Discounted Selfish Mining: Is It Profitable?

Jing Huang

University of Chicago

Ling Ren

University of Illinois Urbana-Champaign

June 3, 2021

ABFER 8th Annual Conference

Blockchain & Cryptocurrency

Introduction

Rational Agents

- *Protocols*$\neq$*mechanisms* that implement equilibrium
  - Protocols to solve fault tolerant replication
  - *Honest parties*: follow what the protocols "program" them to do
- Rational agents and exploitation of protocols

Selfish Mining

- Block holding attack under Nakamoto Protocol
  - Strategically times block dissemination to orphan others
  - Payoff larger than fair share

Selfish Mining

Question: Why haven't we observed selfish mining in practice?

Some explanations

- Stakeholders: care about Bitcoin value.
- Computation power to attack still demanding.

But... agents could rent computation power to attack, and short sell.

This paper: discounted payoff in selfish mining not profitable!

- At 3% annual rate, threshold computation power increases by 20%.

This Paper

Analytical tractable framework

- Incorporate "time" for a general class of selfish mining strategies
  - Cash flow arrivals, difficulty adjustment

Tradeoffs within selfish mining

- Accumulate strategic advantage
- Time preference, uncertainty in cash flow arrival, (other financial frictions, limits of arbitrage)
- Inventory policies

Incentive for attacking

- Higher computation power threshold
- Sensitivity to γ

Implications

- Forking
- Safety vs liveness

Related Literature

Selfish Mining

- Eyal and Sirer (2014), Nayak, Kumar, Miller, and Shi (2016), Sapirshtein, Sompolinsky, and Zohar (2016)

Mitigation of Selfish Mining

- Zhang and Preneel (2019),Pass and Shi (2017)

Blockchain Incentives

- Eyal (2015), Carlsten, Kalodner, Weinberg, and Narayanan (2016)

Links to Economic Literature

- Folk Theorem in repeated games, Shleifer and Vishny (1997)

Road Map

Background

- Nakamoto Protocol
- Selfish Mining

Analytical Framework

- Model setup
- Discounted payoffs

Strategies and Attack Incentive

- Different strategies and difficulty adjustment
- Incentive to attack

Implications and Conclusion

- Safety vs. liveliness
- Folk theorem in repeated games

Bitcoin Blockchain

Bitcoin Blockchain

- Decentralized ledger keeping (script: BTC transactions)
- Miners: permissionless network

Nakamoto Protocol

- Randomly choosing leader via PoW crypto puzzles; BTC reward.

1. Longest chain rule.
2. Immediate dissemination.

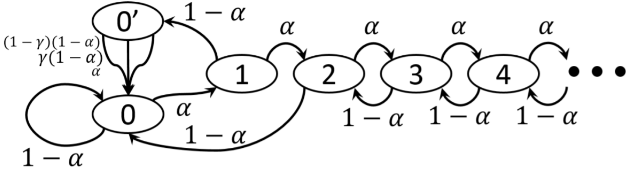
- Important details
  - Fork of equal length: randomly choose one.
  - Difficulty adjustment: per 2016 blocks to target speed at 10min/ block
    - Flexibility for open network vs. Randomness

Selfish mining: rational miner's incentive to follow 2. immediate disemmination?

Selfish Mining

Eyal and Sirer (2014)

- Withhold mined blocks and time the publishing: higher payoff



  - $s = 0, 1, 2, \cdots$: # withheld blocks on private chain
  - $0'$: two forks of equal length under public view

- Where do the gains come from? Forking rule.
  - Lead $s \geq 2$: longest chain rule. Orphan others, and withheld blocks are rewarded.
  - Lead $s = 1$: risky. Who mines the next block? (α) Which fork to follow? (γ)

- Our baseline strategy in the presentation.

Selfish Mining: Markovian Strategy

Why does hurting others benefit myself?

- Riskiness in the reward for $s = 1$. Delaying payoff.

Zero-Sum Game

- Fixed total stock of BTC. Selfish mining till the end.
- Increase my mining efficiency: difficulty adjustment.

Why haven't we observed any selfish mining attacks?

