Cryptocurrencies and Decentralized Finance (Defi)

by Igor Makarov and Antoinette Schoar

Great paper!

Identifies important potential problems with Defi & offers relevant solutions

Public blockchains

No central authority

Who decides which transactions (blocks) should be appended to chain ?

$\Rightarrow$ Blockchain protocol designed to implement ``distributed democracy''

$\Rightarrow$ Validators randomly drawn + vote

Blokchain protocol => implements distributed random draw

Proof of Work (Nakamoto): PoW -> burns too much electricity ☹

Proof of Stake (Buterin): PoS

Proof of Stake

``every account has a certain chance per second of being selected, and this chance is proportional to the account's balance. The simplest formula is:

SHA256(prevhash + address + timestamp) <= 2^256 * stake / diff

Prevhash: hash of previous block,
address: address of miner,
timestamp: current Unix time in second,
stake: account of miner (corresponding to address)
diff: adjustable global difficulty parameter.''

Vitalik Buterin On Stake

This paper identifies important potential problems and offers solutions

1) Cryptos and blockchains can impede enforcement of taxes, AML and anti-terrorism

2) Defi supplied and maintained by validators and developers: If concentrated then rents

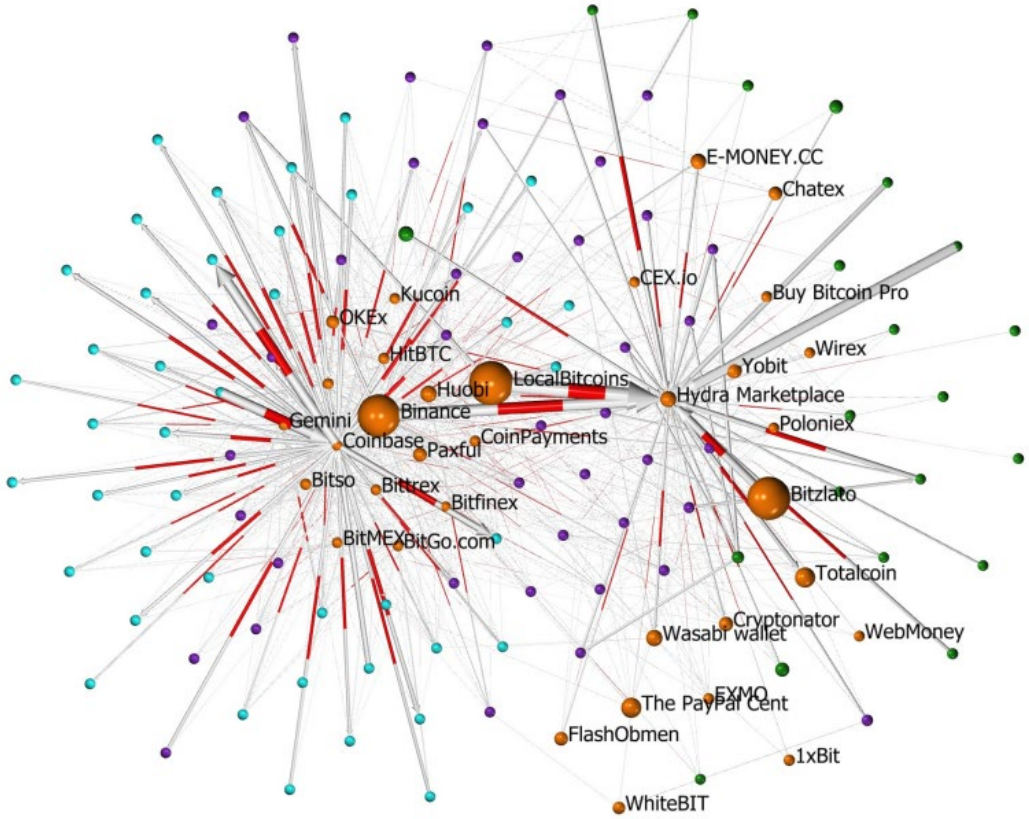
3) Miners/validators resist technology upgrade reducing returns on past investment

