Blockchain-based Mechanisms for Timed Data Release and Timed Transactions

Balaji Palanisamy, University of Pittsburgh

Project website: https://www.sis.pitt.edu/lersais/research/nsf-time-release/index.html

- ***Self-emerging data infrastructures keep the protected data secure and undiscovered such that it is not available prior to the release time and the data appears automatically at the release time.***

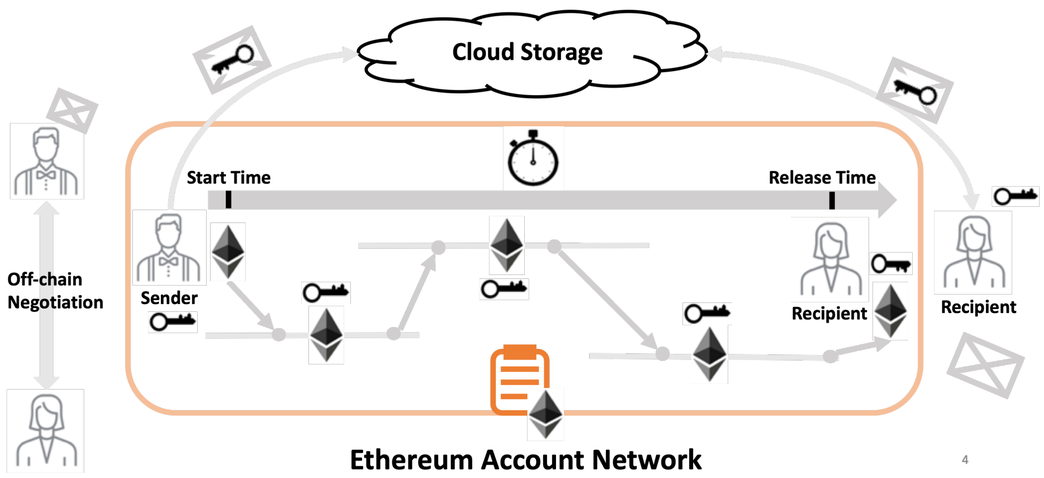
Limitations of existing solutions:

Cloud-based solutions:

- ***Cloud-based solutions are limited to a single point of trust***

Cryptographic solutions:

- ***Time lock puzzles can not ensure precise release time***
- ***Computationally expensive and difficult to scale***



Attack Resilience:

Drop Attack

- ***destroys the data before the prescribed release time***

Release-ahead Attack

- ***results in premature release of the data***

Rational adversaries

- ***violate the protocol only when there is monetary gain***

Malicious adversaries

- ***violate the protocol irrespective of monetary gain***

Features:

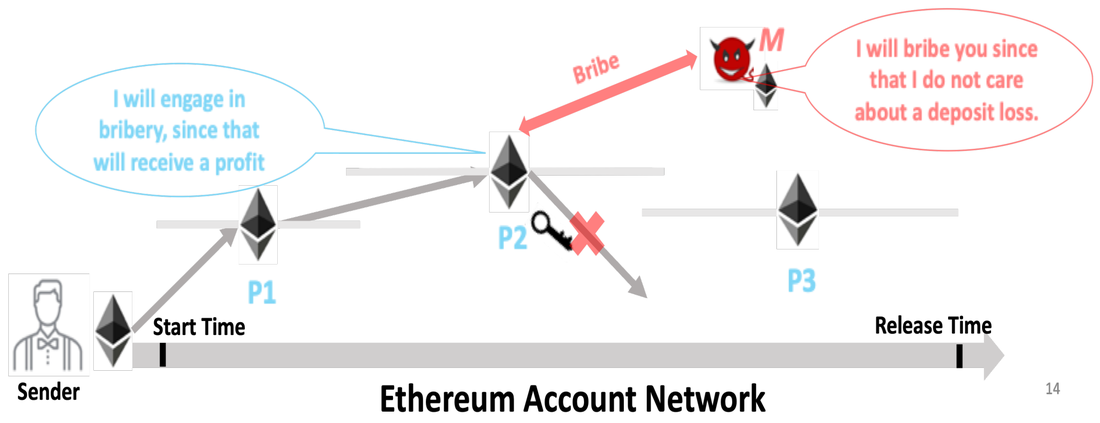
- ***Access control and access revocation, Release time modification, Data tracking, Event-driven data release, Timed execution***
- ***Gas cost optimization***

Scientific Impact:

- ***Will directly support decentralized applications requiring timed release of data or timed execution without a single point of trust.***
- ***The insights gained from this research can significantly foster decentralized application development in new areas and application domains where there is lack of support for decentralized control of data.***
- ***Applications such as secure auction systems, secure electronic voting and timed transactions benefit from these mechanisms.***

Protocol outline:

- ***Small shares of encryption key are dispersed and routed on the P2P network. The shares are assembled at the release time.***
- ***Peers are chosen based on reputation and the system is incentivized through monetary reward.***
- ***Misbehaviors and deviation from the protocols are penalized***
- ***Protect against rational adversaries using gamification***
- ***Mitigate malicious adversarial attacks using reputation***



Broader impact on society

- ***Will directly address the growing concerns of loss of control issues with centralized data storage and processing systems.***
- ***The research tackles the emerging needs of decentralized data management and application development through the novel concept of decentralized timed data release and timed execution in blockchain platforms.***

Education and Outreach

- ***Topics related to the research is being integrated into courses at Pitt.***
- ***A new doctoral seminar course on blockchain was offered in Spring 2022***
- ***Our plan for integrating education and research is aimed at creating a long term impact of developing a workforce trained in applying privacy concepts, models and techniques in designing large-scale distributed systems.***

Broader participation

- ***Educational module for high school students***
- ***Engage high school students in selected projects related to decentralized data management.***
- ***Summer HealthCare IT classes where the key concepts behind decentralized self-emerging data will be presented.***