Notes on Cryptocurrency and Blockchain Protocols

Mahdi Zamani
Visa Research, Palo Alto, CA
mzamani@visa.com

The Flat Model [GKL15]. To model the hashing power of parties in a blockchain protocol, it is usually easier to assume all parties have the same quota of hashing power per round. The *non-flat model* where parties have different hashing powers can be easily captured by clustering the flat-model parties into larger virtual entities that are comprised by more than one flat-model party. For example, mining pools in Bitcoin can be thought of such aggregations of flat-model parties.

Common-Prefix Property [GKL15]. Let n be the total hashing power in the network and t be the total hashing power of the adversary. If $\frac{t}{n-t}$ is suitably bounded below 1, the blockchains maintained by honest nodes will have a large common prefix. More specifically, if an honest party removes k blocks from the end of its local chain, then the probability that the resulting chain will not be a prefix of another honest party's chain drops exponentially in the security parameter.

Chain-Quality Property [GKL15]. For any coalition of nodes (following any mining strategy), the fraction of blocks in the blockchain discovered by these nodes is exactly proportional to their collective hashing power. It is shown that the ratio of blocks in the chain of any honest node that are contributed by malicious nodes is bounded by $\frac{t}{n-t}$.

Chain Growth [?]. The number of blocks that are added to the blockchain during any given number of rounds.

Selfish Mining Attack [ES14]. A pool of parties keeps its discovered blocks private to intentionally fork the chain. When the public chain approaches the pool's private branch in length, the selfish miners reveal blocks from their private chain to the public in order to waste computational resources of honest miners. It is shown that the honest miners waste proportionally more than selfish miners. Therefore, the selfish pool's rewards exceed its share of the network's mining power, incentivizing rational miners to join the selfish mining pool.

Proof-of-Stake (PoS) [?]. The idea is to pick a node as the leader with a probability that is proportional to its stake in the system (i.e., the number of coins the node owns). Similar to a PoW-based consensus, the chosen leader gets to broadcast a block to the network. This process is called *minting* (rather than mining as in PoW-based consensus). PoS needs a secure coin flipping protocol to select an unpredictable leader randomly with respect to the distribution of stakes.

Bribery Attack. The attacker builds an alternative chain secretly based on the block prior to the one containing a transaction `T`. After `T` gains the necessary number of confirmations (e.g.,

six), and the attacker's chain becomes longer than the honest chain, the attacker publishes its chain. His chain will be accepted as the new valid blockchain, and as a result, T is reversed after being confirmed. Most PoS-based consensus protocols including [?, Mic16] are vulnerable to bribery attacks while such attacks are much harder in PoW-based consensus, because in the latter, bribed leaders have to solve new PoWs quickly (which is expensive) to reverse an already-confirmed transaction.

Coin vs Token. A coin is a unit of a digital currency that can be used like cash to transfer values and pay for goods and services. A token is a unit of shared computing resources such as bandwidth, computation, and storage. Since tokens are backed by hardware and/or Internet bandwidth, they are usually less vulnerable to speculative investment problems that most digital coins suffer from.

Sidechain [ABW14]. A sidechain is a blockchain that independently grows in parallel to a main blockchain (called a *mainchain*). A sidechain is usually accompanied by a sidechaining mechanism that allows tokens from the main chain to be securely used within the sidechain and vice versa.

References

[ABW14] Luke Dashjr Mark Friedenbach Gregory Maxwell Andrew Miller Andrew Poelstra Jorge Timon Adam Back, Matt Corallo and Pieter Wuille. Enabling blockchain innovations with pegged sidechains, 2014. https://www.blockstream.com/sidechains.pdf.

[ES14] Ittay Eyal and Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. In Nicolas Christin and Reihaneh Safavi-Naini, editors, *Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers*, pages 436–454, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[GKL15] Juan Garay, Aggelos Kiayias, and Nikos Leonardos. *The Bitcoin Backbone Protocol: Analysis and Applications*, pages 281–310. Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[Mic16] Silvio Micali. ALGORAND: the efficient and democratic ledger. *CoRR*, abs/1607.01341, 2016.