On the Security and Scalability of Proof of Work Blockchains

Arthur Gervais

ETH Zurich

Scaling Bitcoin 2016 - Milan
Synchronization

Broadcast of transactions/blocks

- All transactions, blocks need to be broadcast into the whole network

- Larger blocks
  - slower propagation
  - increased consensus latency

- Risks of network partition (stale blocks...)
Synchronization

Broadcast of transactions/blocks

- All transactions, blocks need to be broadcast into the whole network

- Larger blocks
  - slower propagation
  - increased consensus latency

- Risks of network partition (stale blocks...)
Synchronization

Broadcast of transactions/blocks

- All transactions, blocks need to be broadcast into the whole network
  - Larger blocks
    - Slower propagation
    - Increased consensus latency
  - Risks of network partition (stale blocks…)

---
Synchronization

Broadcast of transactions/blocks

• All transactions, blocks need to be broadcast into the whole network

• Larger blocks
  slower propagation
  increased consensus latency

• Risks of network partition (stale blocks…)

[Diagram showing network nodes and arrows for broadcast of transactions/blocks]
Synchronization

Broadcast of transactions/blocks

- All transactions, blocks need to be broadcast into the whole network

- Larger blocks
  - Slower propagation
  - Increased consensus latency

- Risks of network partition (stale blocks…)

Selfish Mining
Denial of Service
Double Spending
Decentralised PoW Blockchains

Which one is a better Blockchain?

- Bitcoin: 10 minutes
- Litecoin: 2.5 minutes
- Dogecoin: 1 minute
- Ethereum: 20 seconds
Decentralised PoW Blockchains

Which one is a better Blockchain?

**Faster block generation**
- Bitcoin: 10 minutes
- Litecoin: 2.5 minutes
- Dogecoin: 1 minute
- Ethereum: 20 seconds

**Faster payments**

**Bigger block size**

**More payments / slower propagation**
Decentralised PoW Blockchains

Which one is a better Blockchain?

- **Faster block generation**
- **Bigger block size**
- **Faster payments**
- **More payments / slower propagation**

<table>
<thead>
<tr>
<th></th>
<th>Bitcoin</th>
<th>Litecoin</th>
<th>Dogecoin</th>
<th>Ethereum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Propagation Time</td>
<td>8.7 s</td>
<td>1.02 s</td>
<td>0.85 s</td>
<td>0.5 - 0.75 s</td>
</tr>
<tr>
<td>Medium Block size</td>
<td>534.8 KB</td>
<td>6.11 KB</td>
<td>8 KB</td>
<td>1.5 KB</td>
</tr>
</tbody>
</table>
Contributions

Quantitative Framework

- Compare security of PoW blockchains
- Account for double-spending and selfish mining
- Determine the optimal adversarial strategies
- Provide # of secure confirmations depending on tx value
- Increasing throughput without penalizing security

Open Source Bitcoin Simulator

- Realistic simulation of network and blockchain properties
- Flexible reparametrization
- Scalable to thousands of nodes
- Open Source and documented
Decentralised PoW Blockchains

Blockchain and Forks

Block 1 → Block 2 → Block 3 → Block 4
Decentralised PoW Blockchains

Blockchain and Forks

Block 1

Block 2

Block 3

Block 4

Block 3'

Block 4'
Blockchain and Forks

Block 1 → Block 2 → Block 3 → Block 4

Block 3' → Block 4'

Stale blocks = lost effort
Decentralised PoW Blockchains

Blockchain and Forks

Block 1

Block 2

Block 3

Block 4

Block 3'

Block 4'

Stale blocks = lost effort

Block 1''

Block 2''

Block 3''

Block 4''

Block 5''
Decentralised PoW Blockchains

Blockchain and Forks

Stale blocks = lost effort

Block 1
Block 2
Block 3
Block 4

Block 1’
Block 2’
Block 3’
Block 4’

Block 1”
Block 2”
Block 3”
Block 4”
Block 5”

Stale Block rates

<table>
<thead>
<tr>
<th>Currency</th>
<th>Stale Block Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin</td>
<td>0.41%</td>
</tr>
<tr>
<td>Litecoin</td>
<td>0.273%</td>
</tr>
<tr>
<td>Dogecoin</td>
<td>0.619%</td>
</tr>
<tr>
<td>Ethereum</td>
<td>6.8%</td>
</tr>
</tbody>
</table>
Double Spending

$TX_{\text{legitimate}}$ - Pays the vendor

$TX_{\text{doublespend}}$ - Pays the adversary
**Double Spending**

- $\text{TX}_{\text{legitimate}}$ - Pays the vendor
- $\text{TX}_{\text{doublespend}}$ - Pays the adversary
Double Spending

