Selfish Mining and Dyck Words in Bitcoin and Ethereum Networks

Cyril Grunspan (De Vinci Research Center, Paris-La Défense)
Ricardo Pérez-Marco (CNRS, IMJ-PRG, Univ. Paris 7)

Tokenomics Conference

Paris

May 6, 2019

Block withholding strategies

Bibliography

- *"On profitability of selfish mining"*, ArXiv:1805.08281, May 2018.

Bibliography

- *"On profitability of selfish mining"*, ArXiv:1805.08281, May 2018.
- *"On profitability of stubborn mining"*, ArXiv:1808.01041, August 2018.

Bibliography

- *"On profitability of selfish mining"*, ArXiv:1805.08281, May 2018.
- *"On profitability of stubborn mining"*, ArXiv:1808.01041, August 2018.
- *"On profitability of trailing mining"*, ArXiv:1811.09322, November 2018.

Bibliography

- *"On profitability of selfish mining"*, ArXiv:1805.08281, May 2018.
- *"On profitability of stubborn mining"*, ArXiv:1808.01041, August 2018.
- *"On profitability of trailing mining"*, ArXiv:1811.09322, November 2018.
- *"Bitcoin selfish mining and Dyck words"*, ArXiv:1902.01513, February 2019.

Bibliography

- *"On profitability of selfish mining"*, ArXiv:1805.08281, May 2018.
- *"On profitability of stubborn mining"*, ArXiv:1808.01041, August 2018.
- *"On profitability of trailing mining"*, ArXiv:1811.09322, November 2018.
- *"Bitcoin selfish mining and Dyck words"*, ArXiv:1902.01513, February 2019.
- *"Selfish Mining and Dyck Words in Bitcoin and Ethereum Networks"*, ArXiv:1904.07675, April 2019.

Bibliography

- *"On profitability of selfish mining"*, ArXiv:1805.08281, May 2018.
- *"On profitability of stubborn mining"*, ArXiv:1808.01041, August 2018.
- *"On profitability of trailing mining"*, ArXiv:1811.09322, November 2018.
- *"Bitcoin selfish mining and Dyck words"*, ArXiv:1902.01513, February 2019.
- *"Selfish Mining and Dyck Words in Bitcoin and Ethereum Networks"*, ArXiv:1904.07675, April 2019.
- *"Selfish Mining in Ethereum"*, ArXiv:1904.13330, May 2019.

Profit and Loss per unit of time

Profit and Loss per unit of time

- **Profit and Loss:**

$$P\&L = R - C$$

where R is the revenue and C is the cost.

Profit and Loss per unit of time

- **Profit and Loss:**

$$P\&L = R - C$$

where R is the revenue and C is the cost.

- **Time considerations:**

Profit and Loss per unit of time

- **Profit and Loss:**

$$P\&L = R - C$$

where R is the revenue and C is the cost.

- **Time considerations:**

What matters for a business is the $P\&L$ per unit of time: $P\&LT$.

Profit and Loss per unit of time

- **Profit and Loss:**

$$P\&L = R - C$$

where R is the revenue and C is the cost.

- **Time considerations:**

What matters for a business is the $P\&L$ per unit of time: $P\&LT$.

And the asymptotic $P\&L$ per unit of time

$$P\&LT_{\infty} = \lim_{T \to +\infty} \frac{R(T) - C(T)}{T}$$

Repetition games

Repetition games

- Warning! Not Game Theory! (terminology from gambling).

Repetition games

- Warning! Not Game Theory! (terminology from gambling).
- Repeat over and over (cycles) a profitable strategy.

Repetition games

- Warning! Not Game Theory! (terminology from gambling).
- Repeat over and over (cycles) a profitable strategy.

We consider three random variables:

Repetition games

- Warning! Not Game Theory! (terminology from gambling).
- Repeat over and over (cycles) a profitable strategy.

We consider three random variables:

- R revenue per cycle.

Repetition games

- Warning! Not Game Theory! (terminology from gambling).
- Repeat over and over (cycles) a profitable strategy.

We consider three random variables:

- R revenue per cycle.

Repetition games

- Warning! Not Game Theory! (terminology from gambling).
- Repeat over and over (cycles) a profitable strategy.

We consider three random variables:

- R revenue per cycle.
- C cost per cycle.

Repetition games

- Warning! Not Game Theory! (terminology from gambling).
- Repeat over and over (cycles) a profitable strategy.

We consider three random variables:

- R revenue per cycle.
- C cost per cycle.

Repetition games

- Warning! Not Game Theory! (terminology from gambling).
- Repeat over and over (cycles) a profitable strategy.

We consider three random variables:

- R revenue per cycle.
- C cost per cycle.
- T time per cycle.

Repetition games

- Warning! Not Game Theory! (terminology from gambling).
- Repeat over and over (cycles) a profitable strategy.

