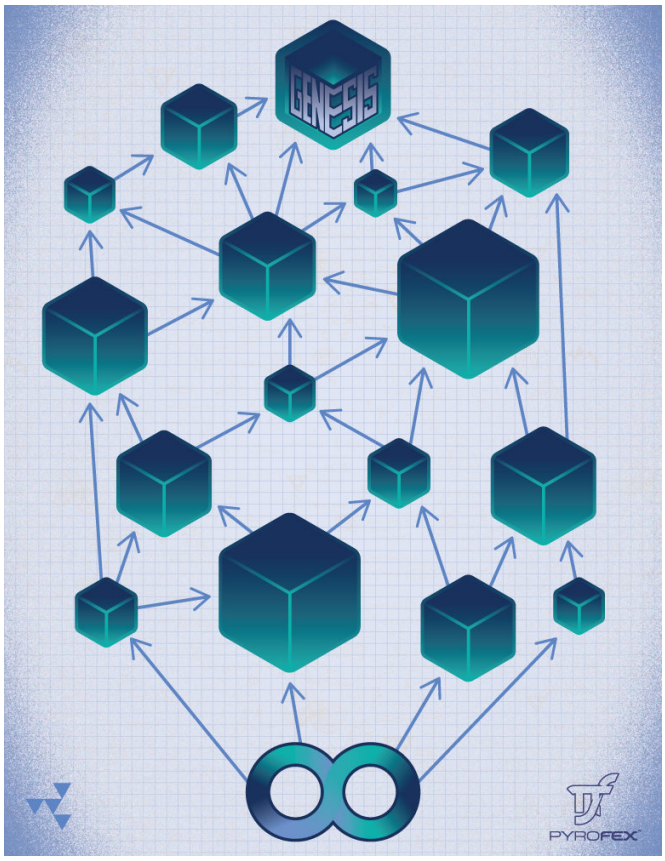
Casanova: A scalable consensus protocol for blockchain

19 December 2018, by Ingrid Fadelli



Casanova graph. Credit: Pyrofex Corporation.

A team of researchers at Pyrofex Corporation recently introduced Casanova, a leaderless optimistic consensus algorithm suited for use in a blockchain. Rather than producing a chain, Casanova produces blocks in a directed acyclic graph (DAG), which is essentially a directed graph with no cycles. Casanova pipelines voting rounds and block production to improve scalability and has a unique 'line item veto' for conflicting transactions such as double spends.

"We were looking for a scalable consensus algorithm that we could use to implement a couple of different blockchain projects we have going," the Pyrofex research team told TechXplore, via e-mail. "We initially thought Casper might be right and tried to prove it was safe and live under ideal network conditions. It didn't take long at all to show that wasn't the case and to conclude that we would have to make some significant changes. Our new algorithm addresses all the issues we were facing, but it required a lot of deviation from previous approaches."

Most existing blockchain technologies waste considerable time and resources getting the entire network to agree on the global ordering of each single transaction. While this might appear reasonable, the researchers feel that a good blockchain approach should be able to process transactions in any order.

"We should only use the energy and resources to come to consensus when it's necessary to do so—i.e., when there are two conflicting transactions and the network must choose exactly one," the researchers said. "Other blockchains have tried something similar, but with Casanova we were able to specify exactly how to accomplish this."

A notable characteristic of Casanova is that it does not build a blockchain per se, but rather builds a DAG. The researchers refer to the structure of Casanova as a 'blockdag'. If a blockchain's structure can be compared to a string, a blockdag resembles a piece of fabric with several strings woven together.

"Therefore, instead of confirming one block at a time, Casanova confirms one block at a time per member of the network," the researchers said. "So if the network has 1,000 members, we can confirm 1,000 blocks at once instead of just 1. We do all this work in the same time a regular blockchain would spend coming to consensus on a single block."

Casanova has validators instead of miners and these produce blocks on a regular basis, once every minute or so. When the validators receive a transaction from a client, they include it in their next block and sign the block to show that they have seen it.

Validators also exchange blocks with each other, to ensure that everyone sees all transactions. When a validator is ready to produce a new block, it includes information about blocks that it has seen from everyone else.

"The only worry is when two conflicting transactions arrive, like when a user tries to double spend," the researchers explained. "When validators see a conflict, they include information about it in their next block. Using the information from everyone's blocks, the network decides which transaction will be valid and which they'll throw away."

While it might feel like this process is not enough to guarantee security, the validators use mathematical structures to track both transactions and the other validators' votes. According to the researchers, this allows them to make important inferences, which ultimately ensure security.

"One of Casanova's more beautiful features is this: you can spam the network with double spends, which will slow it down, but the network will only slow down for the spammer's account," the Pyrofex research team said. "Everyone else's transactions get processed at the usual speed, because you can't force them to conflict with your transactions. Casanova has a sort of 'line item veto' on spammy transactions that's unique in the industry, as far as we know."

Although there are several blockdag algorithms out there, most of them are proof of work (PoW), while Casanova is proof of stake (PoS). In addition, most existing protocols try to give a total order in instances where a partial order would suffice.

"We're the first proof-of-stake blockdag consensus algorithm that we know of, and we keep transactions in a partial order," the researchers wrote. "We've also made some fundamentally new observations about how the members of a blockchain should record and track information."

The researchers are set to publish a new paper in which they will explain why their observations are more general, mathematically stronger and have a clearer meaning than those gathered using other blockchains or cryptocurrencies. A great advantage of Casanova is that it is quite general, making it easy for users to tailor the algorithm around their specific needs.

"The attestation observation is also important; it's one of the main reasons that we expect our consensus algorithm to be screaming fast," the researchers explained. "We designed a consensus algorithm to be fast, secure, and robust against network failures. Then, we built a transaction model for it that could be used to build a blockchain. This is why we think our technology will be faster and simpler than most technologies available today."

To broaden the scope of their study, the researchers are now working on implementing a proof of concept and formally verifying it in the proof assistant Agda. Developing Casanova allowed them to gather valuable insight into the existing pool of consensus literature, which they plan to write up and publish over the next few months.

"We have also developed a ledger model suitable for use with Casanova, which we're going to build into a blockchain in the near future," the researchers said. "We are working on a computation model that is suitable and will allow us to build a smart contracting blockchain. There's a lot to be done, including much of the proof-of-stake machinery like rewards, fees, bonding, unbonding, and so forth. It's going to be a busy year."

More information: Casanova. arXiv:1812.02232 [cs.CR]. arxiv.org/abs/1812.02232