Proof of Authentication for Private Distributed Ledger

Zhiyi Zhang*, Vishrant Vasavada, Randy King, Lixia Zhang

*presenter

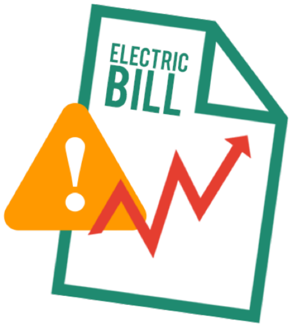
Use Case: Home Solar Networking -- IoT

Rooftop devices record customer energy consumption/production.

These records are transferred to the cloud server for storage.

Records will be used to bill customers

Issues with centralized solutions

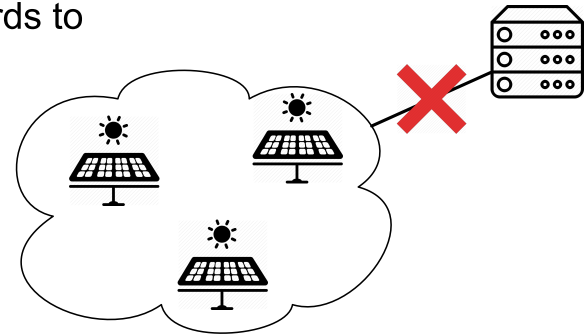


Asymmetric information: Power grid provider controls all the records

- Lack of transparency / surveillance

IoT-friendly?

- No guarantee that IoT devices can successfully upload the records to the server, e.g., partition, intermittent connectivity, etc.



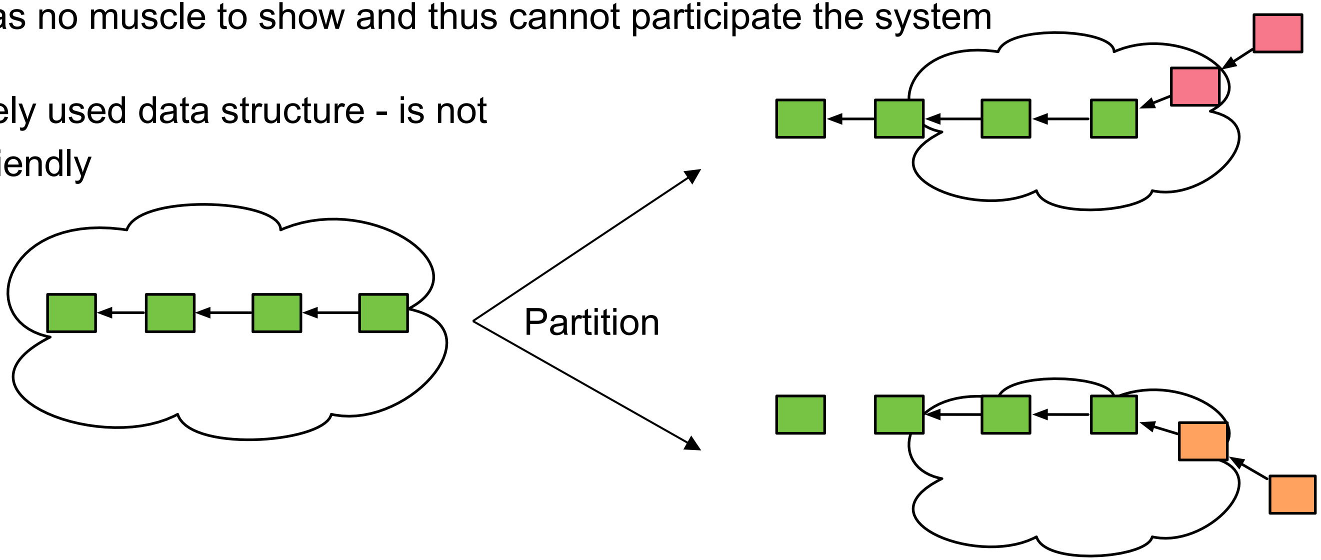
Blockchain-based Distributed Ledger System?

