# 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 [KP16].** 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) [KRDO16].** 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 bribes some miners to not publish their blocks to the network so that the attacker can build an alternative chain secretly with their blocks and based on a 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 chain, and as a result, `T` is reversed after being confirmed. Most PoS-based consensus protocols including [KRDO16, Mic16] are vulnerable to bribery attacks while such attacks are much harder in PoW-based consensus, because in the latter, bribed miners have to solve new PoWs again and within a short amount of time to reverse an already-confirmed transaction.

**Coin vs Token.** A coin is a unit of a digital currency that can be used like a fiat money (e.g., US Dollar) to transfer values and pay for any goods and services. In contrast, a token is a *ticket* that grants access to a particular service or resource. Usually, a token can only be used to buy a specific shared computing resource such as bandwidth, computation, and storage. Since tokens are backed by some external resources/services, they are usually less vulnerable to speculative investment problems that most digital coins suffer from. A person who has a token is free to sell it for any price that the market is willing to buy. Since the total number of tokens is usually limited, the cost of the token typically increases as less tokens become available unless the resource/service behind the token loses its value (e.g., is no longer seen useful).

**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.

**Orphaned Block.** A valid block that is not part of the main chain. Such a block can occur naturally when two miners produce blocks at similar times or it can be caused by an attacker (with enough hashing power) attempting to reverse transactions. Those blocks that do not receive enough confirmations (e.g., at least six blocks on them) become orphaned.

**Stale Block.** A block which has already been mined so any solution to it will not be accepted as a new block by the network even if the solution is valid. The difference between an orphaned block and a stale block is that an orphaned block is initially accepted by the majority of the network, but is later replaced by another block if a longer chain (that does not contain the orphaned blocks) is detected.

**Uncle Block.**

**Nothing-at-Stake Attack.** Some protocols that rely their decisions on how much stake each participant has in the system are vulnerable to a situation, where malicious participants transfer their stake into someone else's account and therefore have nothing to lose if the system's security breaks. This happens because such protocols build their security based on the idea of giving higher priorities to participants with higher stake in the system.

## 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. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 281–310. Springer, 2015.

[KP16] Aggelos Kiayias and Giorgos Panagiotakos. On trees, chains and fast transactions in the blockchain. Cryptology ePrint Archive, Report 2016/545, 2016. https://eprint.iacr.org/2016/545.

[KRDO16] Aggelos Kiayias, Alexander Russell, Bernardo David, and Roman Oliynykov. Ouroboros: A provably secure proof-of-stake blockchain protocol. Cryptology ePrint Archive, Report 2016/889, 2016. http://eprint.iacr.org/2016/889.

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