Team: All on Cloud 9

Aarti Jivrajani (aartijayesh@ucsb.edu), Abtin Bateni (abtinbateni@ucsb.edu), Daniel Shu (danielshu@ucsb.edu) Yiyang Xu (yiyangxu@ucsb.edu)

Problem

Distributed applications usually collaborate using Service Level Agreements(SLAs) to provide different services. Currently, there is no guarantee that both parties will make their promises and don't add fake facts to the blockchain. This makes the collaboration complicated and parties may act maliciously. As a result, it can defeat the whole purpose of the blockchain, to have a distributed ledger that acts as the source of **truth**. Moreover, if we enforce storing every single event in the main blockchain, not only we will waste a lot of our storage capacities but also may companies prefer not to expose their internal transactions.

Our Approach

We will implement a CAPER blockchain [1] to maintain the confidentiality of separate private blockchains while still maintaining good performance. This is done by maintaining application-specific views on each node instead of replicating the entire ledger. Each node will then only see their own transactions and any cross-application transactions that pertain to them. The ledger will be modeled as a DAG.

For reliability, the CAPER paper describes the consensus algorithms as black boxes, so to make our application scalable, we will use Bipartisan Paxos[2], which deals better with more nodes and increases throughput. This will be implemented in a way to make the consensus pluggable to easily switch between different algorithms. For our base case, we plan to have 3 nodes per application, and we will scale to 3 applications using the standard Paxos.

Testing

We will simulate node failures to test the fault tolerance of our system. Node failures can take the form of either causing crashes or implementing a malicious node(Byzantine failure). We can test the performance of our system by running it with different consensus algorithms and comparing the results.

We will also test resistance to tampering in response to node failure to honor the SLA.

Done Criteria

At least three applications will be able to communicate with each other and perform cross-application transactions without seeing each other's blockchain. All the intra-application nodes will be able to achieve consensus with each other. Each application will also still be able to function given one node failure.

References

[1] Mohammad Javad Amiri, Divyakant Agrawal, Amr El Abbadi. CAPER: A Cross-Application Permissioned Blockchain. PVLDB, 12(11): 1385-1398, 2019. DOI: https://doi.org/10.14778/3342263.3342275

[2] Michael Whittaker, Neil Giridharan, Adriana Szekeres, Joseph M. Hellerstein, Ion Stoica. Bipartisan Paxos: A Modular State Machine Replication Protocol https://arxiv.org/abs/2003.00331

https://mwhittaker.github.io/publications/bipartisan_paxos.pdf