Blockchain Protocols for Advancements in Throughput, Fault-Tolerance, and Scalability

Tech ID: 32570 / UC Case 2022-501-0

ABSTRACT

Researchers at the University of California, Davis have developed several blockchain paradigms that provide new approaches and expand on existing protocols to improve performance in large-scale blockchain implementations.

FULL DESCRIPTION

Blockchain is an increasingly popular technology for secure, federated databases due to the transparency and security it provides. Numerous parties validate transactions on a public ledger, creating a decentralized, consensus-based system; this approach is advantageous as it can function even if some users are inactive or have local errors. However, existing blockchain protocols have limitations of their own, especially at larger scales. For example, in primary-backup systems the total transaction throughput is limited by the bandwidth of the primary machine as it is the only one capable of providing new transactions before they are sent to the rest of the network. In other cases, the total network capability is not fully utilized since many operations cannot be effectively ran in parallel, so some machines sit idle waiting for other tasks to complete. There is also difficulty in scaling large databases since a copy of the entire ledger must be sent to every member of the network, which could add a delay with insufficient bandwidth. This problem is especially apparent when users are located in entirely different geographic regions. Since blockchain technology is becoming more sophisticated, it is important to meet these challenges with new protocols that are future-proof and scalable for growing needs. Researchers at the University of California Davis have developed a series of new protocols to address such limitations and improve the performance, reliability, and security of blockchain technologies. There are three distinct advancements, each solving a unique challenge of modern blockchain implementations.

2022-503 RCC: Resilient Concurrent Consensus - In the RCC paradigm, replica machines can independently provide transactions without the single replica bandwidth bottleneck of primary-backup systems. Transaction throughput is improved by running many consensus instances concurrently to use the entire network as efficiently as possible. Through RCC, existing primary-backup systems can easily transition into a concurrent consensus structure. Furthermore, RCC is more reliable as it reduces the coordination dependency between systems. This structure is fault resilient and provides up to a 2.75x performance improvement to transaction throughput.

2022-502 ByShard - ByShard is capable of implementing shard protocols in a Byzantine environment. Blockchain Shards make scaling to large datasets possible by splitting data into smaller partitions that are shared between centrally located clusters – for instance, users in the same geographical region may operate on the same partition. It reduces overhead by allowing individual nodes to process and transmit manageable sizes of data, and improves total throughput by processing shard transactions in parallel. This versatile technology includes 18 novel protocols, each with their own trade-offs between throughput, isolation level, latency, and abort rate.

2022-501 Ring Byzantine Fault Tolerance – Existing shard protocols are efficient when working within a single cluster, but have severe performance penalties when accessing data from other nodes. RingBFT manages conflicts and resolves deadlocks by requiring cross-shard transactions to occur in a linear ring order, offering significant performance improvements. The ring method of processing, forwarding, and re-transmitting information to neighboring nodes improves throughput by up to 25x, and can be scaled up to 500 nodes.

2022-513 Power-of-Collaboration (PoC) Hybrid Protocol - PoC is a hybrid protocol that leverages elements from BFT (Byzantine Fault-tolerant Protocol), PoS (Proof-of-Stake), and PoW (Proof-of-Work) protocols. PoC aims to leverage the resiliency and reconfigurability of PoW, utilizing the PoS-like penalty model, and the democratic and voting model of BFT. The PoC protocol utilizes the power of BFT protocol to substantially reduce the energy consumption needed to solve PoW computational puzzles without weakening its resiliency promise. Furthermore, by incorporating PoS, a new fair economical model is developed such that it only penalizes misbehavior while providing consistent fair rewards to all participating miners

APPLICATIONS

- Integration and coordination of large-scale Blockchain processes

FEATURES/BENEFITS

- Improved performance in transaction throughput and network efficiency
- Maintains desired security functionality of existing blockchain protocols

CONTACT

Michael M. Mueller
mmmueller@ucdavis.edu
tel: .

INVENTORS

- Gupta, Suyash
- Rahnama, Sajjad
- Sadoghi, Mohammad

OTHER INFORMATION

KEYWORDS

blockchain, blockchain protocols, byzantine fault tolerance, shard, transaction

CATEGORIZED AS

- **Computer**
  - Other
  - Security
  - Software
- **Security and Defense**
  - Other

RELATED CASES

2022-501-0

- Protocols are fault tolerant and improve system reliability
- Efficient scaling for large databases with many machines

PATENT STATUS

Country	Type	Number	Dated	Case
United States Of America	Published Application	20230019637	01/19/2023	2022-501

Additional Patent Pending

University of California, Davis
Technology Transfer Office
1850 Research Park Drive, Suite 100, ,
Davis,CA 95618

Tel: 530.754.8649
techtransfer@ucdavis.edu
https://research.ucdavis.edu/technology-transfer/
Fax: 530.754.7620