Sei Giga, Under the Hood - Part 1: Consensus

Sei Giga will be the new exciting era for the Sei blockchain system.[1] Sei Giga will mark a major shift in how transactions are published, processed, and finalized in Sei. For this reason, Sei Labs commissioned Common Prefix to review the Sei Giga proposal and outline its findings in a series of blog posts.

In the first instalment we will focus on the Sei Giga's consensus.

Autobahn consensus

The heart of Sei Giga's consensus is the Autobahn protocol.[2] Autobahn is peer-reviewed[3] and offers state of the art performance and resilience. Therefore, Autobahn's security has been established in detail, with rigorous proofs that are independently verifiable.

Autobahn's main distinguishing feature, compared to past protocols, lies in the network assumptions under which it operates. So far, the literature predominantly used two network models: synchronous and partially synchronous. In the synchronous model, all messages are delivered to the recipient within some amount of time, which is known beforehand to the protocol's designers. On the other hand, in partially synchronous networks time is split in two periods: in the first period messages may be delayed arbitrarily; after a point in time - the Global Stabilization Time (GST) - the network behaves synchronously, that is with known bounded delays. Although these models are powerful tools when arguing about a protocol's security, they are not necessarily realistic reflections of deployed networks. In practice, network outages do happen, albeit infrequently and without a clean separation like the GST.

In such a realistic network, the primary goal of a protocol should be both to remain robust during short outages ("blips") and recover as swiftly as possible when they end, in order to avoid persistent performance degradations ("hangovers"). This useful property was formally defined for the first time in Autobahn and called "seamlessness". In essence, a seamless protocol avoids hangovers, that is *protocol-induced* performance degradations that last beyond a temporary network outage.

The Autobahn protocol's main achievement is achieving low latency and high throughput in a seamless manner. Essentially, Autobahn can process large amounts of transactions (throughput), which are finalized quickly (latency), and can recover immediately from hangovers. This optimality is achieved using the elegant idea of disentangling data dissemination from reaching consensus.

---

[1] https://www.sei.io
[2] https://arxiv.org/abs/2401.10369
[3] Autobahn was published and presented in the 30th Symposium on Operating Systems Principles.

In traditional systems, a chosen party ("leader") at any point in time organizes pending transactions in batches and disseminates them. Following, consensus is reached on each batch individually, resulting in a final agreed ordering of all batches. In blockchain-based systems, each "batch" is a block and leaders are often called different names, like "validators" (Ethereum), "bakers" (Tezos), or "stake pool operators" (Cardano). The drawback with this traditional approach is that when things go wrong, for example when a leader crashes or gets corrupted, then both the consensus process *and* the dissemination of transactions stall.

Autobahn decouples these two operations in a carefully designed manner. In Autobahn, transaction dissemination progresses at the pace of the network, that is the lowest rate between any two nodes, without being affected by possible consensus-related issues. Briefly, the design is based on two ideas.[4]

The first idea is that each protocol participant keeps their own chain of transaction blocks, which grow in parallel. This idea has been previously explored in the literature[5] and can increase throughput to its theoretical limits. Crucially though, Autobahn's consensus coordinates the commitment of these parallel chains in a way that communication complexity is linear to the number of participants, rather than the number of transactions. This enables the protocol to handle loads of transactions and scale as more nodes join the system, while significantly reducing the overhead of the critical consensus process.

The second design idea is that, if a node has not received some transactions that are proposed in a new batch, it does not wait to retrieve them before voting in consensus. Instead, as long as it is convinced that at least one honest party indeed has the data, meaning that the data is available somewhere in the network, the node participates in consensus while retrieving the missing transactions asynchronously. This is a novel idea of Autobahn that is missing from previous protocols and is crucial in reducing the latency of the consensus operation and ensuring seamlessness.

The thoughtful combination of these ideas enables Autobahn to be particularly fast when no network outage or party faults exist. Specifically, transactions are finalized in bounded time and latency is independent of the number of transactions, since communication complexity is linear only to the number of participants. This level of efficiency is on par with the state of the art Byzantine Fault Tolerant (BFT) protocols[6] and has enabled Sei Giga to process 5 Gigagas per second, when benchmarked in lab conditions using 40 validators.

---

[4] For a more detailed description of Autobahn, we refer to the mentioned paper and a detailed blog post by Sei: https://seiresearch.io/articles/autobahn-sei-giga-s-multi-proposer-approach-to-blockchain-consensus.
[5] For example see Prism (https://eprint.iacr.org/2018/992) and Parallel Chains (https://eprint.iacr.org/2018/1119).
[6] See Section 6 (evaluation) of the Autobahn paper.