- Blockchain based
- Consensus algorithms

Issues with existing distributed ledger systems

Most distributed ledgers today are not IoT friendly

- Most consensus mechanisms are “muscle show”
  - E.g. Proof-of-Work, Proof-of-Space, Proof-of-Stake, etc.
  - IoT device has no muscle to show and thus cannot participate the system
- Blockchain - a widely used data structure - is not network partition friendly



DLedger: Goals and Assumption

Goals

- Data authenticity, integrity, and availability
- Be IoT-friendly
  - Efficient for IoT device (IoT device friendly)
  - Heterogeneous Network (IoT network friendly)

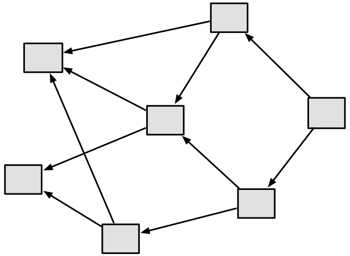
Assumptions

- Trust Relationships in private system
  - Shared trust anchor
  - Issues identity certificate for each node in the system

High-Level Perspective

Three Simple Approaches

- Uses lightweight Proof-Of-Authentication (PoA)
  - An ECDSA signature
  - IoT device friendly
- Uses Directed Acyclic Graph (DAG) as data structure
  - IoT network friendly
  - Efficiency
- Built over Named Data Networking (NDN)
  - More efficient data dissemination in P2P network in IoT
  - Deployable in private network system



NDN

Background 1: IOTA[1]

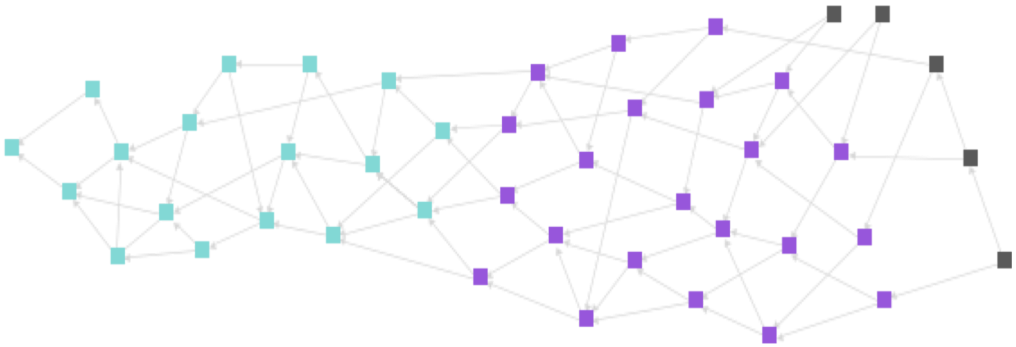
- A cryptocurrency
- Use lightweight PoW to be IoT friendly
- Based on the Tangle (a graph) instead of a single blockchain

However

- Even modern computer takes **time in minutes** to calculate PoW. IoT devices still cannot directly contribute to the ledger.
- Outsource calculation to a server --- Who provide the server? single-point-of-failure? heterogenous network condition?

[1] IOTA: S. Popov, “The tangle,” cit. on, p. 131, 2016.