- Long-term deviation.

Road Map

Model Setup (1)

Players

- Fixed set of agents. One active agent —selfish *"miner"*, and *"others"* who follow Nakamoto.

Mining

- Crypto puzzle is randomly solved with Poisson intensity λ, which is subject to difficulty adjustment.
- Miner has α fraction of computation power.
  - w.p. $\alpha\lambda dt$, miner solves first and thus mines a block.
- Upon concensus that a block is on the longest chain, reward 1 BTC=$1 to whoever mined it.
  - No transaction delay
  - Equal-length forks: w.p. γ, concensus is on the miner's chain.

Miner's utility

$$U = rV \equiv r\mathbb{E}_0\left[\int_0^\infty \left(e^{-rt} \underbrace{c_t}_{\text{cash flow}}\right) dt\right],$$

- r: instantaneous time discount. Relatively high for experts: funding cost, outside options and etc.

Model Setup (2)

Difficulty adjustment

- Crypto difficulty starts with $\lambda = \lambda_0$.
- Approximation: with Poisson intensity β, evaluate block arrival rate $\lambda^{\text{disseminate}}$ on the longest chain.
  - Assume states have reached stationary distribution.
  - If $\mathbb{E}_t\left[\lambda^{\text{disseminate}}\right] = \lambda_0$, do not adjust; otherwise, crypto difficulty adjusts $\lambda_1 = \frac{\lambda_0}{\mathbb{E}_t\left[\lambda^{\text{disseminate}}\right]}$.
- Follow Nakamoto: effectively never adjusts, $\lambda = \lambda_0$.
- Selfish mining: $\lambda = \lambda_0$ before adjustment; crypto difficulty adjusts to λ_1 at $t = \tau$ once and for all.

Start with benchmarks $\beta \in \{0, 1\}$

- $\beta = 0$: cash flow arrives more slowly under selfish mining.

Incorporate Time Discount (1)

Dynamic Programming$\rightarrow$difference equations for value functions

- s: payoff relevant state variables. $V(s)$: value to miner evaluated at $t=0$.

Follow Nakamoto

- There is no state transition. HJB

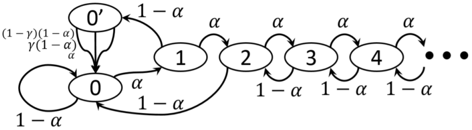
$$\underbrace{(r+1)\,dt}_{\textbf{gross return}} V^0 = \underbrace{\alpha\lambda\,dt}_{\textbf{my block}} \left(\underbrace{1}_{\textbf{flow}} + \underbrace{V^0}_{\textbf{continuation}} \right) + (1-\alpha)\,\lambda\,dt \cdot V^0 + (1-\lambda)\,dt \cdot V^0$$

Hence, $V^0 = \frac{\alpha\lambda}{r}$

Incorporate Time Discount (2)

Selfish Mining

- State variable $s = 0, 1, 1', 2, 3, \cdots$: stock of blocks in private chain.



- When $s \geq 3$, assume cashing in upon miner's publishing

$$\underbrace{rV(s)}_{\text{required return}} = \underbrace{(1-\alpha)\lambda}_{\text{public chain gains}} \left(\underbrace{1}_{\text{flow}} + \underbrace{V(s-1) - V(s)}_{\text{continuation/capital gain}} \right) + \underbrace{\alpha\lambda}_{\text{private chain gains}} \left(V(s+1) - V(s) \right)$$

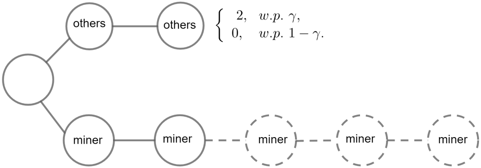
- Analytical solution for $V(s)$
  - Second order difference equation.
  - Two boundary conditions: $s = \infty$, transitions $s = 0, 0', 1, 2$.
- *But, is the published block cashed in immediately?*

Cash-in Time of Private Blocks (1)

Without discount: are blocks eventually rewarded?

- Yes, for $s \geq 2$. At $s = 2$: publish 2 once others mine a block.

