Project Summary

Overview. Emerging decentralized applications (DApps) rely on independent oracle services to communicate with the real world and acquire operation-critical data. A host of challenges arises with the existing oracle services for DApps in the mobile and IoT scenarios: no effective mechanisms to ensure the trustworthiness of the procured data; not supporting diversified information sources to overcome potential bias and manipulation; inability to supply rich data types to fulfill a wide range of DApp-specific data requests. To address these challenges, we propose to develop the AROMA system—Adaptive Robust Oracle for Mobile Decentralized Applications in this project. The AROMA design is inspired by the recent advances in decentralized systems, consensus mechanisms, secure hardware, and privacy-preserving technology. This project will develop the AROMA system suite including the Middleware, Server, and public interfaces to accomplish the following objectives: 1) truthful data provision: a customer DApp can obtain trustworthy operation-critical data feeds from sources locally accessible to the distributed DApp participants; 2) adaptive oracle service optimization for elevated data accuracy, system performance, and user experience in a dynamic mobile environment; 3) resilient architectural design against adversarial influence; 4) participant privacy.

Intellectual Merit. This proposal aims to fully develop AROMA and advance the knowledge of building oracle systems for challenging scenarios. The key research tasks manifest in four thrusts:

• Thrust I: Decentralized Consensus-driven Truth Discovery for Trustworthy Data Feed. This thrust aims to develop the AROMA Middleware and the DCTD mechanism to realize the system's main purpose. It is a new oracle solution to procuring required external data to a mobile DApp from distributed data sources. DCTD makes novel use of truth discovery and a fault-tolerant consensus to allow each DCTD participant to obtain custom-defined data feeds in an efficient, accurate, and fully decentralized manner. The design of DCTD will also generate valuable experience in application-consensus co-design in mobile platforms.

• Thrust II: Learning-aided Consensus Protocol Optimization in Dynamic Environments. To attain a low DCTD latency amid the dynamic networking conditions and high churn rate among the DCTD participants, this thrust aims to develop a reinforcement-learning (RL) approach that can help the system adapt to the optimal consensus protocol setup during runtime. This approach is of independent interest to the fundamental research on consensus protocol optimization in blockchain and P2P networks.

• Thrust III: Multi-layered Security and Privacy Framework for AROMA System. This thrust aims to elevate the security and privacy of AROMA. We will leverage the mobile platform's trusted computing utilities to provide attested execution for our proposed local privacy protection mechanisms on each user that runs a AROMA Middleware. This multi-layered approach also enables stable participation and is featured a data poisoning attack defense to protect DCTD from adaptive and stealthy adversaries.

• Thrust IV: Experiments and Evaluation. We will implement the AROMA prototypes and evaluate them through performance benchmarking, simulation, and public-domain verification. This thrust will bring artifacts and insights into instrumenting a new oracle system for the DApp research community.

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 energy trading. Graduate students involved in this project will receive training on distributed systems and networking, trusted computing, system security, privacy, and software-hardware integration. The results will be used to enrich the relevant curriculum for both undergraduate and graduate students. 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; Truth Discovery; Distributed Consensus; Trusted Computing