We consider three random variables:

- R revenue per cycle.
- C cost per cycle.
- T time per cycle.

Repetition games

- Warning! Not Game Theory! (terminology from gambling).
- Repeat over and over (cycles) a profitable strategy.

We consider three random variables:

- R revenue per cycle.
- C cost per cycle.
- T time per cycle.

Theorem (Profitability of a Repetition Game)

$$P\&LT_\infty = \frac{\mathbb{E}[R] - \mathbb{E}[C]}{\mathbb{E}[T]} .$$

Repetition games

- Warning! Not Game Theory! (terminology from gambling).
- Repeat over and over (cycles) a profitable strategy.

We consider three random variables:

- R revenue per cycle.
- C cost per cycle.
- T time per cycle.

Theorem (Profitability of a Repetition Game)

$$P\&LT_\infty = \frac{\mathbb{E}[R] - \mathbb{E}[C]}{\mathbb{E}[T]} .$$

Repetition games

- Warning! Not Game Theory! (terminology from gambling).
- Repeat over and over (cycles) a profitable strategy.

We consider three random variables:

- R revenue per cycle.
- C cost per cycle.
- T time per cycle.

Theorem (Profitability of a Repetition Game)

$$P\&LT_\infty = \frac{\mathbb{E}[R] - \mathbb{E}[C]}{\mathbb{E}[T]}.$$

Proof. Strong law of large numbers.

Comparing repetition games with equal costs

Comparing repetition games with equal costs

Definition (Revenue and Cost Ratio)

The Revenue Ratio, resp. Cost Ratio, of a Repetition Strategy ξ is

$$\Gamma(\xi) = \frac{\mathbb{E}[R]}{\mathbb{E}[T]} \quad \textit{resp.} \quad \Upsilon(\xi) = \frac{\mathbb{E}[C]}{\mathbb{E}[T]}$$

Comparing repetition games with equal costs

Definition (Revenue and Cost Ratio)

The Revenue Ratio, resp. Cost Ratio, of a Repetition Strategy ξ is

$$\Gamma(\xi) = \frac{\mathbb{E}[R]}{\mathbb{E}[T]} \quad \textit{resp.} \quad \Upsilon(\xi) = \frac{\mathbb{E}[C]}{\mathbb{E}[T]}$$

Comparing repetition games with equal costs

Definition (Revenue and Cost Ratio)

The Revenue Ratio, resp. Cost Ratio, of a Repetition Strategy ξ is

$$\Gamma(\xi) = \frac{\mathbb{E}[R]}{\mathbb{E}[T]} \quad \textit{resp.} \quad \Upsilon(\xi) = \frac{\mathbb{E}[C]}{\mathbb{E}[T]}$$

Theorem (Comparing profitabilities of equal cost strategies)

We consider two integrable strategies with $\Upsilon(\xi) = \Upsilon(\xi')$. Then ξ is more profitable than strategy ξ' in the long run if and only if

$$\Gamma(\xi') \leq \Gamma(\xi) \, .$$

Block withholding mining

- Protocol rules (BTC or ETH) mandate miners to release and propagate blocks as soon as they are mined.

Block withholding mining

- Protocol rules (BTC or ETH) mandate miners to release and propagate blocks as soon as they are mined.
- Block withholding strategy: Timely release blocks in order to invalidate honest blocks.

Block withholding mining

- Protocol rules (BTC or ETH) mandate miners to release and propagate blocks as soon as they are mined.
- Block withholding strategy: Timely release blocks in order to invalidate honest blocks.

There are many block withholding strategies Selfish Mining (SM), Lead Stubborn Mining (LSM), Equal Fork Stubborn Mining (EFSM), etc They differ by the algorithm by which we release blocks. This depends on the chain state (length of official blockchain, length of secret fork, etc)

Block withholding mining

- Protocol rules (BTC or ETH) mandate miners to release and propagate blocks as soon as they are mined.
- Block withholding strategy: Timely release blocks in order to invalidate honest blocks.

There are many block withholding strategies Selfish Mining (SM), Lead Stubborn Mining (LSM), Equal Fork Stubborn Mining (EFSM), etc They differ by the algorithm by which we release blocks. This depends on the chain state (length of official blockchain, length of secret fork, etc)

- Key observation:

Block withholding and honest strategies have exactly the same cost

Important observations

Important observations

- Part of the Revenue comes the block rewards determined by the protocol. The revenue in fiat currency depends on the market exchange rate of the coin, but the comparison of the profitability is independent of the exchange rate.

Important observations

- Part of the Revenue comes the block rewards determined by the protocol. The revenue in fiat currency depends on the market exchange rate of the coin, but the comparison of the profitability is independent of the exchange rate.

- The Cost depends on external factors like energy prize, hardware costs, etc These costs are independent of the strategy as long as the strategy is a full time intensive computation.

