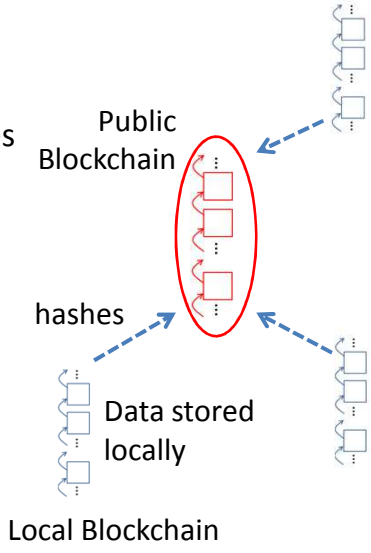
On the efficient use of Blockchains for IoT

Vasilios A. Siris
Mobile Multimedia Lab / AUEB
vsiris@aueb.gr
1/12/2017

Application of Blockchains to IoT

- Various proposals involve
  - Local blockchains that store data/transactions locally
  - Public blockchain that store hashes only
  - "data anchoring", opentimestamp/chainpoint
- Advantages
  - Better privacy: data stored locally rather than in public blockchain
  - Lower overhead/cost: less data sent & stored in public blockchain
  - Can still verify local data has not changed (immutability)



About local blockchains

- Local blockchain can be
  - Fully private
    - Managed by a local manager (e.g. gateway)
    - Does not require consensus mechanisms
  - Permissioned (or consortium blockchains)
- Public blockchain provides additional immutability guarantees to those provided by local blockchain
  - Fully private blockchain: guarantee = how much we trust manager
  - Consortium blockchain: guarantees depend on consensus mechanism

About local blockchains (cont.)

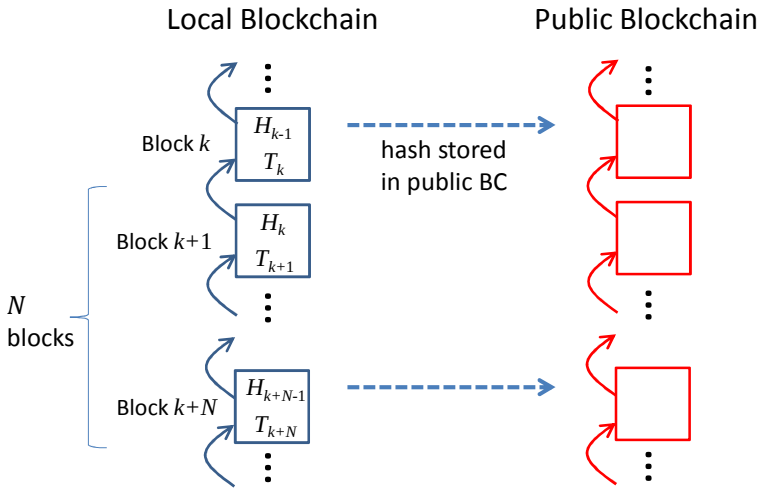
- Sidechains and off-chain transactions pose additional issues
  - Scenarios with multiple entities requiring distributed trust
  - Distributed consensus necessary
  - Asset/currency transfer an issue, e.g. micropayment channels
  - Merged mining (sharing PoW) proposals: second blockchain uses PoW of primary (e.g. bitcoin) blockchain
    - For cases where second blockchain requires consensus

Use cases

- SW updates
- Device/appliance compliance, maintenance, repair
- Device/network authentication
- Product provenance, asset tracking & ownership

- Storing data is different than storing currency transactions
  - relies solely on “proof of publication”
  - no currency transfer between local/public blockchain
  - no double spending problem

Storing local hashes in public blockchain

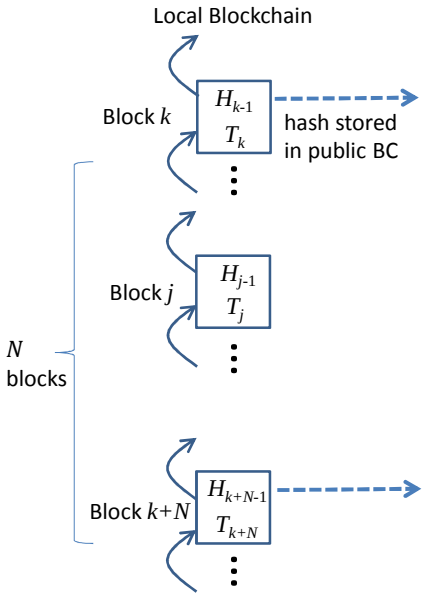


Question investigated

- *How often should local hashes be stored in public blockchain?*
- Costs and tradeoff:
  - **Public blockchain cost**: transmission of hashes, monetary
  - **Verification cost**: number of hashes required for verification
  - ***Tradeoff***: Fewer local hashes stored in public blockchain $\Rightarrow$ lower public blockchain cost but more hashes required for verification, i.e. higher verification cost

Verification for local blockchains

- To verify T_j need hashes from H_{j-1} up to H_{k+N-1}
  - H_{k+N-1} stored in public blockchain
  - # of hashes needed on average is $N/2$ (assuming all data has same popularity)
- $N = \frac{r_{trans}}{f}$
  - r_{trans}: rate of transactions (blocks)
  - f: rate hashes stored in public blockchain



Local data structure alternatives

- Single data file (or concatenation of files)
  - Hash of whole file stored in public blockchain
- Local blockchain (hash chain)
  - Subset of hashes stored in public blockchain
- Merkle tree (binary hash tree)
  - Merkle root hash stored in public blockchain
  - Verification requires fewer hashes
- Alternatives have *different verification cost*

Summary

- Application of blockchains to IoT requires only "proof of publication" feature
  - Unless we require currency/asset transactions
  - Double spending problem more difficult
- Hierarchy of blockchains can facilitate scalability
  - Similarities with sidechains that are proposed for bitcoin scalability