Project Summary

Title: System-Network Co-design for Information Integrity and User Privacy in Decentralized Applications

Overview

Decentralized applications (DApps), enabled by blockchain and smart contracts, critically 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 IoT scenarios: no effective mechanisms to ensure the trustworthiness of the procured data; not protecting the privacy of DApp users with high data sensitivity; inability to transport real-time DApp operational data to the external auditors. To address these challenges, we propose to develop the AROPA system—Auditable Robust Oracle for Privacy-aware Decentralized Applications in this project. The AROPA design is inspired by the recent advances in decentralized systems, consensus mechanisms, secure hardware, and privacy-preserving technology. This project will develop the AROPA 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) enable private and verifiable event triggers that improve the efficiency of DApp data usage; 3) secure and robust auditing mechanism for DApp information transparency and compliance.

Intellectual Merit

This proposal describes a research plan to realize AROPA and advance the knowledge of protecting information integrity and privacy in challenging scenarios. The research tasks manifest in four thrusts:

• **Thrust I: Consensus-driven Truth Discovery for External Data Feed.** This thrust aims to develop the AROPA Middleware and networking mechanism to realize trustworthy data acquisition from external data sources. It is a new oracle solution that makes use of distributed truth discovery and fault-tolerant consensus to allow each participant to obtain custom-defined data feeds in an efficient, accurate, and fully decentralized manner.

• **Thrust II: Hardware-assisted Zero-Knowledge Proof Generation for Private Event Triggers.** When external data reveals sensitive information about a DApp's users, the external data should not be fetched and presented directly on the blockchain. This thrust aims to add privacy to the AROPA framework by leveraging Zero-Knowledge Proof (ZKP) mechanisms and trusted hardware to generate verifiable event triggers based on sensitive information efficiently. This approach is of independent interest to the fundamental research on hardware-assisted crypto performance optimization.

• **Thrust III: Enabling Real-time Capturing and Auditing on DApp Data Flow.** This thrust deals with the other direction: providing access to DApp data for external entities. It aims to elevate information integrity to the broader economical and societal level, since the increased transparency and auditability

• **Thrust IV: Experiments and Evaluation.** We will implement the AROPA prototypes and evaluate them in the public DApp domain. This thrust will bring artifacts and insights into instrumenting a DApp security tool for the community.

Broader Impacts

(TBD)

Keywords: Decentralized Application; System; Truth Discovery; Zero-Knowledge Proof; Trusted Computing; Privacy