Profitability of block withholding strategies

Profitability of block withholding strategies

- A block withholding strategy ξ is profitable in the long run iff

$$\Gamma(HM) \leq \Gamma(\xi)$$

Profitability of block withholding strategies

- A block withholding strategy ξ is profitable in the long run iff

$$\Gamma(HM) \leq \Gamma(\xi)$$

Theorem (Stability Theorem, G-PM, 2018)

Without a difficulty adjustment, no block withholding strategy ξ can be profitable and we always have

$$\Gamma(\xi) \leq \Gamma(HM)$$

Profitability of block withholding strategies

- A block withholding strategy ξ is profitable in the long run iff

$$\Gamma(HM) \leq \Gamma(\xi)$$

Theorem (Stability Theorem, G-PM, 2018)

Without a difficulty adjustment, no block withholding strategy ξ can be profitable and we always have

$$\Gamma(\xi) \leq \Gamma(HM)$$

Profitability of block withholding strategies

- A block withholding strategy ξ is profitable in the long run iff

$$\Gamma(HM) \leq \Gamma(\xi)$$

Theorem (Stability Theorem, G-PM, 2018)

Without a difficulty adjustment, no block withholding strategy ξ can be profitable and we always have

$$\Gamma(\xi) \leq \Gamma(HM)$$

Proof. Martingale techniques, and Doob's Stopping Time Thm.

Profitability of block withholding strategies

- A block withholding strategy ξ is profitable in the long run iff

$$\Gamma(HM) \leq \Gamma(\xi)$$

Theorem (Stability Theorem, G-PM, 2018)

Without a difficulty adjustment, no block withholding strategy ξ can be profitable and we always have

$$\Gamma(\xi) \leq \Gamma(HM)$$

Proof. Martingale techniques, and Doob's Stopping Time Thm.

An attack on the difficulty adjustment

An attack on the difficulty adjustment

Corollary

A block withholding strategy is an attack on the Difficulty Adjustment Formula.

An attack on the difficulty adjustment

Corollary

A block withholding strategy is an attack on the Difficulty Adjustment Formula.

An attack on the difficulty adjustment

Corollary

A block withholding strategy is an attack on the Difficulty Adjustment Formula.

- Main problem in Bitcoin and Ethereum: The DA formula does not account properly orphaned blocks.

An attack on the difficulty adjustment

Corollary

A block withholding strategy is an attack on the Difficulty Adjustment Formula.

- Main problem in Bitcoin and Ethereum: The DA formula does not account properly orphaned blocks.

In ETH this is partially taken into account by signaling nephew blocks, but the DA is continuous which is worse to counter these rogue strategies.

An attack on the difficulty adjustment

Corollary

A block withholding strategy is an attack on the Difficulty Adjustment Formula.

- Main problem in Bitcoin and Ethereum: The DA formula does not account properly orphaned blocks.

In ETH this is partially taken into account by signaling nephew blocks, but the DA is continuous which is worse to counter these rogue strategies.

- Solution: Modification of the DA formula to take this into account.

An attack on the difficulty adjustment

Corollary

A block withholding strategy is an attack on the Difficulty Adjustment Formula.

- Main problem in Bitcoin and Ethereum: The DA formula does not account properly orphaned blocks.

In ETH this is partially taken into account by signaling nephew blocks, but the DA is continuous which is worse to counter these rogue strategies.

- Solution: Modification of the DA formula to take this into account.

An attack on the difficulty adjustment

Corollary

A block withholding strategy is an attack on the Difficulty Adjustment Formula.

- Main problem in Bitcoin and Ethereum: The DA formula does not account properly orphaned blocks.

In ETH this is partially taken into account by signaling nephew blocks, but the DA is continuous which is worse to counter these rogue strategies.

- Solution: Modification of the DA formula to take this into account.

The old Markov model

- Main parameters $0 < q < 1/2$ relative hashrate of the attacker, $0 \leq \gamma \leq 1$ connectivity of the attacker.

The old Markov model

- Main parameters $0 < q < 1/2$ relative hashrate of the attacker, $0 \leq \gamma \leq 1$ connectivity of the attacker.
- Chain state essentially defined by length of official blockchain and of secret fork.

The old Markov model

- Main parameters $0 < q < 1/2$ relative hashrate of the attacker, $0 \leq \gamma \leq 1$ connectivity of the attacker.
- Chain state essentially defined by length of official blockchain and of secret fork.
- One can compute the relative proportion of blocks mined by the block withholders, and this gives the long run profitability of the strategy, but only after the difficulty adjustment.

The old Markov model

- Main parameters $0 < q < 1/2$ relative hashrate of the attacker, $0 \leq \gamma \leq 1$ connectivity of the attacker.
- Chain state essentially defined by length of official blockchain and of secret fork.
- One can compute the relative proportion of blocks mined by the block withholders, and this gives the long run profitability of the strategy, but only after the difficulty adjustment.
- The Markov chain model cannot provide any information about the time it takes to jump from one state to another: Hence it is impossible to answer some basic questions.

