In enterprise business applications, large volumes of data are generated daily, encoding business logics and transactions. Those applications are governed by various compliance requirements, making it essential to provide audit logs to store, track, and attribute data changes. In traditional audit log systems, logs are collected and stored in a centralized medium, making them prone to various forms of attacks and manipulations, including physical access and remote vulnerability exploitation attacks, and eventually allowing for unauthorized data modification, threatening the guarantees of audit logs. Moreover, such systems, and given their centralized nature, are characterized by a single point of failure. To harden the security of audit logs in enterprise business applications, in this work we explore the design space of blockchain-driven secure and transparent audit logs. We highlight the possibility of ensuring stronger security and functional properties by a generic blockchain system for audit logs, realize this generic design through BlockAudit, which addresses both security and functional requirements, optimize BlockAudit through multi-layered design in BlockTrail, and explore the design space further by assessing the functional and security properties the consensus algorithms through comprehensive evaluations.

The first component of this work is BlockAudit, a design blueprint that enumerates structural, functional, and security requirements for blockchain-based audit logs. BlockAudit uses a consensus-driven approach to replicate audit logs across multiple application peers to prevent the single-point-of-failure. BlockAudit also uses the Practical Byzantine Fault Tolerance (PBFT) protocol to achieve consensus over the state of the audit log data. We evaluate the performance of BlockAudit using event-driven simulations, abstracted from IBM Hyperledger.

Through the performance evaluation of BlockAudit, we pinpoint a need for high scalability and high throughput. We achieve those requirements by exploring various design optimizations to the flat structure of BlockAudit inspired by real-world application characteristics. Namely, enterprise business applications often operate across non-overlapping geographical hierarchies including cities, counties, states, and federations. Leveraging that, we applied a similar transformation to BlockAudit to fragment the flat blockchain system into layers of codependent hierarchies, capable of processing transactions in parallel. Our hierarchical design, called BlockTrail, reduced the storage and search complexity for blockchains substantially while increasing the throughput and scalability of the system. We prototyped BlockTrail on a custom-built blockchain simulator and analyzed its performance under varying transaction and network sizes demonstrating its advantages over BlockAudit.

A recurring limitation in both BlockAudit and BlockTrail is the use of the PBFT consensus protocol, which has high complexity and low scalability features. Moreover, the performance of our proposed designs was only evaluated in computer simulations, which sidestepped the complexities of the real-world blockchain system. To address those shortcomings, we created a generic cloud-based blockchain testbed capable of executing five well-known consensus algorithms including Proof-of-Work, Proof-of-Stake, Proof-of-Elapsed Time, Clique, and PBFT. For each consensus protocol, we instrumented our auditing system with various benchmarks to measure the latency, throughput, and scalability, highlighting the trade-off between the different protocols.
Committee in Charge:
Aziz Mohaisen, Chair, Computer Science
Amro Awad, Computer Science
Wei Zhang, Computer Science
Clay Posey, Management

Approved for distribution by Aziz Mohaisen, Committee Chair, on October 11, 2019.

The public is welcome to attend.