4) Decentralized governance runs into coordination problems

5) Regulate validators & developers, since key role in protocol

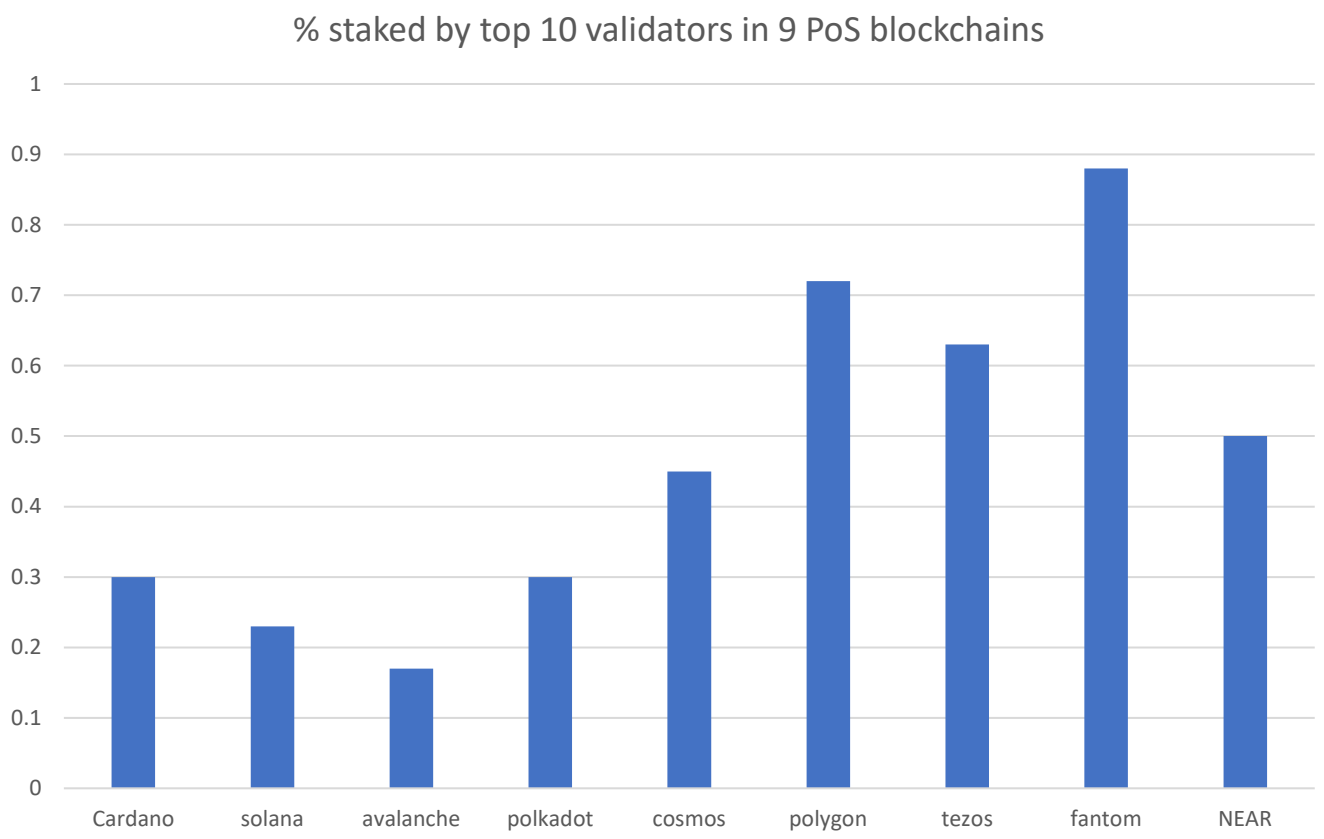
1) Defi can impede enforcement of taxes, AML & anti-terrorism

Large transaction volume between dark net (Hydra) and non KYC exchanges (binance)



Makarov and Schoar, 2022, ``Blockchain analysis of the bitcoin market''