The old Markov model

- Main parameters $0 < q < 1/2$ relative hashrate of the attacker, $0 \leq \gamma \leq 1$ connectivity of the attacker.
- Chain state essentially defined by length of official blockchain and of secret fork.
- One can compute the relative proportion of blocks mined by the block withholders, and this gives the long run profitability of the strategy, but only after the difficulty adjustment.
- The Markov chain model cannot provide any information about the time it takes to jump from one state to another: Hence it is impossible to answer some basic questions.
- Example of practical basic question: How long it takes to the selfish miner to enter profitability?

The old Markov model

- Main parameters $0 < q < 1/2$ relative hashrate of the attacker, $0 \leq \gamma \leq 1$ connectivity of the attacker.
- Chain state essentially defined by length of official blockchain and of secret fork.
- One can compute the relative proportion of blocks mined by the block withholders, and this gives the long run profitability of the strategy, but only after the difficulty adjustment.
- The Markov chain model cannot provide any information about the time it takes to jump from one state to another: Hence it is impossible to answer some basic questions.
- Example of practical basic question: How long it takes to the selfish miner to enter profitability?

Poisson races

Poisson races

- $N'(t)$, resp. $N(t)$, numbers of validated blocks at time t by the selfish, resp. honest, miners are Poisson processes with resp. parameters α' and α, $\alpha' < \alpha$.

Poisson races

- $N'(t)$, resp. $N(t)$, numbers of validated blocks at time t by the selfish, resp. honest, miners are Poisson processes with resp. parameters α' and α, $\alpha' < \alpha$.

$$\mathbb{P}[N(t) = n] = \frac{(\alpha t)^n}{n!} e^{-\alpha t}\ , \quad \mathbb{P}[N'(t) = n] = \frac{(\alpha' t)^n}{n!} e^{-\alpha' t}$$

Poisson races

- $N'(t)$, resp. $N(t)$, numbers of validated blocks at time t by the selfish, resp. honest, miners are Poisson processes with resp. parameters α' and α, $\alpha' < \alpha$.

$$\mathbb{P}[N(t) = n] = \frac{(\alpha t)^n}{n!} e^{-\alpha t}, \quad \mathbb{P}[N'(t) = n] = \frac{(\alpha' t)^n}{n!} e^{-\alpha' t}$$

Theorem (Poisson Races)

N and N' two independent Poisson processes with parameters α' and α with $\alpha' < \alpha$ and $N(0) = N'(0) = 0$.

Poisson races

- $N'(t)$, resp. $N(t)$, numbers of validated blocks at time t by the selfish, resp. honest, miners are Poisson processes with resp. parameters α' and α, $\alpha' < \alpha$.

$$\mathbb{P}[N(t) = n] = \frac{(\alpha t)^n}{n!} e^{-\alpha t}, \quad \mathbb{P}[N'(t) = n] = \frac{(\alpha' t)^n}{n!} e^{-\alpha' t}$$

Theorem (Poisson Races)

N and N' two independent Poisson processes with parameters α' and α with $\alpha' < \alpha$ and $N(0) = N'(0) = 0$.

Poisson races

- $N'(t)$, resp. $N(t)$, numbers of validated blocks at time t by the selfish, resp. honest, miners are Poisson processes with resp. parameters α' and α, $\alpha' < \alpha$.

$$\mathbb{P}[N(t) = n] = \frac{(\alpha t)^n}{n!} e^{-\alpha t}, \quad \mathbb{P}[N'(t) = n] = \frac{(\alpha' t)^n}{n!} e^{-\alpha' t}$$

Theorem (Poisson Races)

N and N' two independent Poisson processes with parameters α' and α with $\alpha' < \alpha$ and $N(0) = N'(0) = 0$. Then, the stopping time

$$\tau = \inf\{t > 0; N(t) = N'(t) + 1\}$$

is finite a.s. and integrable.

Poisson races

- $N'(t)$, resp. $N(t)$, numbers of validated blocks at time t by the selfish, resp. honest, miners are Poisson processes with resp. parameters α' and α, $\alpha' < \alpha$.

$$\mathbb{P}[N(t) = n] = \frac{(\alpha t)^n}{n!} e^{-\alpha t} , \quad \mathbb{P}[N'(t) = n] = \frac{(\alpha' t)^n}{n!} e^{-\alpha' t}$$

Theorem (Poisson Races)

N and N' two independent Poisson processes with parameters α' and α with $\alpha' < \alpha$ and $N(0) = N'(0) = 0$. Then, the stopping time

$$\tau = \inf\{t > 0; N(t) = N'(t) + 1\}$$

is finite a.s. and integrable. Moreover, we have

$$\mathbb{E}[\tau] = \frac{1}{\alpha - \alpha'} , \quad \mathbb{E}[N'(\tau)] = \frac{\alpha'}{\alpha - \alpha'} , \quad \mathbb{E}[N(\tau)] = \frac{\alpha}{\alpha - \alpha'} .$$

Direct computation of long term profitability

- Example: For $q = 0.1$ and $\gamma = 0.9$ it takes 10 weeks for a selfish mining to become profitable.