Background 1: IOTA's Tangle

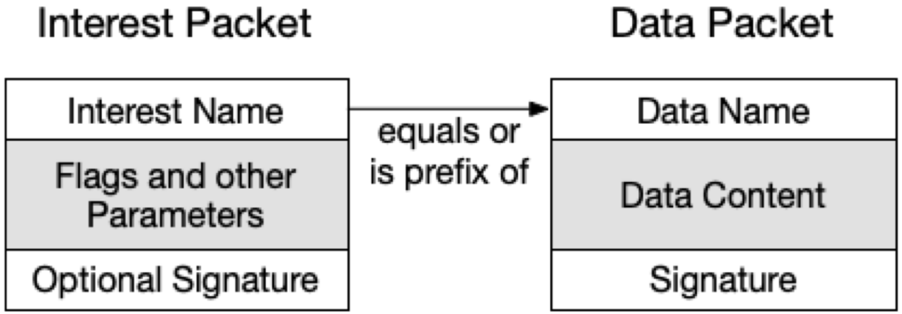


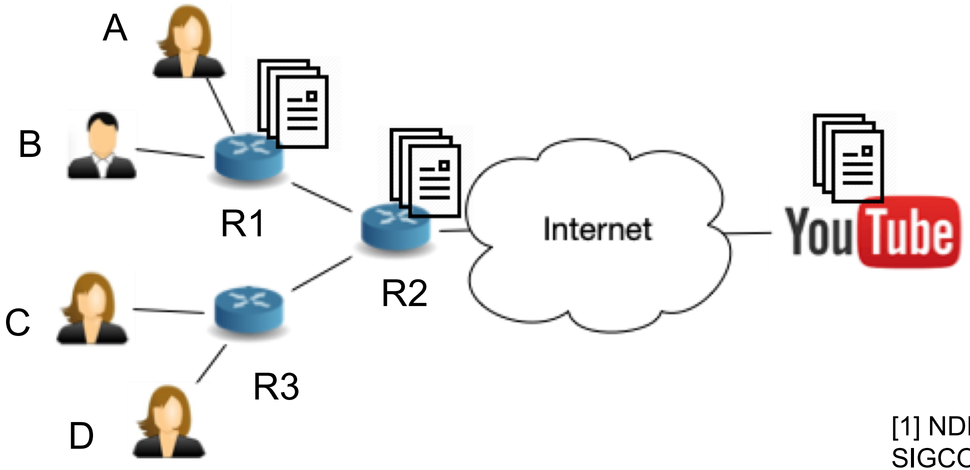
- Each block approves two existing blocks
- IOTA uses weighted random walk (Monte Carlo Markov Chain, MCMC) from ancient block to tailing blocks to select blocks to approve
- Each block carries a weight
  - (PoW + approvers' PoW)

When a block is approved (directly and indirectly) by all the tips, it is said to be fully confirmed and the system reaches consensus on this block

Background 2: Named Data Networking (NDN)[1]

- Use data names to fetch the data from the network using request/response pattern.
  - Request = Interest packet
  - Response = Data packet
- Data is secured at the time of creation: producer signs the Data.





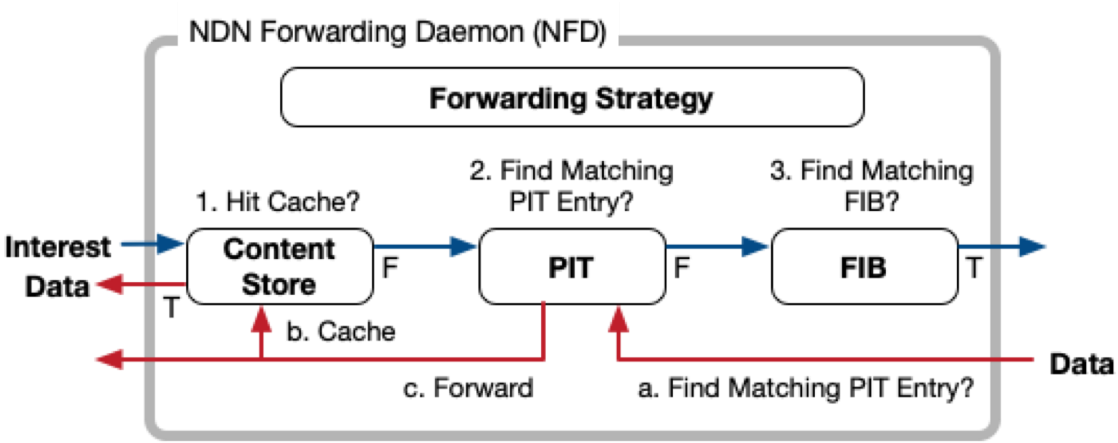
Neither Interest and Data packet carries addresses.