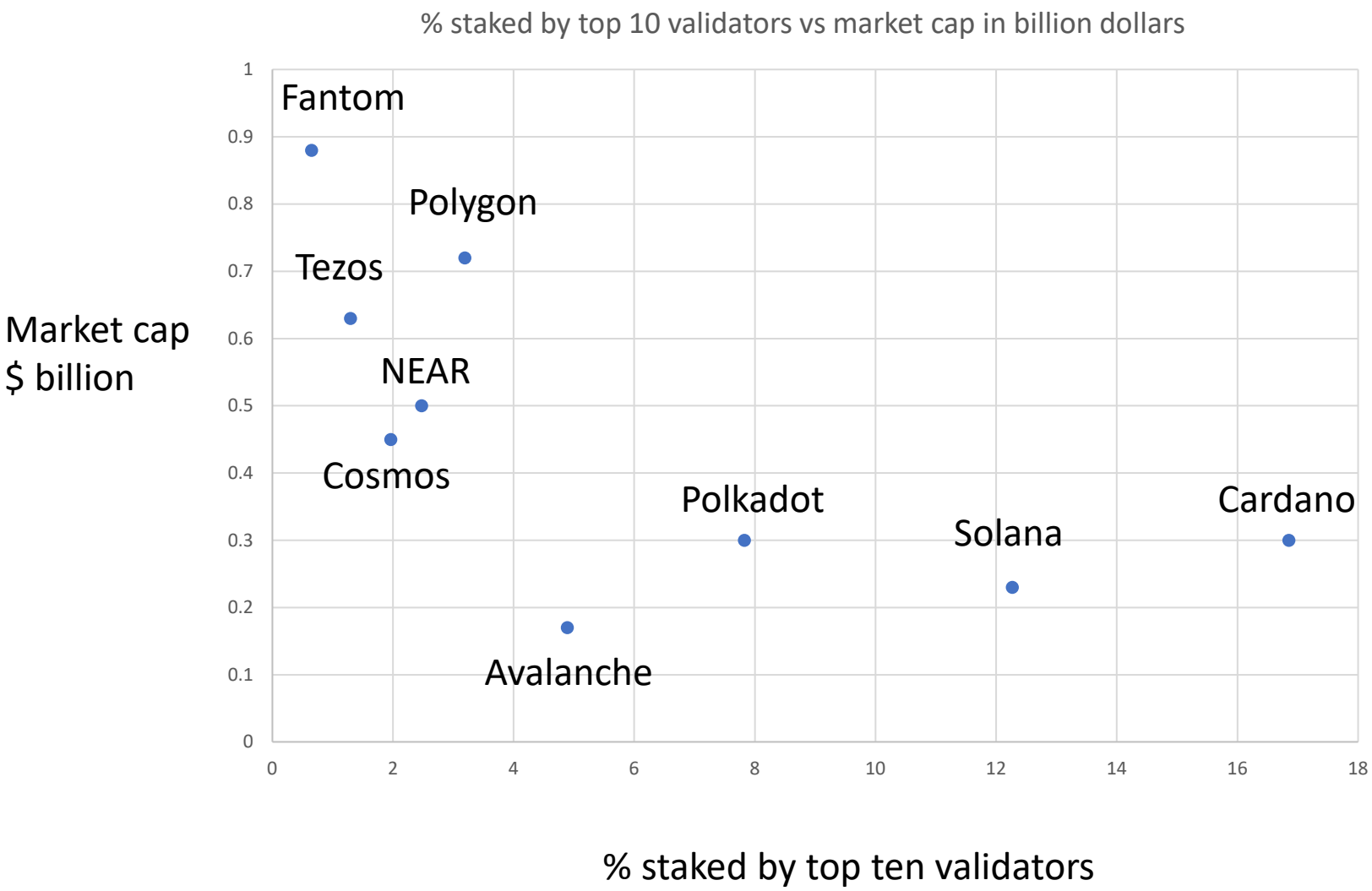
2) If validators concentrated then rents