Direct computation of long term profitability

- Example: For $q = 0.1$ and $\gamma = 0.9$ it takes 10 weeks for a selfish mining to become profitable.
- It is impossible to obtain this type of result using the Markov model approach.

Direct computation of long term profitability

- Example: For $q = 0.1$ and $\gamma = 0.9$ it takes 10 weeks for a selfish mining to become profitable.
- It is impossible to obtain this type of result using the Markov model approach.
- We present a new, very direct, and elementary approach to compute the Revenue Ratio without using Martingales, nor Markov Chains.

Direct computation of long term profitability

- Example: For $q = 0.1$ and $\gamma = 0.9$ it takes 10 weeks for a selfish mining to become profitable.
- It is impossible to obtain this type of result using the Markov model approach.
- We present a new, very direct, and elementary approach to compute the Revenue Ratio without using Martingales, nor Markov Chains.
- It uses Dyck words, Catalan numbers, and Catalan distributions.

Dyck words and Catalan numbers

Dyck words and Catalan numbers

- A Dyck word of length n built on $\{S, H\}$ is a string consisting of n S's and n H's such that no initial segment of the string has more H's than S's.

Dyck words and Catalan numbers

- A Dyck word of length n built on $\{S, H\}$ is a string consisting of n S's and n H's such that no initial segment of the string has more H's than S's.
- The number of Dyck words with length n is the n-th Catalan number $C_n = \frac{1}{n+1}\binom{2n}{n}$.

Dyck words and Catalan numbers

- A Dyck word of length n built on $\{S, H\}$ is a string consisting of n S's and n H's such that no initial segment of the string has more H's than S's.
- The number of Dyck words with length n is the n-th Catalan number $C_n = \frac{1}{n+1}\binom{2n}{n}$.
- We denote by $C(x) = \frac{1-\sqrt{1-4x}}{2x}$ its generating series, and by $\mathcal{D}$ the space of all Dyck words.

Dyck words and Catalan numbers

- A Dyck word of length n built on $\{S, H\}$ is a string consisting of n S's and n H's such that no initial segment of the string has more H's than S's.
- The number of Dyck words with length n is the n-th Catalan number $C_n = \frac{1}{n+1}\binom{2n}{n}$.
- We denote by $C(x) = \frac{1-\sqrt{1-4x}}{2x}$ its generating series, and by $\mathcal{D}$ the space of all Dyck words.
- Catalan distributions: For $(p, q) \in [0, 1]^2$ with $q < p$ and $p + q = 1$:

$$\sum_{n\geq 0} p(pq)^n C_n = 1$$

$$\sum_{n\geq 0} np(pq)^n C_n = \frac{q}{p-q}$$

Selfish Mining and Dyck words

- The attack cycles of the strategy are described with the chronological sequence of discoveries S and H.

Selfish Mining and Dyck words

- The attack cycles of the strategy are described with the chronological sequence of discoveries S and H.
- For example, *SSSHSHH* is an attack cycle.

Selfish Mining and Dyck words

- The attack cycles of the strategy are described with the chronological sequence of discoveries S and H.
- For example, $SSSHSHH$ is an attack cycle.

Theorem (Selfish Mining and Dyck words)

The attack cycles of the SM strategy are H, SHH, SHS and $SSwH$ where $w \in \mathcal{D}$.

Selfish Mining and Dyck words

- The attack cycles of the strategy are described with the chronological sequence of discoveries S and H.
- For example, $SSSHSHH$ is an attack cycle.

Theorem (Selfish Mining and Dyck words)

The attack cycles of the SM strategy are H, SHH, SHS and $SSwH$ where $w \in \mathcal{D}$.

Selfish Mining and Dyck words

- The attack cycles of the strategy are described with the chronological sequence of discoveries S and H.
- For example, $SSSHSHH$ is an attack cycle.

Theorem (Selfish Mining and Dyck words)

The attack cycles of the SM strategy are H, SHH, SHS and $SSwH$ where $w \in \mathcal{D}$.

Corollary

Let L be the number of official blocks added to the blockchain after an attack cycle. Then, $\mathbb{P}[L = 1] = p$, $\mathbb{P}[L = 2] = p + pq^2$ and

$$\mathbb{P}[L = n] = pq^2(pq)^n C_{n-2}$$

Selfish Mining

- Similarly, we get the distribution of $Z =$ number of blocks mined by the attacker and added to the blockchain after an attack cycle.

