On the Security and Performance of Proof of Work Blockchains

Srdjan Čapkun

ETH Zurich
Decentralised PoW Blockchains

Bitcoin et al.

- Peer-to-peer decentralised currency
- Proof of Work (PoW)
- No trusted third parties (?)

- Blockchain: distributed DB
  - Transactions
  - Blocks
Decentralised PoW Blockchains

Blockchain

Block 1  Block 2  Block 3  Block 4
Blockchain

Mining

- Creates blocks
- Miner includes transactions (txs)
Decentralised PoW Blockchains

Blockchain and Transaction / Block Propagation

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

- Larger blocks => slower propagation => increased consensus latency

- Risks of network partition (stale blocks …)
Decentralised PoW Blockchains

Towards a better Blockchain

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

- **Faster payments**

- **Bigger block size**

- **More payments / slower propagation**

---

### Table: Blockchain Performance Comparison

<table>
<thead>
<tr>
<th></th>
<th>Bitcoin</th>
<th>Litecoin</th>
<th>Dogecoin</th>
<th>Ethereum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block interval</td>
<td>10 min</td>
<td>2.5 min</td>
<td>1 min</td>
<td>10-20 sec</td>
</tr>
<tr>
<td>Public nodes</td>
<td>6000</td>
<td>800</td>
<td>600</td>
<td>4000 [11]</td>
</tr>
<tr>
<td>Mining pools</td>
<td>16</td>
<td>12</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>$t_{MBP}$</td>
<td>8.7 s [8]</td>
<td>1.02 s</td>
<td>0.85 s</td>
<td>0.5 - 0.75 s [12]</td>
</tr>
<tr>
<td>$r_s$</td>
<td>0.41%</td>
<td>0.273%</td>
<td>0.619%</td>
<td>6.8%</td>
</tr>
<tr>
<td>$s_B$</td>
<td>534.8KB</td>
<td>6.11KB</td>
<td>8KB</td>
<td>1.5KB</td>
</tr>
</tbody>
</table>
Block 1 → Block 2 → Block 3 → Block 4

Block 3’ → Block 4’
Decentralised PoW Blockchains

Blockchain and Forks

Mining
- Creates blocks
- Blocks can conflict
Decentralised PoW Blockchains

Blockchain and Forks

Block 1
Block 2
Block 3
Block 4

Block 1''
Block 2''
Block 3''
Block 4''
Block 5''

Stale blocks = lost effort

- Bitcoin: 0.41%
- Litecoin: 0.273%
- Dogecoin: 0.619%
- Ethereum: 6.8%
What is Selfish Mining? [Eyal et al]

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

Other miners will perform wasteful computations

Adversary looses block rewards
What is Double Spending?

Spending money more than once

\[ TX_{\text{legitimate}} \] - Pays the vendor

\[ TX_{\text{doublespend}} \] - Pays the adversary
What is Double Spending?

Spending money more than once

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

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

Spending money more than once

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

Ok, I accept the payment
What is Double Spending?

Spending money more than once

\( TX_{\text{legitimate}} \) - Pays the vendor

\( TX_{\text{doublespend}} \) - Pays the adversary

Ok, I accept the payment
What is Double Spending?

Spending money more than once

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

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

Majority accepts $TX_{\text{doublespend}}$

Ok, I accept the payment

Goods/Service
What is Double Spending?

Spending money more than once

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

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

Ok, I accept the payment

Goods/Service

Majority accepts $TX_{\text{doublespend}}$

$TX_{\text{legitimate}}$ invalidated
Decentralised PoW Blockchains

Towards a better Blockchain

- Slower payments → Better security
- Faster payments → Less security
- Slower propagation → Faster block size
- Faster propagation → Smaller block size
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 provisions
Security Model

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

Security Parameters
- Adversarial mining power
- Block Propagation ability of the adversary
- Eclipse attack impact
- Mining costs
- Number of block confirmations
Selected Findings …

Due to the **smaller block rewards** and the **higher stale block rate** of Ethereum compared to Bitcoin (from 0.41% to 6.8% due to the faster confirmation time), Ethereum (block interval 10-20 seconds) needs at least **37 confirmations** to match Bitcoin security (block interval of 10 minutes on average) with **6 confirmations** against an adversary with 30% of the total mining power.

Similarly, Litecoin would require 28, and Dogecoin 47 block confirmations respectively to match the security of Bitcoin.
Selected Findings …

Setting the \textit{block size} to an average \textit{1 MB}, and decreasing the \textit{block interval time} to \textit{1 minute} do not considerably penalize security.

\Rightarrow \textit{PoW blockchains can attain an effective throughput above 60 transactions per second (tps)}

\Rightarrow \textit{the current throughput of Bitcoin of 7 tps can be substantially increased without compromising the security of the system.}
Selected Findings …

The objective of selfish mining is to increase the relative share of the adversarial blocks committed to the main chain (mining reward).

*As long as the difficulty of a PoW blockchain does not change, selfish mining yields fewer block rewards than honest mining.*

E.g., following an optimal selfish mining strategy an adversary with 30% of the mining power earns **209 block** rewards on average in a duration where 1000 blocks are mined by the whole network (*as opposed to 300* for honest mining). Similarly, Eyal and Sirer's [14] strategy yields on average 205.80 blocks rewards.
Selected Findings …

In double spending the adversary aims to maximize his absolute revenue (double spent transaction value).

One can show that the higher the block reward of a blockchain (in e.g., USD) the more resilient it is against double-spending (for a fixed transaction value).

i.e., for a given transaction value/reward, it is better to mine than to cheat

⇒ merchant can vary the # of confirmation blocks according to the transaction value
Summary

Selfish Mining vs. Double Spending

Analyse both independently

- 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)
References

Arthur Gervais, Ghassan Karame, Karl Wüst, Vasileios Glykantzis, H. Ritzdorf, S. Capkun
On the Security and Performance of Proof of Work Blockchains
Crypto ePrint, 2016

Arthur Gervais, Hubert Ritzdorf, Ghassan O. Karame, Srdjan Capkun
Tampering with the Delivery of Blocks and Transactions in Bitcoin
in Proceedings of ACM CCS, 2015

Ghassan O. Karame, Elli Androulaki, Marc Roeschlin, Arthur Gervais, Srdjan Capkun
Misbehavior in Bitcoin: A Study of Double-Spending and Accountability
ACM Transactions on Information and System Security (TISSEC), 2015

Arthur Gervais, Ghassan Karame, Damian Gruber, Srdjan Capkun
On the Privacy Provisions of Bloom Filters in Lightweight Bitcoin Clients
In Proceedings of ACSAC, 2014

Arthur Gervais, Ghassan O. Karame, Srdjan Capkun, Vedran Capkun
Is Bitcoin a Decentralized Currency?

Ghassan O. Karame, Elli Androulaki, Srdjan Capkun
Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin
In Proceedings of ACM CCS, 2012

Elli Androulaki, Ghassan O. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun
Evaluating User Privacy in Bitcoin
In Proceedings of FC 2013

http://www.syssec.ethz.ch/research/Bitcoin.html