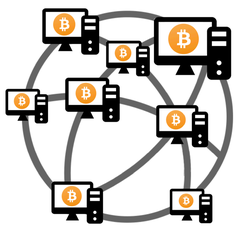
Calibrating the Performance and Security of Blockchains via Information Propagation Delays

Julius Fechner, Balakrishnan Chandrasekaran, Marc Makkes
Vrije Universiteit Amsterdam

Motivation



Blockchains rely on the underlying *(peer-to-peer) network*

Information propagation delays?

Speed at which new information disseminates across the network.

These delays have implications on the *performance* and *security* of blockchains

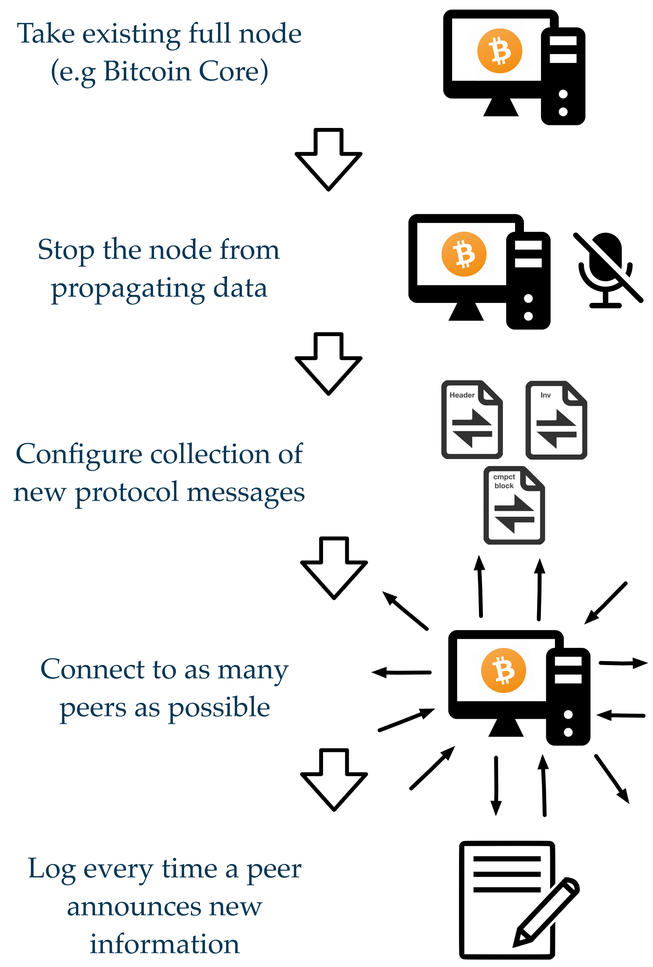
2013: Wattenhofer and Decker studied information propagation delays in Bitcoin.

After ~9 years of technological advancements, we revisit these delays in the following four blockchains.

Bitcoin Bitcoin Cash Litecoin Dogecoin

Methodology

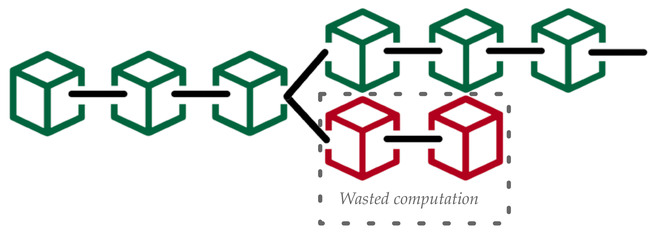
Reproducible, publicly available procedure



Implications of Delays

Delays in block propagation can cause *forks*.

Forks imply wasted work (i.e computations).



Forks decrease the *effective computational power* of the blockchain.

A decrease in the effective computational power increases the likelihood of an attack (on the chain).

Observed and worst-case fork rates

Blockchain	*# forks*	*Fork rate (%)*	*Worst-case (%)*
Bitcoin	1	0.015	0.576
Bitcoin Cash	1	0.014	0.106
Litecoin	8	0.032	0.417
Dogecoin	70	0.127	2.660

Low fork rates hint at low wastages of computational resources caused by delays.

Blockchain	*Effective comp. power* (%)	*Security threshold (%)*
Bitcoin	99.424	49.712
Bitcoin Cash	99.893	49.947
Litecoin	99.583	49.792
Dogecoin	97.325	48.663

Due to low computational wastage, the threshold an attacker requires remains close to the theoretical limit.

Network Footprint

Unique IP addresses observed, the number of autonomous systems (AS) they belong to, and the observed churn

Network	*Unique IP addrs.*	*Unique ASes*	*Churn (%)*
Bitcoin	8247	1435	53
Bitcoin Cash	503	118	14
Litecoin	3044	118	26
Dogecoin	14856	1568	68

Churn: The turnover rate of peers in the network. The percentage of peers that remained connected for < 75% of the observation period.

Blockchains with higher churns have delay distributions with longer tails.