Selfish Mining

- Similarly, we get the distribution of $Z =$ number of blocks mined by the attacker and added to the blockchain after an attack cycle.
- We express a dimensionless Revenue Ratio in b/τ_0 units where $b =$ is the coinbase and $\tau_0 =$ Bitcoin interblock time.

Theorem (Revenue Ratio of SM strategy)

The Revenue Ratio of SM is

$$\Gamma_B = \frac{[(p-q)(1+pq)+pq]q-(p-q)(1-\gamma)p^2q}{pq^2+p-q}$$

Selfish Mining

- Similarly, we get the distribution of $Z =$ number of blocks mined by the attacker and added to the blockchain after an attack cycle.
- We express a dimensionless Revenue Ratio in b/τ_0 units where $b =$ is the coinbase and $\tau_0 =$ Bitcoin interblock time.

Theorem (Revenue Ratio of SM strategy)

The Revenue Ratio of SM is

$$\Gamma_B = \frac{[(p-q)(1+pq)+pq]q-(p-q)(1-\gamma)p^2q}{pq^2+p-q}$$

Selfish Mining

- Similarly, we get the distribution of $Z =$ number of blocks mined by the attacker and added to the blockchain after an attack cycle.
- We express a dimensionless Revenue Ratio in b/τ_0 units where $b =$ is the coinbase and $\tau_0 =$ Bitcoin interblock time.

Theorem (Revenue Ratio of SM strategy)

The Revenue Ratio of SM is

$$\Gamma_B = \frac{[(p-q)(1+pq)+pq]q-(p-q)(1-\gamma)p^2q}{pq^2+p-q}$$

Sketch of proof.

We have $\mathbb{E}[T] = \mathbb{E}[L]\tau_0$, $\mathbb{E}[Z] = \mathbb{E}[L] - \left(p + (2-\gamma)p^2q\right)$ and $\mathbb{E}[L] = 1 + \frac{p^2q}{p-q}$. □

Other classical block witholding strategies

Other classical block witholding strategies

- LSM and EFSM: strategies invented by Miller & al.

Other classical block witholding strategies

- LSM and EFSM: strategies invented by Miller & al.

Theorem (Revenue Ratio of LSM strategy)

The Revenue Ratio of LSM is

$$\Gamma_{LSM} = \frac{q(p+pq-q^2)}{p+pq-q} - \frac{pq(p-q)(1-\gamma)}{\gamma} \cdot \frac{1-p(1-\gamma)C((1-\gamma)pq)}{p+pq-q}$$

Other classical block witholding strategies

- LSM and EFSM: strategies invented by Miller & al.

Theorem (Revenue Ratio of LSM strategy)

The Revenue Ratio of LSM is

$$\Gamma_{LSM} = \frac{q(p+pq-q^2)}{p+pq-q} - \frac{pq(p-q)(1-\gamma)}{\gamma} \cdot \frac{1-p(1-\gamma)C((1-\gamma)pq)}{p+pq-q}$$

Other classical block witholding strategies

- LSM and EFSM: strategies invented by Miller & al.

Theorem (Revenue Ratio of LSM strategy)

The Revenue Ratio of LSM is

$$\Gamma_{LSM} = \frac{q(p+pq-q^2)}{p+pq-q} - \frac{pq(p-q)(1-\gamma)}{\gamma} \cdot \frac{1-p(1-\gamma)C((1-\gamma)pq)}{p+pq-q}$$

Theorem (Revenue Ratio of EFSM strategy)

The Revenue Ratio of EFSM is

$$\Gamma_{EFSM} = \frac{q}{p} - \frac{(1-\gamma)(p-q)}{\gamma p}\left(1-pC\left((1-\gamma)pq\right)\right)$$

Comparison of strategies

Comparison of strategies

We color the region $(q, \gamma) \in [0, 0.5] \times [0, 1]$ according to which strategy is more profitable.

