Cross-Blockchain Transactions

Dongfang Zhao
University of Nevada, Reno
dzhao@unr.edu

1. MOTIVATION

Blockchains [1] offer an immutable, decentralized, and encrypted mechanism for transaction processing. Nonetheless, realized by its first widely-used application Bitcoin [2], blockchain was not originally designed for OLTP workloads; instead, it aimed to offer an autonomous and highly-secure data management service among untrusted parties, partly by sacrificing the transaction throughput performance. Recent research [3, 4] advocates to leverage blockchains for OLTP workloads by proposing various techniques (e.g., sharding, sidechains [5]) to boost up the transaction throughput of blockchains, such that blockchains would deliver similarly high performance as relational databases and become a competitive alternative to the latter as a general-purpose data management system.

There is yet another critical issue that must be addressed before blockchains can be widely adopted as a general data management system: the interoperability across blockchains. While SQL is available between different database vendors, no such standardization or interface exists for blockchains. Recent attempts (e.g., Cosmos [6]) on such cross-blockchain transactions are all *ad hoc*: making strong assumptions on the blockchains such as their consensus protocols and programming interface. In addition, existing cross-blockchain systems exhibit design limitations such as poor scalability and huge overhead.

2. PROPOSED APPROACH

We started with designing a multi-party transaction protocol across heterogeneous blockchains without a centralized broker. The most straightforward means to design multiparty protocols seems to be extending the sidechain protocol; however, it turns to be a challenging problem when the number of participants increases from two to an arbitrary n: we need to reapply the sidechain protocol for up to $\binom{n}{2} = n \cdot (n-1)$ times each of which takes 1-2 days—not a practical solution. To this end, we propose two techniques for efficient multi-party transactions:

10th Annual Conference on Innovative Data Systems Research (CIDR '20)
January 12-15, 2020, Amsterdam, Netherlands.

(I) Complementary Transaction. We will employ a passive principle for the multi-party transactions: instead of waiting for the branches, we simply mark concurrent branches valid and will trigger additional intra-blockchain transactions between branches to resolve the inconsistency right before short branches are invalidated.

(II) Parallelization of Subtransactions. We will parse the given multi-party transaction into a directed acyclic graph (DAG) where each vertex represents a series of operations over the same set of parties. We will then leverage multiple cores to parallelize the independent paths from the DAG.

At the writing of this paper, We have designed a distributed commit protocol among heterogeneous blockchains without a centralized component and implemented the protocol on a blockchain emulator called BlockLite [7]. We note that there are efforts on SQL wrappers over blockchains [8]. At this point, it is unclear whether a new standardization is needed and we leave this as an open question.

3. REFERENCES

[1] Kaiwen Zhang and Hans-Arno Jacobsen. Towards dependable, scalable, and pervasive distributed ledgers with blockchains. In *38th IEEE International Conference on Distributed Computing Systems (ICDCS)*, 2018.

[2] Bitcoin. https://bitcoin.org/bitcoin.pdf, Accessed 2018.

[3] Hung Dang, Tien Tuan Anh Dinh, Dumitrel Loghin, Ee-Chien Chang, Qian Lin, and Beng Chin Ooi. Towards scaling blockchain systems via sharding. In *International Conference on Management of Data (SIGMOD)*, pages 123–140, 2019.

[4] Jiaping Wang and Hao Wang. Monoxide: Scale out blockchains with asynchronous consensus zones. In *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, pages 95–112, 2019.

[5] Sidechains. https://blockstream.com/sidechains.pdf, Accessed 2019.

[6] Cosmos Network. https://cosmos.network, Accessed 2019.

[7] Xinying Wang, Abdullah Al-Mamun, Feng Yan, and Dongfang Zhao. Toward accurate and efficient emulation of public blockchains in the cloud. In *12nd International Conference on Cloud Computing (CLOUD)*, 2019.

[8] Johannes Gehrke et al. Veritas: Shared verifiable databases and tables in the cloud. In *Biennial Conference on Innovative Data Systems Research (CIDR)*, 2019.