Network Infrastructure

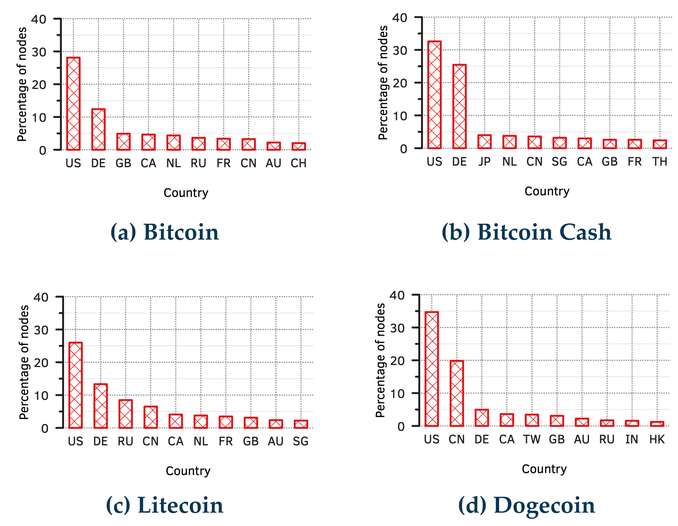
Percentages of peers hosted on cloud-provider networks

ASN	*Bitcoin*	*Bitcoin Cash*	*Litecoin*	*Dogecoin*
Amazon	7.70	17.89	8.08	0.78
Digital Ocean	3.30	9.94	3.58	0.23
Google	3.78	1.99	1.28	0.24
OVH	2.24	2.58	3.55	0.44

There are overlaps in the *digital hosting providers* used amongst the networks.

Around 30% of all nodes across the networks are hosted on cloud-provider networks.

This sharing of AS infrastructure introduces *common* points of failure across the networks.



(a) Bitcoin (b) Bitcoin Cash (c) Litecoin (d) Dogecoin

The top 10 countries that host nodes for each blockchain

Top 3 countries: United States, Germany, and China.

Geographic centrality may help reduce propagation delays.

Percentages of peers located in networks of state-owned Internet operators

Bitcoin	*Bitcoin Cash*	*Litecoin*	*Dogecoin*
5.17	1.19	10.25	23.88

Geographic centrality and reliance on *state-owned Internet operators* increases the risk of nation state attacks.

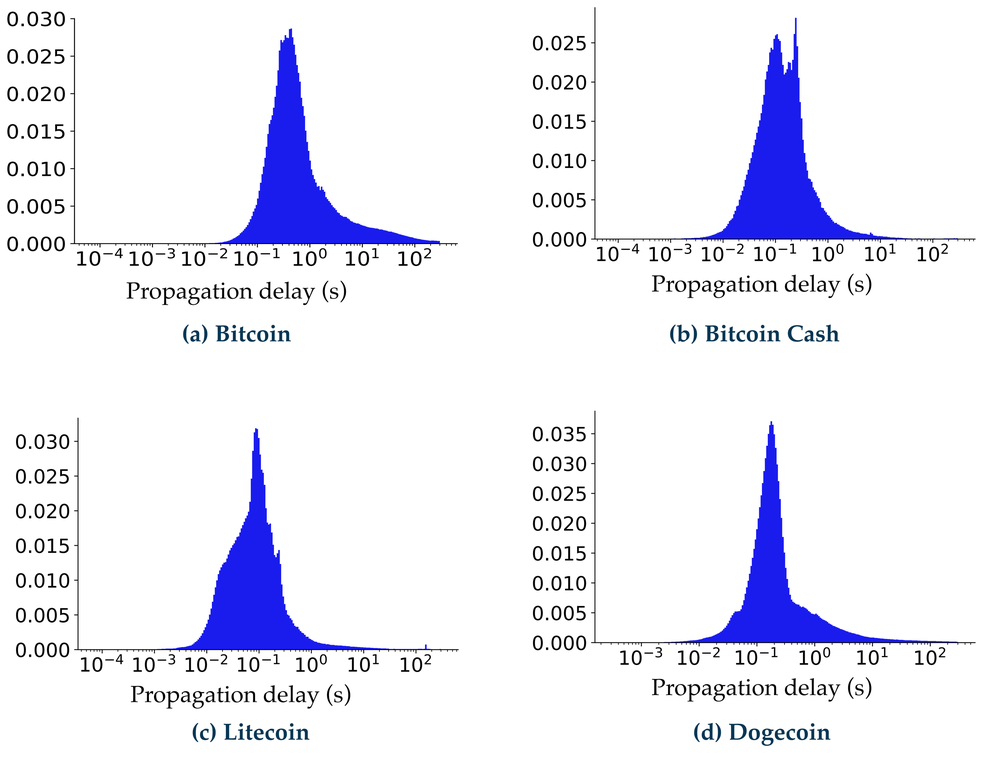
Large numbers of nodes may become affected by regulation changes.

May 2021: the average Bitcoin time-to-mine remains at ~600s.

Early June 2021: China bans mining across its provinces

Mid June 2021: Bitcoin time-to-mine rises to ~800s. A ~30% loss of hashing power across the network

What do we observe today?



(a) Bitcoin (b) Bitcoin Cash (c) Litecoin (d) Dogecoin

Normalised histograms of block propagation delays across the studied blockchains. The majority of peer announcements for a new block occured within one second, with Bitcoin and Dogecoin seeing larger tails to their distributions than Litecoin and Bitcoin Cash.

2013: Bitcoin delays were 6.5 seconds in the median and 12.6 seconds in the mean.

Current delays show a *14x reduction* in the median

Majority (> 75%) of nodes receive a block within *one second* of its first announcement.

Conclusion

- Information propagation delays of blockchains are low.
- Forks and wastages, hence, are rare.
- Potential infrastructure sharing across blockchains.
- Deployment concentrated in few countries, and also present in state owned networks.
- Are we sacrificing security for performance?
- Our tools are publicly available on Github.

github.com/JuliusAF/information-propagation-delays-2021

Reach me at: j.a.r.fechner@gmail.com