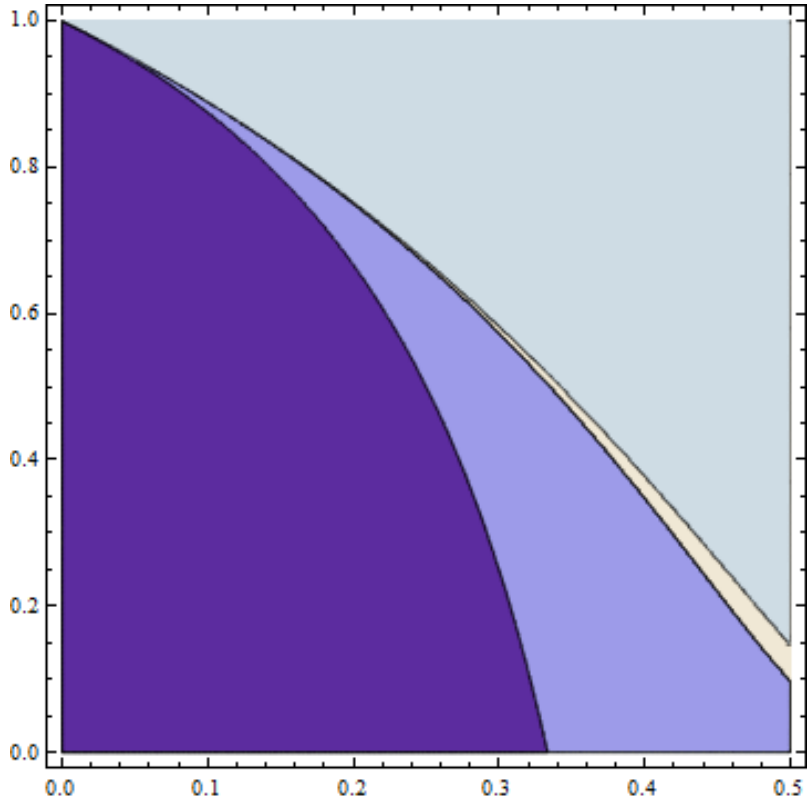


Figure: From left to right: HM, SM, LSM, EFSM.

Ethereum mining rewards

- Different reward system and difficulty adjustment algorithm.

Ethereum mining rewards

- Different reward system and difficulty adjustment algorithm.
- Takes uncles and nephews into account.

Ethereum mining rewards

- Different reward system and difficulty adjustment algorithm.
- Takes uncles and nephews into account.
- Only one SM strategy in Bitcoin but several in Ethereum

Ethereum mining rewards

- Different reward system and difficulty adjustment algorithm.
- Takes uncles and nephews into account.
- Only one SM strategy in Bitcoin but several in Ethereum
- SM1: Maximum belligerence and signals all uncles. Goal: Maximize the revenue.

Ethereum mining rewards

- Different reward system and difficulty adjustment algorithm.
- Takes uncles and nephews into account.
- Only one SM strategy in Bitcoin but several in Ethereum
- SM1: Maximum belligerence and signals all uncles. Goal: Maximize the revenue.
- SM2A: Minimum belligerence and signals all uncles.

Ethereum mining rewards

- Different reward system and difficulty adjustment algorithm.
- Takes uncles and nephews into account.
- Only one SM strategy in Bitcoin but several in Ethereum
- SM1: Maximum belligerence and signals all uncles. Goal: Maximize the revenue.
- SM2A: Minimum belligerence and signals all uncles.
- SM2B: Minimum belligerence and signals no uncle. Goal: Minimize the difficulty parameter.

Selfish Mining in Ethereum

Theorem (Comparison of SM strategies in Ethereum)

For any (q, γ), $\Gamma(SM1) < \Gamma(SM2A)$ *and for* $q > 30.1\%$, $\Gamma(SM2A) < \Gamma(SM2B)$

Selfish Mining in Ethereum

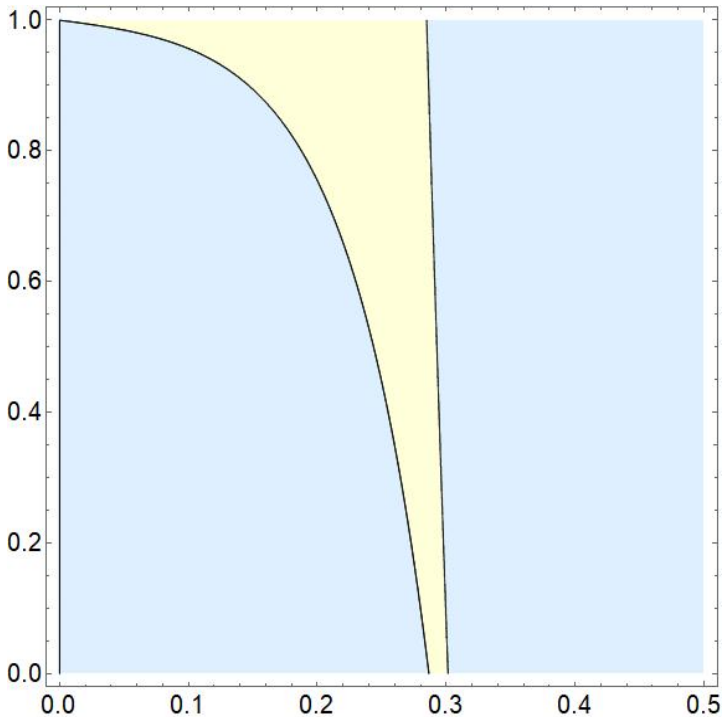
Theorem (Comparison of SM strategies in Ethereum)

For any (q, γ), $\Gamma(SM1) < \Gamma(SM2A)$ *and for* $q > 30.1\%$, $\Gamma(SM2A) < \Gamma(SM2B)$

Selfish Mining in Ethereum

Theorem (Comparison of SM strategies in Ethereum)

For any (q, γ), $\Gamma(SM1) < \Gamma(SM2A)$ *and for* $q > 30.1\%$, $\Gamma(SM2A) < \Gamma(SM2B)$



Threshold of profitabilities Bitcoin/Ethereum

Ethereum more resilient than Bitcoin iff $q < q_0$ with $q_0 \approx 25\%$.