$TX_{\text{legitimate}}$ - Pays the vendor

$TX_{\text{doublespend}}$ - Pays the adversary
Double Spending

$\text{TX}_{\text{legitimate}}$ - Pays the vendor

$\text{TX}_{\text{doublespend}}$ - Pays the adversary
Double Spending

\( \text{TX}_{\text{legitimate}} \) - Pays the vendor

\( \text{TX}_{\text{doublespend}} \) - Pays the adversary
What is Selfish Mining? [Eyal and Sirer]

- Instead of publishing, keep a block private
- Release block to compete

Other miners will perform wasteful computations
Adversary loses block rewards
Selfish Mining vs. Double Spending

**Selfish Mining**
- Increases *relative* reward
- Not necessarily rational

**Double Spending**
- Increase *absolute* reward
- Economically rational adversary

Consider them independently
Towards a better Blockchain

Block generation

Slower payments → Slower

Faster payments → Faster

better security

Faster propagation

Smaller

Bigger

Slower propagation
Understanding Security / Performance of PoW Blockchains

**Framework**

- Consensus & Network parameters
  - PoW Blockchain
  - Block propagation times
  - Throughput

- Stale block rate

**Security parameters**

- Security Model
  - Optimal adversarial strategy
  - Security characteristics
**Decentralised Blockchain**

**PoW Blockchain**

Blockchain instance can be
- A **real** blockchain (e.g. Bitcoin, Ethereum)
- **Simulated** blockchain

Simulator captures (**Open Source**)

<table>
<thead>
<tr>
<th>Consensus parameter</th>
<th>Network-Layer Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block interval distribution</td>
<td>Block size distribution</td>
</tr>
<tr>
<td>Mining power dist.</td>
<td>Geographical distribution of nodes/miners</td>
</tr>
<tr>
<td></td>
<td>Number of connections of nodes/miners</td>
</tr>
<tr>
<td></td>
<td>Propagation Protocol</td>
</tr>
</tbody>
</table>

- Stale block rate
- Block propagation times
- Throughput
**PoW Blockchain**

Blockchain instance can be
- A **real** blockchain (e.g. Bitcoin, Ethereum)
- **Simulated** blockchain

**Simulator captures (Open Source)**

<table>
<thead>
<tr>
<th>Consensus parameter</th>
<th>Network-Layer Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block interval distribution</td>
<td>Block size distribution</td>
</tr>
<tr>
<td>Mining power dist.</td>
<td>Geographical distribution of nodes/miners</td>
</tr>
<tr>
<td>Number of connections of nodes/miners</td>
<td>Propagation Protocol</td>
</tr>
</tbody>
</table>
**Decentralised Blockchain**

## PoW Blockchain

Blockchain instance can be
- A **real** blockchain (e.g. Bitcoin, Ethereum)
- **Simulated** blockchain

**Simulator captures (Open Source)**

<table>
<thead>
<tr>
<th>Consensus parameter</th>
<th>Network-Layer Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block interval distribution</td>
<td>Block size distribution</td>
</tr>
<tr>
<td>Mining power dist.</td>
<td>Geographical distribution of nodes/miners</td>
</tr>
<tr>
<td></td>
<td>Number of connections of nodes/miners</td>
</tr>
</tbody>
</table>

**Consensus & Network parameters**

- Stale block rate
- Block propagation times
- Throughput

**Propagation Protocol**

<table>
<thead>
<tr>
<th>Region</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td>51.59%</td>
</tr>
<tr>
<td>North America</td>
<td>38.69%</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>1.13%</td>
</tr>
<tr>
<td>South America</td>
<td>1.66%</td>
</tr>
<tr>
<td>Japan</td>
<td>1.19%</td>
</tr>
<tr>
<td>Australia</td>
<td>5.74%</td>
</tr>
</tbody>
</table>
Security Model

Captures **optimal adversarial** strategies
- for Selfish Mining
- for Double Spending
- based on **Markov Decision Processes**

Security Parameters
- Adversarial mining power
- Stale block rate
- Connectivity of the adversary
- Impact of eclipse attacks
- Mining costs
- Number of required confirmations
Markov Decision Process

Extension of Markov Chains
- Adds actions and rewards
- State space and action space

State: (3, 1)
Markov Decision Process

Extension of Markov Chains
- Adds actions and rewards
- State space and action space

State: (3, 1)

Attacker chain
Markov Decision Process

Extension of Markov Chains
- Adds actions and rewards
- State space and action space

State: (3, 1)
Markov Decision Process

Extension of Markov Chains

- Adds actions and rewards
- State space and action space

State: (3, 1)

Attacker chain

Honest chain
Markov Decision Process

Extension of Markov Chains
- Adds actions and rewards
- State space and action space

State: (3, 1)

Reward for adversary: 2
Markov Decision Process

Extension of Markov Chains
- Adds actions and rewards
- State space and action space

State: (3, 1) ➔ (1, 1)

Reward for adversary: 2

Attacker chain

Honest chain
How many confirmations required to match security?

