IN5420-Beyond the bitcoin.

SoK: Research Perspectives and Challenges for Bitcoin andCryptocurrencies

During init connection node attempts to establish 8 outgoing and 125 ingoing connections. How to get other nodes? Seed nodes- nodes that have addresses and after initial connection node can save a list of known addresses. How to communicate? Throught new coonection - connect and get from the neighbour a list of other nodes. Bitcoin nodes only relay transactions and blocks which satisfy stricter validation rules than what is permitted by the general transaction validity rules (refuse to relay more than a few thousand transactions below 0.001 per minute as a penny-flooding defense).

Stability: Canonical rules by Satsohi, but bugs can be fixed by users (case of 2013). De facto governance is required: bitcond devs, Bitcoin foundation, miners.

All miners follow their own economic incentives - incentive compatibility. We can consider compliant miners whose strategy is following the default mining rules. The original Bitcoin paper [90] models a
malicious miner trying to reverse a transaction by “trying to generate an alternate chain faster than the honest chain.” as a binomial random walk and shows that the attacker will eventually lose the “race” with the rest of the network.

Transition from block rewards to transaction fees.

Goldfinger Attack - 51 % destroy of the Bitcoin net. Feather-forking - blacklist block wit htransaction destroy the idea of uncensored crypto.

The attacking pool/miner joins the competitive pool. It calculates shares (to receive payouts) but hides the full blocks it finds. As a result: The attacker's costs remain low since hidden blocks do not increase the complexity of the network. The competing pool's income falls, making it less attractive to other miners.

Upgrading Bitcoin - Hard, soft forks. Relay policy updates. Some transactions may be valid but not transmitted over the network (for example, due to a filtering policy).

Merged mining.

ASIC-resistant miningpuzzles.

Network de-anonymization. Proposals for anonimity: Methods inside bitcoin (Coinjoin - few users combine their transactions in one, Coinshuffle, Mix and Blindcoin), alternative crypto (Zerocoin or Zerocash)

Majority is not Enough: Bitcoin Mining is Vulnerable

If an individual selfish miner mines within an honest pool, he does not benefit since the reward is divided proportionally to the hashrate. But if the pool itself uses selfish mining, it increases its profits by deceiving honest miners and the entire network. Bitcoin chain is no longer safe that 33%.
Than selfish mining pool is pushing his blocks in chain if chain the same it is a toss up (y param)

The γ parameter (the proportion of honest miners choosing the selfish chain in a conflict) greatly affects the effectiveness of the attack:

If γ = 1 (perfect selfish mining). Even one selfish miner can use the strategy.

If γ = 0 (honest miners always choose the public chain) .Attack threshold = 1/3 (33%) — only pools with a power greater than 33% can consistently earn more than honest miners.
If γ = 0.5 (realistic case). Attack threshold = 1/4 (25%) — if a selfish pool reaches 25% of the hashrate, it starts earning more than honest miners.

Selfish miners can manipulate γ by sybil atack (a lot of virtual miners that ignore the main chain). The solution: randomization of branch choice. This will make γ 25% and incerase threshold to 25%. This is great solution, cause of backword compatible, progressive improvement (more miners - harder to attack) and does not decrease the safety(Currently, chain selection is already random due to network latency, just a formalization)

System collaps - monopoly on bitcoin. Altruistic Agents that will decline selfish mining branch - not enough. Technically, it is almost impossible to detect and stop Selfish Mining. If someone in the pool is giving out its secret blocks, the administrator will quickly figure out the "traitor" and remove him.

On Scaling Decentralized Blockchains

Effective throughput - ho w many miners get block before mining the next one

Thorughtput limit - 4 MB, if more - decontentration of network.

Latency limit - 12 s,
The problem is latency, for example in 2015 then size of block was 540KB 10% of nodes - 0.8 sec, 90% - 79%. If we increase the block size to 1MB, 10 % - 1,5s and 90% - 2.4 MINUTES.

If block is less than 80KB - limited by latency. It is not possible to increase the block size indefinitely without taking into account the limitation on the speed of propagation.

Other, more difficult-to-measure metrics could also reveal scaling limitations. One example is fairness. (one block start to mine next block 2.4 minutes before)

Bottlenecks: Gossip protocol inefficiency (transaction appears twice, gossiping and in the block), no pipelining (only node to node). The main bottleneck is a netwrok structure and not computations.

Network plane - transport txs and blocks between nodes. Problems: local validation and double tx. Improvements - Set Reconciliation (ask about TX what you dont have), Relay(private) nterworks, imporvements in p2p topology, incentivization ofthe participants (send transaction is free, make a reward for this)

Consensus plane - if tx verified, security of blockchain. PoW - Ghost and Bitcoin-NG. BFT protocols faster, but need a set of trusted entities. Sharding and side chains.

Storage plane - ledger how to store blocks. Problems: full blockchain download and maintain, no opportunity to delete old. Improvements: Sharding, Distributed Hash Tables + Merkle Proof, SPV nodes and side chains for old data

View plane- get data. The state of blockhain. Outsourcing Computing with Cryptography (SNARKs)

Side plane - transactions outside the main blockchain network. Sidechains and payment networks