Threshold of profitabilities Bitcoin/Ethereum

Ethereum more resilient than Bitcoin iff $q < q_0$ with $q_0 \approx 25\%$.

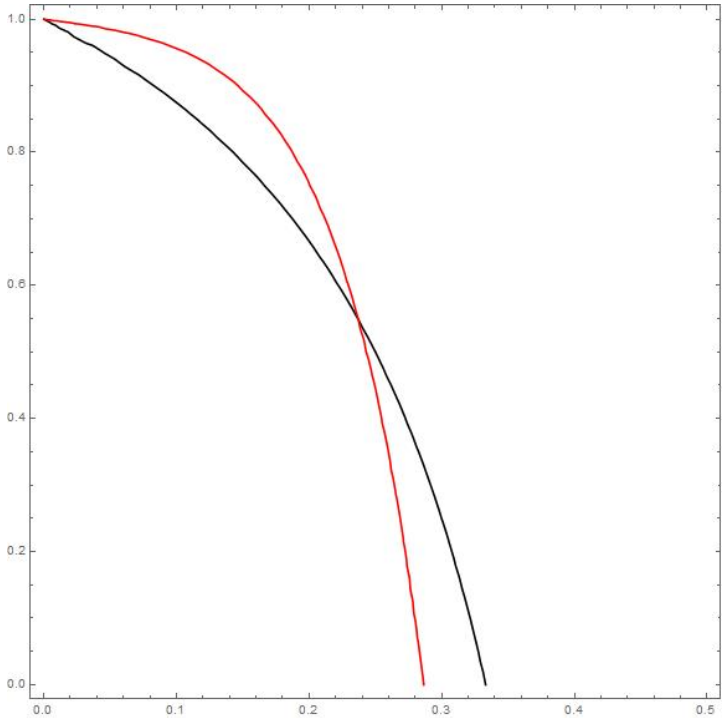


Figure: Blue: Bitcoin, Red: SM2A

Conclusions

- The **Revenue Ratio** is the correct objective function to compare profitabilities of mining strategies and not the ”relative revenue”.

Conclusions

- The **Revenue Ratio** is the correct objective function to compare profitabilities of mining strategies and not the ”relative revenue”.
- Direct combinatorial approach with Dyck words for long term profitability. Gives closed-form formulas.

Conclusions

- The **Revenue Ratio** is the correct objective function to compare profitabilities of mining strategies and not the ”relative revenue”.
- Direct combinatorial approach with Dyck words for long term profitability. Gives closed-form formulas.
- The study in Ethereum confirms that SM is an attack to the DA.

Conclusions

- The **Revenue Ratio** is the correct objective function to compare profitabilities of mining strategies and not the ”relative revenue”.
- Direct combinatorial approach with Dyck words for long term profitability. Gives closed-form formulas.
- The study in Ethereum confirms that SM is an attack to the DA.
- Ethereum is more resilient to SM than Bitcoin for small hashrates.

Conclusions

- The **Revenue Ratio** is the correct objective function to compare profitabilities of mining strategies and not the ”relative revenue”.
- Direct combinatorial approach with Dyck words for long term profitability. Gives closed-form formulas.
- The study in Ethereum confirms that SM is an attack to the DA.
- Ethereum is more resilient to SM than Bitcoin for small hashrates.
- Ethereum continuous Difficulty Adjustment favors SM.

Conclusions

- The **Revenue Ratio** is the correct objective function to compare profitabilities of mining strategies and not the ”relative revenue”.
- Direct combinatorial approach with Dyck words for long term profitability. Gives closed-form formulas.
- The study in Ethereum confirms that SM is an attack to the DA.
- Ethereum is more resilient to SM than Bitcoin for small hashrates.
- Ethereum continuous Difficulty Adjustment favors SM.
- Ethereum has a better DA formula than in Bitcoin because in considers uncles, but has a biased reward system.

Conclusions

- The **Revenue Ratio** is the correct objective function to compare profitabilities of mining strategies and not the ”relative revenue”.
- Direct combinatorial approach with Dyck words for long term profitability. Gives closed-form formulas.
- The study in Ethereum confirms that SM is an attack to the DA.
- Ethereum is more resilient to SM than Bitcoin for small hashrates.
- Ethereum continuous Difficulty Adjustment favors SM.
- Ethereum has a better DA formula than in Bitcoin because in considers uncles, but has a biased reward system.
- Best strategy (for $q > 25\%$): Avoid competitions and ignore uncles.

Thank you for your attention!