Stale block rate

- Ethereum: 6.8%
- Bitcoin: 0.41%
How many confirmations required to match security?

**smaller block rewards**

**higher stale block rate**

| Stale block rate | 6.8 % | 0.41 % |
How many confirmations required to match security?

smaller block rewards

higher stale block rate

Stale block rate
6.8 %
0.41 %

Matching Block confirmations, 30% adversary
37
6
12.4 minutes
60 minutes

Litecoin would require 28, and Dogecoin 47 block confirmations respectively to match the security of 6 Bitcoin confirmations.
Increasing throughput?

Based on Simulator results

- 1 MB blocks
- 1 Minute Block interval
Selected findings

Increasing throughput?

Based on Simulator results

- 1 MB blocks
- 1 Minute Block interval

Stale block rate does not increase substantially
Increasing throughput?

Based on Simulator results

- 1 MB blocks
- 1 Minute Block interval

Stale block rate does not increase substantially

From 7 tps to 60 tps, without sacrificing security
Selected findings

Selfish Mining under constant difficulty

Mining 1000 blocks

- 30% selfish miner mines 209 blocks, instead of 300! (under optimal strategy)
- Eyal and Sirer’s strategy yields on average 205.8 blocks

Selfish Mining yield fewer block rewards than honest mining.
Influence of Stale Block rate on Selfish Mining

The higher the stale block rate the higher the relative revenue
Double-Spending

Profitability depends on transaction value

- Quantifying resilience using minimum $v_d$, s.t. double-spending is profitable

![Graph showing profitability against stale rate $r_s$ for Bitcoin and Ethereum, with lines representing different values of $\alpha$.]
Double-Spending

Profitability depends on transaction value

- Quantifying resilience using minimum $v_d$, s.t. double-spending is profitable

The higher the $v_d$, the better

Threshold at which double-spending is more profitable than honest mining
Selected findings

Number of required confirmations (Bitcoin)

The graph shows the relationship between the number of necessary confirmations \( k \) and the adversarial mining power \( \alpha \). The graph includes three lines, each representing a different value of \( v_d \):

- Blue line: \( v_d = $100000 \)
- Green line: \( v_d = $10000 \)
- Red line: \( v_d = $1000 \)

As \( \alpha \) increases from 0.0 to 0.5, the necessary confirmations \( k \) increase significantly, especially for higher values of \( v_d \).
Double Spending Bitcoin vs. Ethereum

Double-spending resistance of Ethereum (k in \{6, 12\}) vs. Bitcoin (k=6)
Selected findings

Block reward impact

For a fixed transaction value
- We show that the higher the block reward (e.g., in USD), the more resilient it is against double-spending

Merchant can vary the # of confirmations depending on the transaction value
Summary

Quantitative Framework

Compare PoW blockchains objectively

- Selfish Mining not always rational
- Double Spending is rational

Blockchain Simulator
http://arthurgervais.github.io/Bitcoin-Simulation/index.html
Summary

Quantitative Framework

Compare PoW blockchains objectively

- Selfish Mining not always rational
- Double Spending is rational

Blockchain Simulator
http://arthurgervais.github.io/Bitcoin-Simulation/index.html

Block confirmation equivalence

6 Bitcoin = 37 Ethereum (20 sec)
= 28 Litecoin (2.5 min)
= 47 Dogecoin (1 min)

The higher the block reward in USD, the more resilient against double spending
Summary

Quantitative Framework

Compare PoW blockchains objectively

- Selfish Mining not always rational
- Double Spending is rational

Blockchain Simulator
http://arthurgervais.github.io/Bitcoin-Simulation/index.html

Block confirmation equivalence

6 Bitcoin = 37 Ethereum (20 sec)
  = 28 Litecoin (2.5 min)
  = 47 Dogecoin (1 min)

The higher the block reward in USD, the more resilient against double spending

Good block size/interval

1 MB block and
1 Minute block interval

+60 transactions/s without scarifying security

(instead of Bitcoin 7 tps)
Summary

Quantitative Framework

Compare PoW blockchains objectively

- Selfish Mining not always rational
- Double Spending is rational

Block confirmation equivalence

6 Bitcoin = 37 Ethereum (20 sec)
  = 28 Litecoin (2.5 min)
  = 47 Dogecoin (1 min)

The higher the block reward in USD, the more resilient against double spending

Good block size/interval

1 MB block and
1 Minute block interval

+60 transactions/s without scarifying security

(instead of Bitcoin 7 tps)