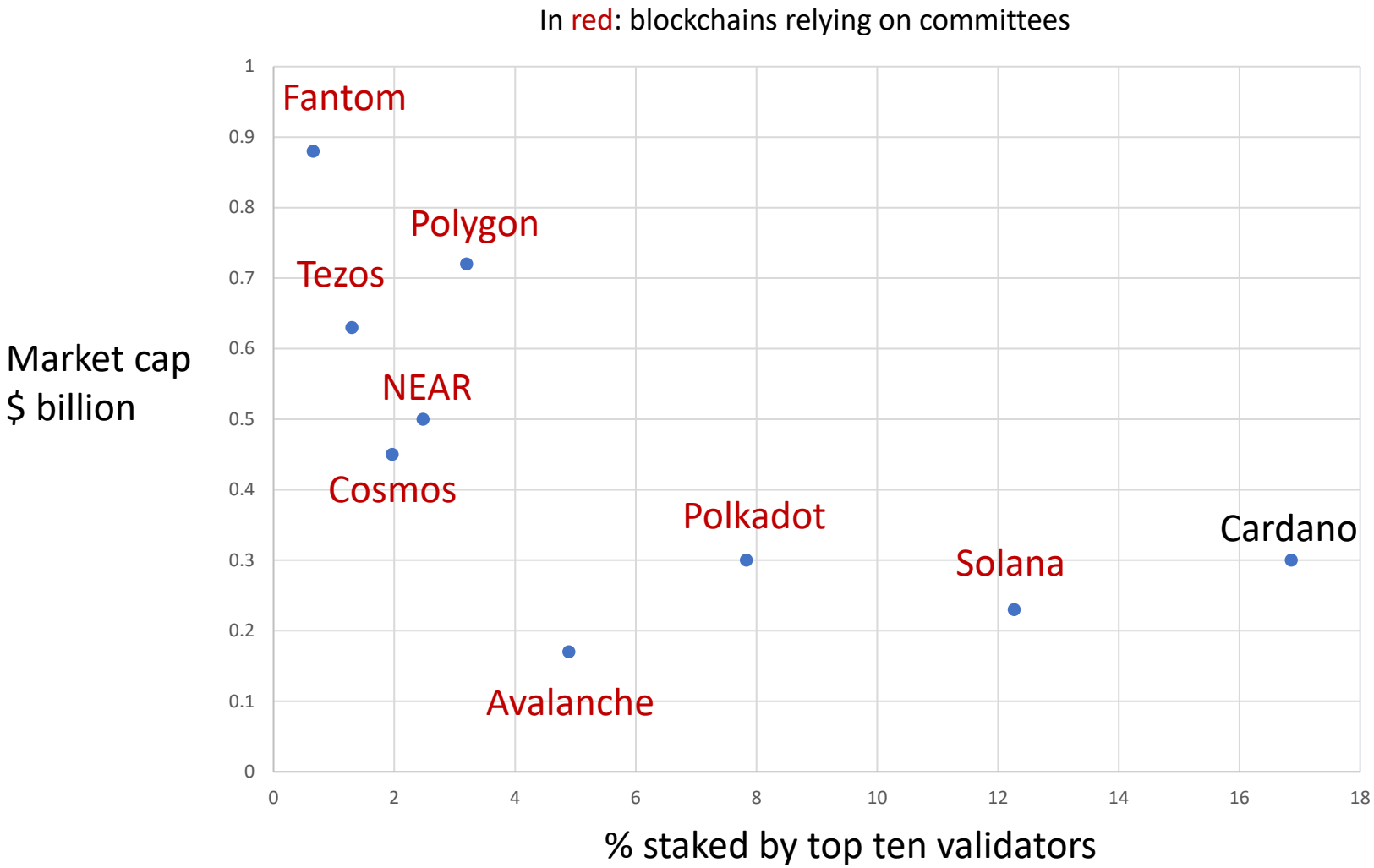
But threshold linear in stake => no increasing returns to scale