With discount: γ also matters for block values when $s \geq 3$!



$$\begin{cases} 2, & w.p.\ \gamma, \\ 0, & w.p.\ 1-\gamma. \end{cases}$$

Rewarded eventually due to s=2 strategy

- Cash in time: upon concensus that block is on the longest chain.
  - Qualitative benchmark.
- m: # of unrewarded, published blocks. When $s > 2$ and $m > 0$,

$$rV(s,m) = \underbrace{(1-\alpha)\lambda}_{\text{public chain gains}} \left[\underbrace{\gamma}_{\text{win}} \left(\underbrace{m+1}_{\text{cash in}} + V(s-1,0) - V(s,m) \right) + \underbrace{(1-\gamma)}_{\text{lose}} \left(V(s-1,m+1) - V(s,m) \right) \right]$$
$$+ \underbrace{\alpha\lambda}_{\text{private chain gains}} \left(V(s+1,m) - V(s,m) \right)$$

Cash-in Time of Private Blocks (2)

- Same value $v(s)$ for each postponed reward in m: $V(s,m)$ satisfy

$$V(s,m) = h(s) + m \cdot v(s). \quad (1)$$

- One state variable! For $s \geq 3$, per postponed reward $v(s)$

$$rv(s) = \underbrace{\alpha\lambda\left[v(s+1) - v(s)\right]}_{\text{private chain gains}} + \underbrace{(1-\alpha)\lambda}_{\text{public chain gains}}\left[\gamma\underbrace{(1+0-v(s))}_{\text{win: cash in}} + \underbrace{(1-\gamma)(v(s-1)-v(s))}_{\text{lose: continuation value}}\right]$$

Intercept value $h(s)$

$$rh(s) = \underbrace{\alpha\lambda\left[h(s+1) - h(s)\right]}_{\text{private chain gains}} + \underbrace{(1-\alpha)\lambda}_{\text{public chain gains}}\left[\underbrace{\gamma(1+h(s-1)-h(s))}_{\text{win: cash in}} + \underbrace{(1-\gamma)(v(s-1)+h(s-1)-h(s))}_{\text{lose: +1 delayed payoff}}\right]$$

- Analytical solution!

Road Map

Background

- Nakamoto Protocol
- Selfish Mining

Analytical Framework

- Model setup
- Discounted payoffs

Strategies and Attack Incentive

- Different strategies and difficulty adjustment
- Incentive to attack

Implications and Conclusion

- Safety vs. liveliness

Tradeoffs in Selfish Mining Strategies

Strategic advantage

- Accumulate private lead: stubborn mining, short-term loss

On the other hand, discount and uncertainty in reward time

- Inventory policy: stop accumulating when $s = k$, immediate publish.
  - Boundary condition at k

$$rV(k,m) = \underbrace{\alpha\lambda(m+1)}_{\text{immediate publish, no state transition}} + (1-\alpha)\lambda\left[(m+1) + \gamma V(k-1,0) + (1-\alpha)\lambda(1-\gamma)V(k-1,m+1)\right]$$

  - We find that k does not increase value when $k \geq \underline{k}$.
    In contrast, without discount, tail states $s \geq k$ brings in positive gain.
- Uncertainty in reward time: if $\gamma \to 0$, may even publish 2 blocks at $s \geq 3$.

Others Concerns

- Borrowing frictions: unable to take short-term loss.

Incentive to Attack

Without difficulty adjustment

- If BTC stock sufficiently large, never attack.

