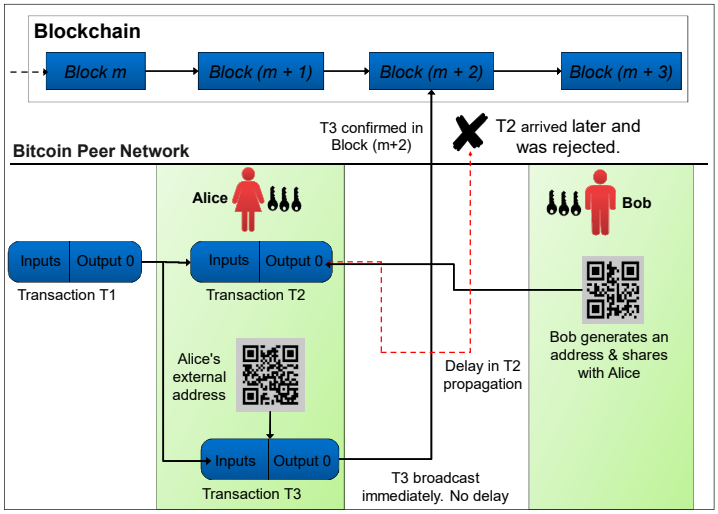
Secure Systems Group, Aalto University

Rakesh Gopinath Nirmala, Andrew Paverd, N. Asokan

Improving Security and Efficiency of Blockchain-based Cryptocurrencies

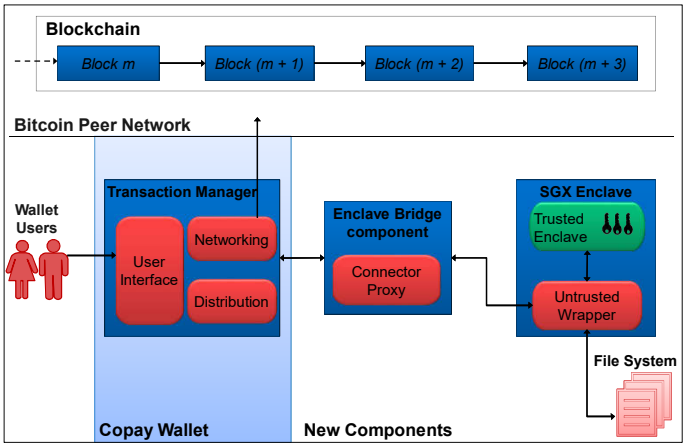
Blockchain and Double-spending

- Malicious payer can double-spend bitcoins
- Bitcoin recommends waiting for 6 blocks (60 minutes) for transaction to be confirmed
- Payee can accept payments sooner; but risks loss if payer double-spends
- Previous mitigation techniques require changes to Bitcoin protocol and/or miners



Solution Overview

- Secure wallet that uses a Trusted Execution Environment (TEE) to enforce:
  - Sign-once semantics: Ensures a key can sign only one transaction
  - Verifiable sign-once guarantee to payee sent as QR code
- Instant bitcoin payments, similar to credit cards
- No modifications to Bitcoin protocol or miners
- Realizable with off-the-shelf hardware



Design and Implementation

- Proof-of-concept implementation using Intel Software Guard Extensions (SGX):
  - SGX Enclave: Isolated and protected region of memory (C-library)
  - Integrated with Copay bitcoin wallet from Bitpay (JavaScript)
- Sign-once: Ensured by encapsulating trusted operations within the SGX enclave
- Verifiable confirmation: Remote attestation quote from enclave

Evaluation

- Minimal Trusted Computing Base
  - Number of enclave functions: 2
  - Lines of code: 1560
- Side-channel resistance
  - Deterministic controlled channel attacks: Input-independent operation
  - Cache attacks: Intel IIP crypto library hardened functions

Aalto University

Collaborative Research Institute for Secure Computing

cloSer