethical miners are greedy, in which the DPoS blockchain may fail. In some situations especially the block reward is enough high, all miners will keep being honest. Or in some situations, blockchain works under the collaboration.

References

[1] Sence, M.1973. Job market signaling , Quarterly Journal of Economics 87, 355-374.

[2] Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system.

[3] Biais, B., C. Bisière, M. Bouvard, and C. Casamatta. 2019. The blockchain folk theorem. Review of Financial Studies 32:1662–715.

[4] Fahad, S 2021. Blockchain without Waste: Proof-of-Stake.

[5] Cong, L. W., Z. He, and J. Li. 2020. Decentralized mining in centralized pools.

[6] Emiliano, P 2021. Decentralizing Money: Bitcoin Prices and Blockchain Security.

[7] Lowe D G. Distinctive image features from scale-invariant keypoints, International journal of computer vision, 2004, 60(2): 91-110.

[8] de Vries, A. 2018. Bitcoin's growing energy problem. Joule 2:801–5.

[9] Zamfir,V. 2017. Casper the Friendly Ghost: A correct-by-construction blockchain consensus protocol. Report, Ethereum Foundation, Zug, Switzerland. https://github.com/ethereum/research/blob/master/papers/CasperTFG/CasperTFG.pdf.

[10] Xiao et al. (2020) survey distributed consensus protocols and discuss the FTS algorithm within the PoS. section.