SHA256(prevhash + address + timestamp) <= 2^256 * stake / diff

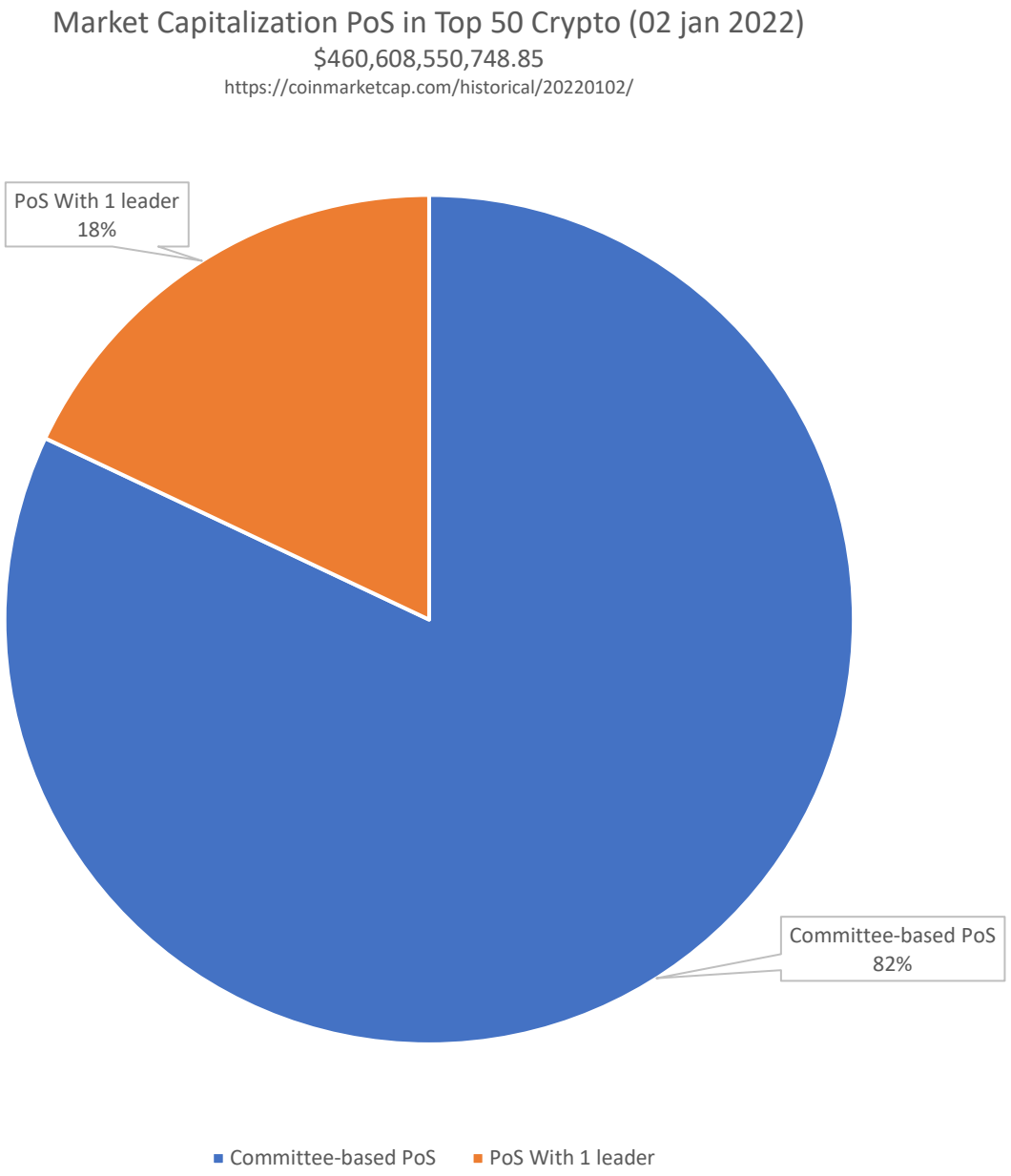
Large blockchains less concentrated



Proof of Stake blockchains often rely on committees: vote on blocks



Committee => no single validator can decide next block


Market Capitalization PoS in Top 50 Crypto (02 jan 2022)
$460,608,550,748.85
https://coinmarketcap.com/historical/20220102/
PoS With 1 leader
18%
Committee-based PoS
82%
Committee-based PoS
PoS With 1 leader

3) Resist technology upgrades reducing returns on past investment

Biais, Bisière, Bouvard & Casamatta (RFS 2019):

Game theoretical analysis of validators choosing to adopt technology upgrade or not (some validators can derive private benefit from old technology)

Even if upgrade more efficient there exist equilibria in which upgrade not adopted

Also equilibria in which only fraction of validators adopt upgrade, while others don’t (fork)

4) Decentralized governance runs into coordination problems

Amoussou-Guénou, Biais, Potop-Butucaru & Tucci (2021):

Game theoretical analysis of committee based blockchain protocol:

committee members (selected by PoS): check block validity + vote to append block iff valid

validity check = costly unobservable action

even when stakes can be slashed there exist equilibria in which invalid blocks appended:

each validator prefers to free ride and let others bear cost of validity check

5) Regulate validators & developers, since key role in protocol

Regulators can intervene off chain, harder to regulate on chain

China bans mining (farms with computers consuming electricity: on chain)

does not affect bitcoin price, nor mining: just moves elsewhere (Kazakhstan, Texas)

Natural solution: regulate centralized crypto exchanges (binance, coinbase,…)

receive funds, off chain, from investors setting up accounts

send funds, off chain, to investors selling crypto

KYC, transparency vis as vis regulators, police, and tax authorities

Conclusion

Great paper, insightful economic discussion of important current issues

Must read ☺