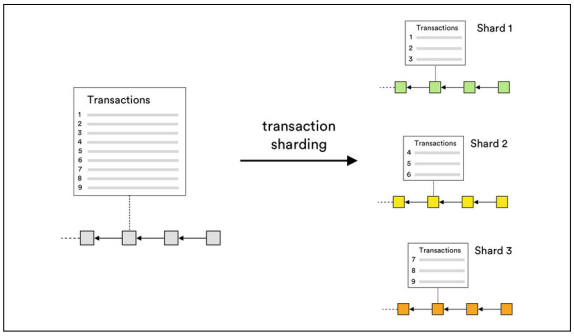
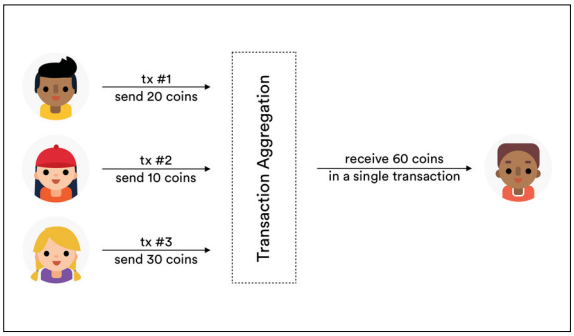
Roman
Blum

Student	Roman Blum
Examiner	Prof. Dr Thomas Bocek
Subject Area	Software and Systems

Scalability for the Bazo Blockchain with Sharding



With sharding, each node will process only a part of the data on the blockchain, and not the entire information.

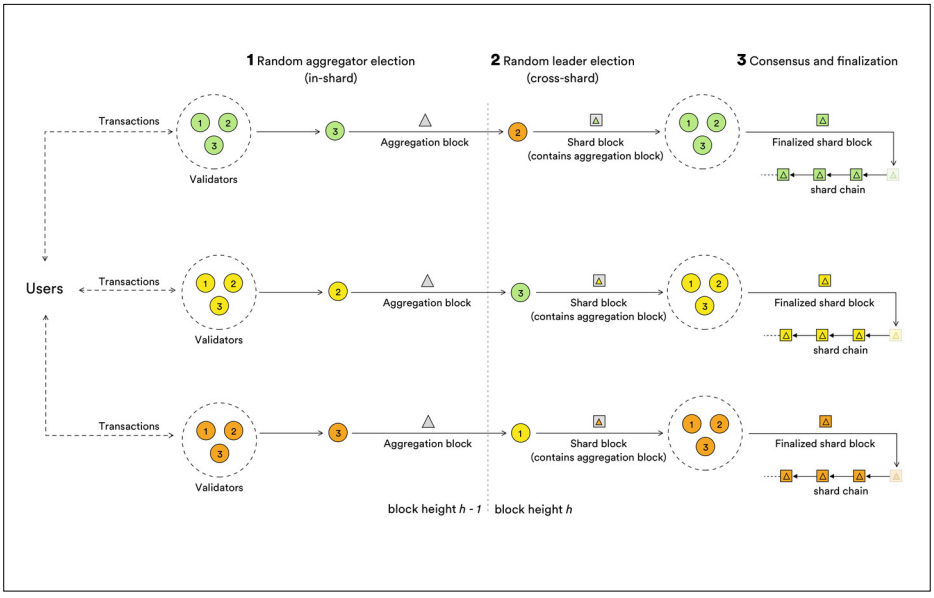


Multiple transactions are aggregated to a single one to reduce the overall size of the blockchain over time.

Introduction: The blockchain trilemma claims that distributed ledger systems are subject to an impossible trinity between decentralization, scalability, and security. Such systems can only achieve two out of these three properties to a highest degree. However, with the increasing popularity of cryptocurrencies and smart contract platforms, all three properties are required to its full extent in order to facilitate future adoption.

Solution: In this work, we present a sharding concept for the Bazo blockchain designed to scale as the number of users increases. With new users joining and using the network, the protocol load-balances the computational work by dynamically adjusting the number of partitions (shards). The core of Bazo's consensus protocol relies on self-contained proofs, a new primitive for blockchain protocols to prove that a user has sufficient funds without a validator relying on the full blockchain history.

We further propose a mechanism to reduce the overall size of the blockchain over time. The mechanism follows a transaction aggregation style using coalesced transactions and collectively signed state blocks. Within the realm of this new concept, we provide examples of in-shard and cross-shard transactions and briefly discuss mitigated attack scenarios to preserve the consistency and integrity of the Bazo blockchain.



An architecture overview highlighting the three important steps of the consensus protocol.