Consensus

A blockchain consensus protocol ensures that all network participants agree on a growing chain of finalized blocks containing transactions, thereby providing consensus on a total order of these transactions. The Concordium Platform uses a proof of stake (PoS) mechanism to ensure resource-efficient operation of the network. It consists of two layers, combining a Nakamoto-style consensus (NSC) blockchain with a novel finalization method, providing fast finality.

Nakamoto-Style Proof-of-Stake Blockchain

The Concordium proof-of-stake mechanism is based on Ouroboros Praos [DGKR18]. Concordium has also undertaken research to improve the efficiency and security of NSC blockchains [KMM+21].

The parties producing blocks are called bakers. Time is divided into equally sized units called slots, where each slot corresponds to 0.25 seconds. In every slot, each baker locally evaluates a verifiable random function (VRF). If the obtained random value is below a pre-set threshold, the baker "wins" in that slot and extends the current longest chain by a fresh block. The threshold depends on the baker's relative stake and a common difficulty parameter. The parameters are set such that the winning probability is roughly proportional to the baker's relative stake and there is on average a block every 10 seconds.

The protocol is secure as long as honest bakers hold more than 50% of the stake of all bakers. The security has also been formally verified [TS21].

Finality Layer

Concordium's finality layer, Afgjort [DMMNT20], is running on top of the NSC blockchain. It dynamically "checkpoints" the blockchain by using Byzantine agreement to identify common blocks in the chains of honest nodes and then marks them as final. Final blocks are guaranteed to never be rolled back.

Finalization is run by a finalization committee whose members are called finalizers. The efficiency of the finalization depends on the total number of finalizers, which thus needs to be limited. The finalization committee consists of bakers holding at least 0.1% of all existing CCD, which ensures that there are at most 1000 finalizers in the committee and that all nodes with substantial stake can participate.

The finalization committee is continuously finalizing blocks. In each iteration, finalizers run a protocol to agree on a unique block at a given depth d (i.e., with distance d from the genesis block). Finalization for a given d roughly proceeds as follows. When a finalizer has a chain that has reached depth $d + 1$, it votes on the block it sees at depth d on its chain. If all finalizers vote for the same block, this block is declared final. Otherwise, the finalizers wait for their chains to grow and iteratively retry voting for the blocks at depth d on their new longest chains. Since parties agree on the prefix of their longest chains in NSC blockchains, this process is guaranteed to eventually succeed. In practice, it usually succeeds within the first try.

Concordium's finality layer has been proven secure as long as honest finalizers hold more than ⅔ of the total stake among all finalizers [DMMNT20].

Next-Generation Consensus: ConcordiumBFT

As part of an ongoing initiative to improve scalability, Concordium is currently implementing a new consensus protocol, called ConcordiumBFT, based on Jolteon [GKSSX22]. This should allow for even faster finalization and an improved throughput. ConcoridumBFT is expected to roll out in 2023.

The basic idea of the new protocol is as follows: A VRF-based PoS lottery produces a list of bakers, where those with more stake are proportionally more likely to be chosen more often. The next baker in the list then produces a block and the finalizers validate the block and sign it if it is valid. Once finalizers with more than ⅔ relative stake have signed a block, the next baker can build on that block and produce the next one. This allows new blocks to be created as soon as their parents are validated, without having to set a predetermined block time. Once two consecutive blocks are signed by finalizers with more than ⅔ relative stake, the first of the two is directly declared final. In case the current baker fails to produce a valid block that gets enough signatures, the finalizers sign a timeout message, which allows the next baker in the list to move on.

The new protocol has also been proven secure as long as honest finalizers hold more than ⅔ of the total stake among all finalizers [GKSSX22].

References

[DGKR18] David B., Gaži P., Kiayias A., Russell A. Ouroboros Praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. Advances in Cryptology – EUROCRYPT 2018. Lecture Notes in Computer Science, vol 10821. Springer, Cham, 2018. https://doi.org/10.1007/978-3-319-78375-8_3.

[DMMNT20] Dinsdale-Young, T., Magri, B., Matt, C., Nielsen, J.B., Tschudi, D. Afgjort: A partially synchronous finality layer for blockchains. Security and Cryptography for Networks (SCN) 2020. Lecture Notes in Computer Science, vol 12238. Springer, Cham. https://doi.org/10.1007/978-3-030-57990-6_2

[GKSSX22] Gelashvili, R., Kokoris-Kogias, L., Sonnino, A., Spiegelman, A., Xiang, Z. Jolteon and Ditto: Network-adaptive efficient consensus with asynchronous fallback. Financial Cryptography and Data Security (FC) 2022. Lecture Notes in Computer Science, vol 13411. Springer, Cham. https://doi.org/10.1007/978-3-031-18283-9_14

[KMM+21] Kamp, S.H., Magri, B., Matt, C., Nielsen, J.B., Thomsen, S.E., Tschudi, D. Weight-based Nakamoto-style blockchains. Progress in Cryptology – LATINCRYPT 2021. Lecture Notes in Computer Science, vol 12912. Springer, Cham. https://doi.org/10.1007/978-3-030-88238-9_15

[TS21] Thomsen, S. E. and Spitters, B. Formalizing Nakamoto-style proof of stake, IEEE Computer Security Foundations Symposium (CSF), 2021, pp. 1-15, https://dx.doi.org/10.1109/CSF51468.2021.00042