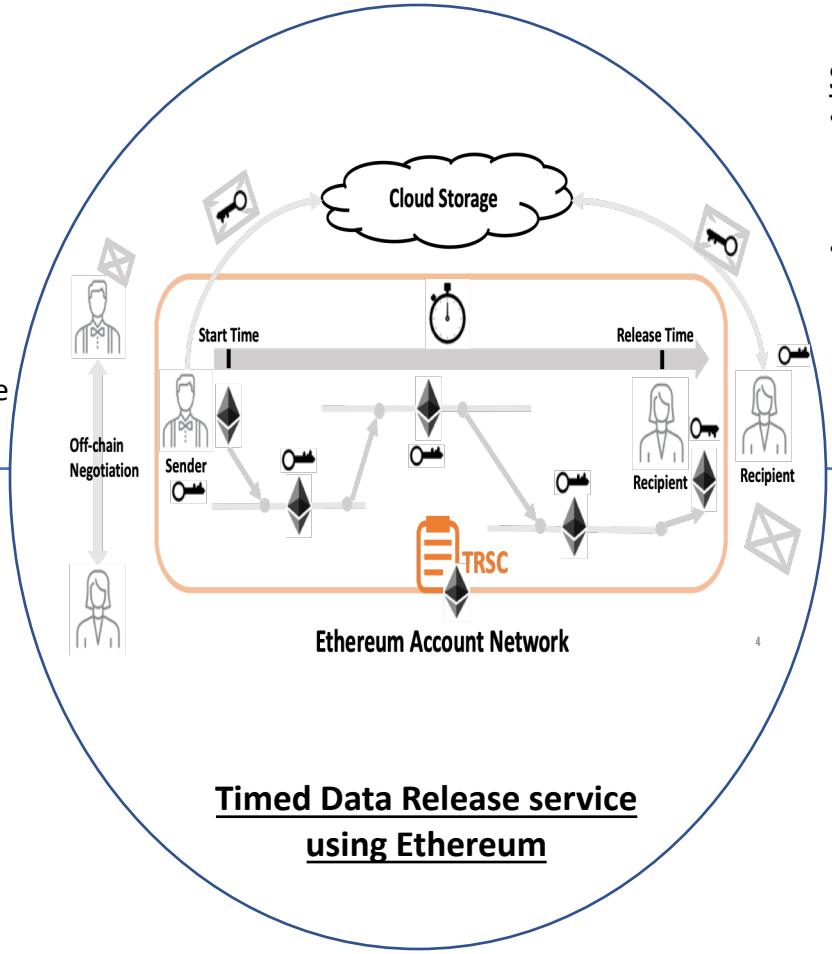
Blockchain-based Mechanisms for Timed Data Release and Timed Transactions

Challenge:

- Develop techniques to support Timed Data Release and Timed Execution using blockchains.
- Ensure attack resilience and minimize gas cost
- Applications such as secure auction systems, secure electronic voting and timed transactions benefit from these mechanisms..

Solution:

- 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.
- The techniques are resilient to both rational and malicious adversaries.



Timed Data Release service using Ethereum

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.

Broader Impact and Broader Participation:

- Will directly address the growing concerns of loss of control issues with centralized data storage and processing systems.
- Topics related to the research is being integrated into courses at Pitt.
- New doctoral seminar course on blockchain.
- Educational module for high school students.

Project info (# 2020071, University of Pittsburgh, Balaji Palanisamy (PI) bpalan@pitt.edu)