A Distributed System Approach to Responsive and Secure Decentralized Applications

Overview. Decentralized applications (DApps) are showing great promise in breaking down information silos and promoting transparency and equitable access to web applications that are traditionally hosted in a centralized cloud system. For example, the finance and healthcare industries have been invested in blockchain-enabled DApps for transaction processing and secure data sharing with minimum trusted third parties. However, the current DApp operational model, spanning from front-end app browsers to back-end blockchain databases, faces scalability challenges that hinder its extension to more expansive application scenarios, particularly the mobile scenes, where traditional applications are still dominant. Besides performance, DApp operations are further complicated by privacy laws which however the existing paradigm cannot accommodate efficiently. In the face of these challenges, this project aims to develop a new distributed system approach that extends DApps to their full potential—achieving the same level of performance as with their cloud-based incumbents while achieving better security in the decentralized, low-trust scenes.

Intellectual Merit. The research plan and intellectual merit manifest in four thrusts:

- Thrust I: An Extensible DApp Operating System with Responsive End-to-end Consensus Utilities. This thrust aims to develop a new DApp-hosting operating system that can be instantiated in mobile/resource-constrained devices. This new operating system paradigm harbors two transformative designs: (i) supporting highly efficient *ad hoc* consensus operations directly between DApp user devices and (ii) new message-light transport-layer consensus utilities. This approach is designed to relieve the global blockchain consensus from complex computation and thus help DApps achieve better throughput and delay performance.
- Thrust II: Data-driven Consensus Protocol Optimization in Dynamic Networks. To accommodate the dynamic networking delays and varying computing capability among the mobile DApp users, this thrust aims to develop a reinforcement-learning (RL) approach that allows the users to adapt to the optimal consensus setup during runtime. This approach will allow the ad hoc consensus operation to maximally take advantage of the available network bandwidth and local computation capability. It is of independent interest to the fundamental research on consensus protocol optimization in blockchain and P2P networks.
- Thrust III: Confidential Yet Verifiable DApp Execution with System-cryptographic Co-design. This thrust aims to provide security and privacy features essential to the DApps that operate and produce sensitive data in an externally verifiable manner. The key technique is to leverage secure multiparty computation (MPC) to substitute originally consensus-based operation and zero-knowledge proofs (ZKPs) to produce execution proofs in a distributed manner. These two functions will be customized to resource-constrained mobile devices with novel hardware-assisted cryptographic designs.
- Thrust IV: Experiments and Evaluation. We will implement the protocols and system prototypes and evaluate them through performance benchmarking, simulation, and public-domain verification. This thrust will bring artifacts and insights into instrumenting a new operating system for the DApp research community.
- Education Plan. Each research thrust will be integrated with layered educational modules catered to students at different levels, from K-12 to college students and the general public. The plan also features an annual DApp development competition open to participants from the University and the local region.

Broader Impacts. This project will extend our theoretical know-how in designing reliable distributed systems and decentralized applications in challenging mobile scenarios, such as IoT, healthcare, and sensor networks. Undergrad and graduate students involved in this project will receive training on distributed systems and networking, trusted computing, system security, privacy, and software-hardware integration. The project will also be in line with the broader impact goal of NSF to provide research training and mentoring to undergraduate and underrepresented students. The research outcome, including tutorials, software packages, and publications will be made available online to the public.

Keywords: Decentralized Application; Distributed System; Security and Privacy