Consensus

The Concordium Platform uses a proof of stake (PoS) mechanism to ensure resource-efficient operation of the network. A major innovation of our consensus design is the two-layer consensus approach, which combines a Nakamoto-style consensus (NSC) blockchain with a novel finalization method, providing fast finality.

The rationale for this approach is that blocks can be quickly added using NSC, but for every block there is a risk that this block may be rolled back. This risk slowly decreases as subsequent blocks are added, but Concordium finalisation allows this risk to be eliminated shortly after the block is added to the chain. Thus, blocks can be added very efficiently using the NSC and the finality method ensures that blocks can quickly be declared as final.

Nakamoto-Style Proof-of-Stake Blockchain

While Concordium is currently undertaking research to improve the efficiency and security of NSC blockchains [KMM+20], the Concordium proof-of-stake mechanism is a simplified variation of Ouroboros Praos [DGKR18]. The simplification is made possible due to the Concordium finality layer, which prevents long-range attacks. 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 [TS20].

The party that participates in the production of blocks is called a baker. Time is divided into equally sized units called a slot. In every slot, each baker locally evaluates a verifiable random function (VRF). If the random value is below a pre-set threshold, we say that baker wins in the corresponding slot. The threshold depends on the party's relative stake and a common difficulty parameter f. The winning probability is roughly proportional to, and higher difficulty parameters decrease the winning probability for all parties. A winning party then extends the current longest chain by a fresh block.

Finality Layer

Concordium's finality layer can be added on top of NSC blockchains [DMMNT19]. The Concordium finality layer allows the dynamic 'checkpointing' of the blockchain by using Byzantine agreement to identify and then mark common blocks in the chains of honest users as final. Final blocks are guaranteed to never be rolled back. The security of the Concordium finality layer has been proven secure [DMMNT19]. To further ensure the reliability of Concordium formal verification methods are being investigated to prove the security of our finality layer [DSTT19].

Finalization is run by a finalization committee whose members are call finalizers. For finalization to work properly, honest finalizers need to hold more than ⅔ of the total stake among all 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 with at least 0.1% of the total stake, 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 using the Concordium CBFT consensus protocol. This protocol is designed such that it succeeds if all finalizers vote for the same block, otherwise it might fail. If the consensus protocol is successful, the block it outputs is defined to be final. If the consensus protocol fails, the finalizers iteratively retry until it succeeds. It has been proven that the protocol always succeeds eventually [DMMNT19], and in practice it usually succeeds within the first try. Moreover, the protocol provides a meaningful way of measuring the health of the chain by indexing how long it takes to finalize a block. This allows the consensus parameters to be adaptively optimized.

Security Guarantees

Overall, the two-layer approach provides the following guarantees:

- As long as corruption of the total stake is below ⅓, the finality layer declares blocks as final faster than the finality rule in a pure Nakamoto-style blockchain, which is required to wait for 'sufficiently many' blocks.
- When corruption is between ⅓ and ½, the Nakamoto-style blockchain can still be relied upon to obtain the same guarantees as a pure Nakamoto-style blockchain.

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.

[DMMNT19] Dinsdale-Young, T., Magri, B., Matt, C., Nielsen J., Tschudi, D. Afgjort: A partially synchronous finality layer for blockchains. SCN'20, 2020. https://eprint.iacr.org/2019/504.

[DSTT19] Dinsdale-Young, T., Spitters, B., Thomsen, S., Tschudi, D.: WIP: Formalizing the Concordium consensus protocol in Coq. CoqPL 2019. https://cs.au.dk/~sethomsen/coqpl19.pdf.

[KMM+20] Kamp, S., Magri, B., Matt, C., Nielsen, J., Thomsen, S., Tschudi, D.:
Leveraging weight functions for optimistic responsiveness in blockchains. IACR Cryptology ePrint Archive, Report 2020/328, 2020. https://eprint.iacr.org/2020/328.

[TS20] Thompson S. E., Spitters B.: Formalizing Nakamoto-Style Proof of Stake, 2020. ePrint.