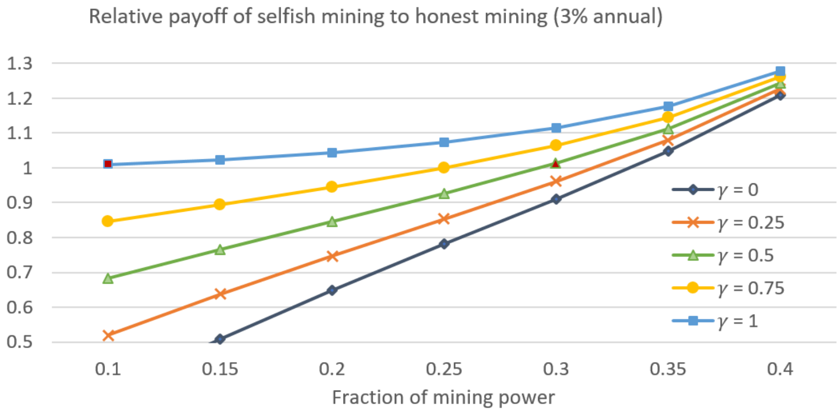
Incorporating difficulty adjustment

- $V(s,m;\lambda_1)$: continuation value after adjustment. When $s \geq 3$,

$$
\begin{aligned}
r\tilde{V}(s,m) =& \underbrace{\beta\left(V(s,m;\lambda_1)-\tilde{V}(s,m)\right)}_{\text{difficulty adjustment}} \\
&+ \underbrace{(1-\alpha)\lambda}_{\text{public chain gains}}\left[\underbrace{\gamma}_{\text{win}}\left(\underbrace{m+1}_{\text{cash in}}+\tilde{V}(s-1,0)-\tilde{V}(s,m)\right)+\underbrace{(1-\gamma)}_{\text{lose}}\left(\tilde{V}(s-1,m+1)-\tilde{V}(s,m)\right)\right] \\
&+ \underbrace{\alpha\lambda}_{\text{private chain gains}}\left(\tilde{V}(s+1,m)-\tilde{V}(s,m)\right)
\end{aligned}
$$

- 2016 rule and small r: $\tilde{V}(s,m) \approx V(s,m;\lambda_1)$.

Incentive to Attack (2)



- Small r: $\gamma = 0.5$, hurdle $\alpha \uparrow 20\%$; $\gamma \to 1$, require significant α.
- Intermediate r: compensated by difficulty adjustment.
  - annual r=40%, two-week effect small.

Mitigating Selfish Mining

Safety vs. Liveliness

- $\downarrow$ Postpone difficulty adjustment: β
- $\downarrow$ Block generation intensity λ_0

Protocols

- Selfish mining takes advantage of forking
- Difficulty adjustment: count orphaned blocks (these are solved crypto puzzles)

Economics

"Off-equilibrium strategies"

- Desirable outcome: immediate dissemination.
- Miner takes advantage of forking rules. Forking: trembling hand path.
- Properly define strategies upon long forks: restrict selfish mining strategy space.

Folk Theorem and Repeated Games

- If the players are patient enough and far-sighted ($r \to 0$), then repeated interaction can result in virtually any average payoff in an SPE equilibrium.
- Importance of discount!

Conclusions

- The long-term feature of selfish mining has important financial implications
  - Discount, (limits of arbitrage and etc)
  - Ex ante contract
- Importance of “off-equilibrium” strategies
  - Unable to design
  - Neglected to design

References

Carlsten, Miles, Harry Kalodner, S Matthew Weinberg, and Arvind Narayanan, 2016, 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.

Eyal, Ittay, 2015, The miner's dilemma, in *2015 IEEE Symposium on Security and Privacy* pp. 89–103. IEEE.

———, and Emin Gün Sirer, 2014, Majority is not enough: Bitcoin mining is vulnerable, in *International conference on financial cryptography and data security* pp. 436–454. Springer.

Nayak, Kartik, Srijan Kumar, Andrew Miller, and Elaine Shi, 2016, Stubborn mining: Generalizing selfish mining and combining with an eclipse attack, in *2016 IEEE European Symposium on Security and Privacy (EuroS&P)* pp. 305–320. IEEE.

Pass, Rafael, and Elaine Shi, 2017, Fruitchains: A fair blockchain, in *Proceedings of the ACM Symposium on Principles of Distributed Computing* pp. 315–324.

Sapirshtein, Ayelet, Yonatan Sompolinsky, and Aviv Zohar, 2016, Optimal selfish mining strategies in bitcoin, in *International Conference on Financial Cryptography and Data Security* pp. 515–532. Springer.

Shleifer, Andrei, and Robert W Vishny, 1997, The limits of arbitrage, *The*