What about blockchains?

Although Autobahn is a robust and provably secure consensus protocol, using it as the backbone of a real world permissionless distributed ledger can be tricky.

Autobahn, being a BFT protocol, operates in a setting where the participants are known. In other words, each node has an identity associated with it, namely a known public key used to sign and authenticate messages. However, blockchain-based distributed ledgers are traditionally *permissionless*, meaning that anyone can (or should be able to) join and leave the protocol at will. How this gap can be bridged is a standard concern in BFT-based distributed ledgers, but it is doable with a careful design. Without a centralized way to coordinate and approve participants, as is assumed in traditional BFT protocols, BFT-based blockchain systems often use the ledger itself for coordination.

In Sei Giga, no precise description exists yet on how the set of participants changes over time and across different epochs. It can be expected though that it will involve choosing the parties using some stake-based metric. For example, given a snapshot of the stake distribution at some point in time, the system could pick the top-X parties with most stake, or any party with stake above a certain threshold. Afterwards a handover process may be executed, where the previous set of participants is replaced by the newly chosen committee. Nonetheless, the devil lies in the details, so a detailed and precise specification of this process is of utmost importance to ensure that pitfalls are avoided.

Another point of interest concerns Autobahn's scalability. BFT protocols are typically very efficient but struggle to scale beyond tens or low hundreds of nodes. For example, the seminal PBFT protocol[7] can run over only a few tens of nodes before becoming essentially unusable, mostly due to bandwidth consumption due to its quadratic communication complexity. Follow-up protocols achieve significantly better performance, for example Bullshark[8] or mir-BFT[9] are able to realistically support 100-200 validators before bandwidth, batching, and storage become a bottleneck.

Autobahn has been stress-tested up to 20 nodes, in the original paper, and 40 nodes, by Sei. These tests operate under the assumption that all nodes are correct. However, when more nodes participate, it can be expected that leader failures become more frequent. The concern is that, in the bad case when the leader is faulty, communication complexity increases from linear to quadratic on the number of nodes, similar to traditional BFT protocols. Therefore, it will be interesting to explore how Autobahn performs in the presence of such faults.

The number of nodes on which Autobahn can run is important because it sets its fault tolerance. For example, if the protocol can run over 200 nodes, then it can tolerate failures of 66 among

---

[7] Practical Byzantine Fault Tolerance (PBFT) was published at the third Symposium on Operating Systems Design and Implementation (http://pmg.csail.mit.edu/papers/osdi99.pdf).
[8] Published at the 2022 ACM Conference on Computer and Communications Security (https://arxiv.org/abs/2201.05677).
[9] https://arxiv.org/abs/1906.05552

them. The more nodes it can handle, the more failures it can tolerate, hence the more robust it becomes. In essence, will Sei Giga be able to compete with the most widely used distributed ledger systems like Bitcoin, which supports over 20,000 nodes,[10] or Ethereum, which supports over 1 million validators across 10,000 nodes[11]? Will it be on par with competing Proof-of-Stake systems like Cardano, where more than 2,000 pools operate,[12] Tezos, which supports 250-300 “bakers”,[13] or Sui, with 100-120 validators[14]? Or will it be as decentralized as its current deployment (Sei v2), where among 40 total validators 7 control 33% of the total participating stake and 17 control 66%,[15] or systems like XRP (35 core validators)[16] and Stellar (23 Tier 1 validators)[17]? At this point, the answers to these questions are inconclusive, but it will be very exciting to find out.

Conclusion

In summary, Sei Giga is a very promising direction and is poised to be an interesting era for the Sei ecosystem. Autobahn, the consensus protocol at the heart of it, meets the highest academic standards of provable security and is on par with the state of the art in BFT protocols in terms of performance. However, the leap from a theoretical description to a production-level implementation is often trickier than expected. This is particularly the case when BFT protocols are used within permissionless distributed ledgers. Perhaps more interestingly, the fundamental promise of blockchain-based distributed ledgers is that of decentralization. To achieve this, the system needs to be able to support a large number of nodes, with power spread among them as evenly as possible. The extent to which Sei Giga can become decentralized remains to be seen, but it is definitely worth paying close attention.

---

[10] https://bitnodes.io
[11] https://beaconcha.in/charts/validators; https://ethernodes.org
[12] https://cexplorer.io/pool
[13] https://tzstats.com/bakers
[14] https://suivision.xyz/validators
[15] https://sei.explorers.guru/validators; https://www.seiscan.app/pacific-1/validators.
[16] https://xrpscan.com/validators
[17] https://stellarbeat.io/