SplitChain

PrCLeSS
Proof-of-Concept

WIDE, Inria Rennes, IRISA, UR1
CIDRE, Inria Rennes, IRISA, UR1
GDD, LS2N, University of Nantes
IODE, University of Rennes 1

Initial Concept

SplitChain: Sharding in presence of an adaptive adversary

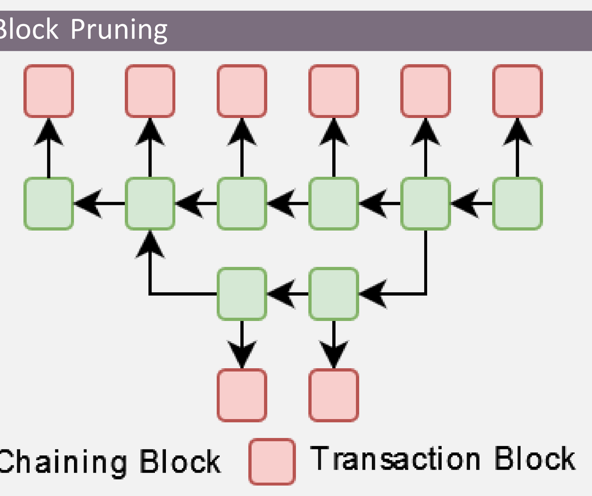
Introduction

Blockchains suffer from various technical issues, such as their inability to scale due to problematic communication costs and latency and a fairly low transaction throughput. We present SplitChain [2, 3], a protocol intended to support the creation of scalable account-based blockchains without undermining decentralization and security. This is achieved by using sharding , i.e. by splitting the blockchain into several lighter chains managed by their own disjoint sets of validators called shards. These shards balance the load by processing disjoint sets of transactions in parallel.

Contributions

- A distributed validator attribution mechanism.
- Chain merging and chain splitting protocols to automatically adapt the number of chains to the current payload of the system.
- A routing protocol allowing chains to efficiently redirect transactions and deliver messages.

Chain Structure and Block Pruning

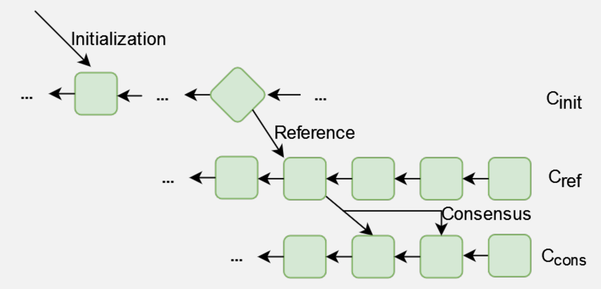


Most transactions inside a blockchain are independent from each other and do not need to be totally ordered inside a single chain of blocks. Instead, the storage of transactions and user accounts and the computation of new blocks are subdivided into multiple independent chains. Chains contain two types of blocks:

- Transaction blocks contain the actual transactions stored only inside the chain.
- Chaining blocks link the blocks of a chain together. They are only a few hundred bytes in size and are broadcasted through the entire system to provide synchronization data.

Periodically (e.g. 1000 blocks), a chaining block called cue block serves as a checkpoint. This allows to gradually prune the previous chaining blocks and transaction blocks.

Assigning Validators to Chains



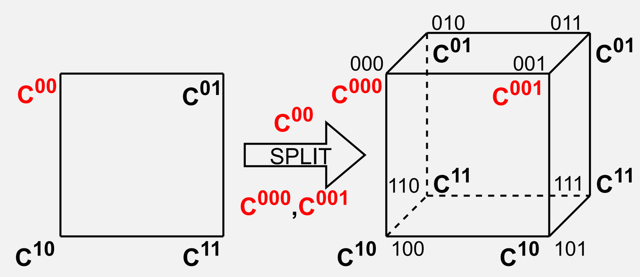
Partitioning the system into smaller chains reduces the amount of colluding validators required to corrupt them. To prevent the adaptive adversary from devising complex strategies to concentrate its manipulated validators in a targeted chain, the attribution of validators to a chain is a three-stage process that makes validator attribution unpredictable and ephemeral. Specifically, each chain of SplitChain has three roles in relation to validators: Initialization, reference and consensus.

