Secured Offline Blockchain Transactions for the Internet of Things (IoT)

**Context**

**Blockchain on IoT devices**
- No trusted participants
- No trusted middleman
- Unsecured devices
- Distributed ledger

**Challenges**
- Resource constraint devices:
  - Low power capabilities
  - Communication cost
  - Radio range
  - Delayed transactions
  - Proof of Work (PoW) no feasible on IoT devices
  - Limited device storage to store the whole ledger

**Offline Transactions in IoT**
- No need for constant connectivity
- No human interaction
- Decentralized approach to handle of payments
- Scalability

**Approach**
- Secure transaction based on payment channels
- Periodic connection to proxy
- Settlement over the Blockchain

**Outcome**
- No-fee transactions
- Secured device-to-device transaction
- Low energy consumption per transaction
- Integration with cloud-based Blockchain

**Research Area I**

**Example**

**Representation of the architecture**

**Research Area II**

**Securing IoT Devices**

**Environment**
- Low power devices
- Computation capabilities: ARM® Cortex® - M0
- Operation system: TockOS
- Offline transactions for Blockchain

**Goals**
- Extensive system security:
  - Verify Boot
  - Secured OS (TockOS)
  - Application layer security
  - Trusted Blockchain transactions
  - Monitoring energy consumption

**Example**

**IoT Device Verification Chain**

- Firmware
- Bootloader
- Operating System
- Blockchain Application
- Transaction

---

Christos Profentzas, Olaf Landsiedel