Blockchain Simulator
http://arthurgervais.github.io/Bitcoin-Simulation/index.html

Thank you!
# BITCOIN SIMULATOR

## IMPACT OF BLOCK GENERATION INTERVAL

<table>
<thead>
<tr>
<th>Interval</th>
<th>$t_{\text{mean}}$ (s)</th>
<th>$t_{\text{median}}$ (s)</th>
<th>$t_{10%}$ (s)</th>
<th>$t_{25%}$ (s)</th>
<th>$t_{75%}$ (s)</th>
<th>$t_{90%}$ (s)</th>
<th>$s_r$</th>
<th>Bandwidth (kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>25 mins</td>
<td>61.23</td>
<td>35.73</td>
<td>18.43</td>
<td>24.15</td>
<td>52.59</td>
<td>91.02</td>
<td>1.72%</td>
<td>14.14</td>
</tr>
<tr>
<td>10 mins</td>
<td>25.83</td>
<td>14.7</td>
<td>7.87</td>
<td>10.14</td>
<td>21.29</td>
<td>35.47</td>
<td>1.51%</td>
<td>14.26</td>
</tr>
<tr>
<td>2.5 mins</td>
<td>6.83</td>
<td>4.18</td>
<td>2.52</td>
<td>3.06</td>
<td>5.76</td>
<td>9.12</td>
<td>1.82%</td>
<td>14.51</td>
</tr>
<tr>
<td>1 mins</td>
<td>3.02</td>
<td>2.08</td>
<td>1.43</td>
<td>1.65</td>
<td>2.68</td>
<td>3.76</td>
<td>2.15%</td>
<td>14.71</td>
</tr>
<tr>
<td>30s</td>
<td>1.81</td>
<td>1.43</td>
<td>1.07</td>
<td>1.2</td>
<td>1.77</td>
<td>2.3</td>
<td>2.54%</td>
<td>15.39</td>
</tr>
<tr>
<td>20s</td>
<td>1.45</td>
<td>1.21</td>
<td>0.95</td>
<td>1.05</td>
<td>1.45</td>
<td>1.83</td>
<td>3.20%</td>
<td>16.12</td>
</tr>
<tr>
<td>10s</td>
<td>1.09</td>
<td>1</td>
<td>0.8</td>
<td>0.88</td>
<td>1.13</td>
<td>1.38</td>
<td>4.77%</td>
<td>17.67</td>
</tr>
<tr>
<td>5s</td>
<td>0.93</td>
<td>0.89</td>
<td>0.73</td>
<td>0.79</td>
<td>0.97</td>
<td>1.13</td>
<td>8.64%</td>
<td>21.03</td>
</tr>
<tr>
<td>2s</td>
<td>0.85</td>
<td>0.84</td>
<td>0.68</td>
<td>0.74</td>
<td>0.91</td>
<td>1</td>
<td>16.65%</td>
<td>31.44</td>
</tr>
<tr>
<td>1s</td>
<td>0.84</td>
<td>0.82</td>
<td>0.67</td>
<td>0.71</td>
<td>0.89</td>
<td>0.97</td>
<td>26.74%</td>
<td>49.83</td>
</tr>
</tbody>
</table>
# BITCOIN SIMULATOR

## IMPACT OF NUMBER OF MINERS

<table>
<thead>
<tr>
<th>Block Size (MB)</th>
<th>Block Interval</th>
<th>( s_r )</th>
<th>Throughput (tps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.25</td>
<td>30s</td>
<td>0.76</td>
<td>33.4</td>
</tr>
<tr>
<td>0.1</td>
<td>10s</td>
<td>1.76</td>
<td>40</td>
</tr>
<tr>
<td>0.25</td>
<td>20s</td>
<td>1.11</td>
<td>50</td>
</tr>
<tr>
<td>0.25</td>
<td>15s</td>
<td>1.45</td>
<td>66.7</td>
</tr>
<tr>
<td>0.5</td>
<td>30s</td>
<td>0.98</td>
<td>66.7</td>
</tr>
<tr>
<td>1</td>
<td>1mins</td>
<td>0.74</td>
<td>66.7</td>
</tr>
</tbody>
</table>
Decentralised PoW Blockchains

Proof of Work Blockchains

\[ B_0 \rightarrow B_2 \rightarrow B_3 \]

- \( H(B_2) \)
- txs
Decentralised PoW Blockchains

Proof of Work Blockchains

Mining
- Find Nonce N, s.t. $H(H(B_3) | \text{txs} | N) < \text{target}$