- The initialization chain is the chain that processed the transaction creating the validator's account. The validator becomes active when the next cue block of the chain is created and a chain is randomly selected as its referencing chain.
- The referencing chain provides validators with a stable foothold in the network, and attributes them to their consensus chain. The referenced validators are distributed fairly among the different chains of the system using a pseudo-random attribution algorithm executed during each consensus execution. A Merkle root of the attribution of the validators is embedded to the newly created chaining block to serve as proof of their assignment.
- A validator can only participate to at most $T_A - 1$ consecutive consensus executions of its consensus chain. That is because the adversary is adaptive over a period T_A, i.e. it can target any validator in the system, which will be corrupted after a delay of T_A consensus executions. To ensure that validator credentials expire whether or not they participate in the consensus, only the credentials referenced by the latest chaining blocks of a chain are accepted for the consensus. Once its credentials have expired, a validator must issue a new request to its referencing chain with new credentials to obtain a new consensus chain.

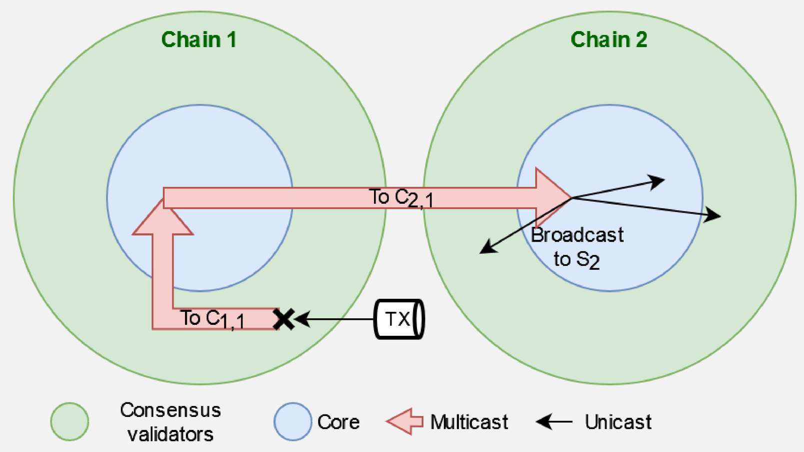
.

Hypercube Network Topology and Routing Protocol

All the chains of SplitChain are organized in a loosely hypercubic topology. A hypercube of dimension n (or n-cube) has 2^n vertices, each of which is connected to n neighbors and at a maximum distance of n edges of their furthest vertex of the n-cube. Each chain is a vertex of the hypercube.



Initially, SplitChain consists merely of an unique chain. When the number of transactions per block of the chain exceeds a certain threshold, the chain is replaced by two new chains called siblings. We call this operation a split. Similarly, if the number of transactions per block of a chain is too low, this chain will merge with its sibling.



A small subset of a chain's validators call core stores and maintains the routing tables used for intra-chain communication and message forwarding between the core validators of neighboring chains in the hypercube. Whenever a core validator receives a message, it either broadcasts it to the validators of its chain or forwards it to the core of one of its neighboring chains depending of the message's destination.

Conclusion

SplitChain supports the creation of scalable account-based blockchains without undermining decentralization and security. It distinguishes itself from other sharded blockchains by minimizing the synchronization constraints among shards while maintaining security guarantees. SplitChain is the first sharded blockchain that does not require a dedicated shard or a global blockchain to attribute validators to their consensus chain. This avoids the need for a global reconfiguration of the shards each time a new batch of validators is added to the system. A dedicated routing protocol enables transactions to be redirected between shards with a low number of hops and messages. Finally, SplitChain dynamically adapts the number of shards to the system load to avoid over-dimensioning issues.

Current Development

Recruitement

Three engineers actively working on the project since Spring 2024:

- Two engineer on original SplitChain Concept.
- One engineer on Blockchain-free SSI.

Splitchain Implementation

Human Resources

Olivier Deloubriere from June 2024 to May 2024 Patricio Inzaghi from July 2024 to June 2024

Achieved Milestones

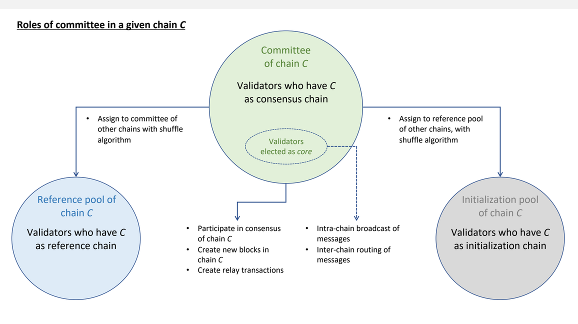
- Implementation of Consensus Algorithm
- Basic communication among nodes

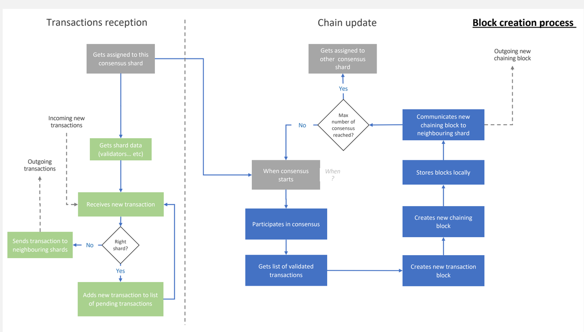
Upcoming Work

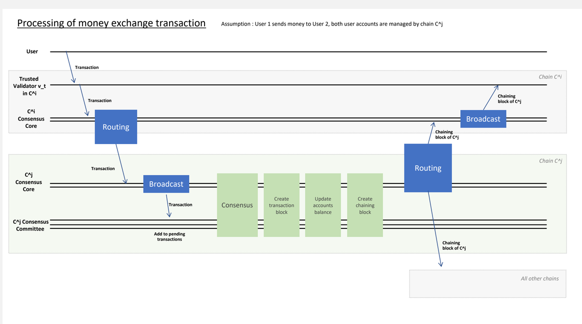
- Implementation of Attribution of Validator Roles
- Implementation of HyperCube and Routing Protocol for Intershard communication
- Implementation of Block-Creation Process
- Prototype implementation of complete system

Plan beyond the project

Original plan included additional months for experimentation. We will postpone this to a future PhD thesis/master internship.







Blockchain-Free Self-Sovereign Identity

From Theory to Practice

Leverage our work on Decentralized Identity, and Broadcast-Based Distributed Objects.

- Funded by SplitChain and H2020 overhead funds from SOTERIA project.

Our work [4] shows that the implementation of SSI solutions does not require global consensus. Similar to a sharded cryptocurrency system, an SSI platform can operate without a global synchronized ledger.

Human Resources

Elie Raspaud from April 2024 to March 2025.

Work done

- Analysis of the State of the art
- Report on the SSI systems in the PhD thesis of Mathieu Gestin
- High-level design of a blockchain-free SSI system.
- Implemtation of the first version of the CAC algorithm [1].
- Initial Experiments on the implementation.

Upcoming Tasks

- Optimization of CAC implementation.
- Prototype of Credential Management.
- Prototype of Consensus-Free Ledger.
- Prototype of Complete System

Plan beyond the project

Apply for further engineering funds (Inria ADT, or other short-term project).

References

[1] Timothé Albouy et al. Context Adaptive Cooperation. 2024. arXiv: 2311.08776 [cs.DC]. URL: https://arxiv.org/abs/2311.08776.
[2] Emmanuelle Anceaume, Davide Frey, and Arthur Rauch. "Sharding in Permissionless Systems in Presence of an Adaptive Adversary". In: SIROCCO 2024. Vietri sul Mare, Italy: Springer-Verlag, 2024, pp. 481–487. ISBN: 978-3-031-60602-1. DOI: 10.1007/978-3-031-60603-8_26. URL: https://doi.org/10.1007/978-3-031-60603-8_26.
[3] Emmanuelle Anceaume, Davide Frey, and Arthur Rauch. "Sharding in Permissionless Systems in Presence of an Adaptive Adversary". In: Networked Systems. Ed. by Armando Castañeda, Constantin Enea, and Nirupam Gupta. Cham: Springer Nature Switzerland, 2024, pp. 1–31. ISBN: 978-3-031-67321-4.
[4] Davide Frey, Mathieu Gestin, and Michel Raynal. "The Synchronization Power (Consensus Number) of Access-Control Objects: The Case of AllowList and DenyList". In: DISC 2023. Oct. 2023.

Workshop Organization

Blockchain & Privacy: International and Comparative Aspects

16 November 2023, University of the French Antilles - organized by Brunessen Bertrand et Sandrine Turgis

Goals:

- Gathering international experts on Blockchains & Privacy issues, with points of view on on the different legal regulations in the world.
- International and comparative aspects: not only the European point of view.
- The workshop took place the 16 November in Guadalupe and online with American, Canadian, Brazilian and African colleagues.