- Interest aggregation
- In-network Cache

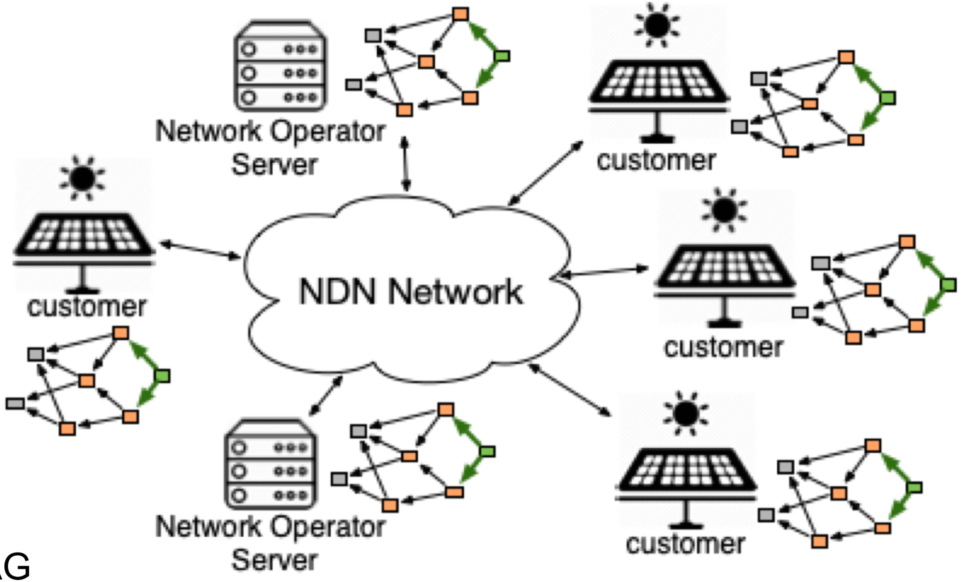
[1] NDN: L. Zhang, A. Afanasyev et al., "Named Data Networking," ACM SIGCOMM Computer Communication Review, 2014.

Background 2: NDN's Stateful Forwarding

- Forward Interest packet by **Name**.
- Keep each Interest's **state** in the Pending Interest Table (PIT)
  - Interest Name
  - Incoming interface, outgoing interface
- Forward the Data packet following the **Interest's path reversely** back to the requester



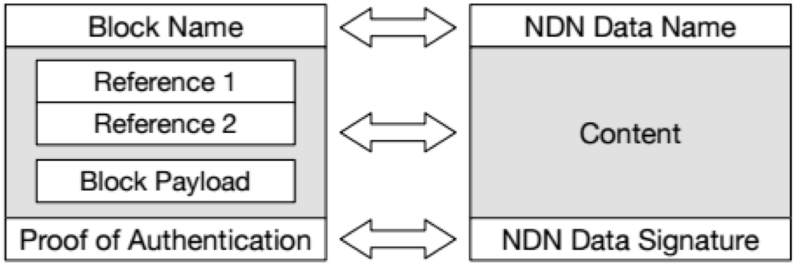
DLedger's P2P network

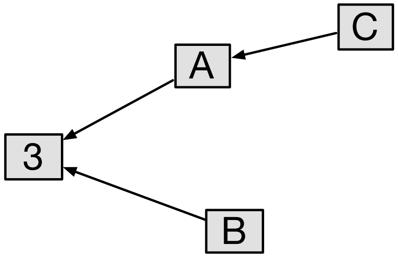


- A **peer-to-peer network** of
  - Customer nodes
  - Business Provider's Servers
- Each peer maintains a local ledger – a DAG
- Use DLedger's protocols to advertise now blocks and sync up the local ledgers.
  - Notification Protocol
  - Synchronization Protocol

DAG-based Ledger and Proof-of-Authentication

- Store all the energy usage, certificate issuance, certificate revocation into the **records (blocks)** in the DAG.
- Each record also carries a Name and PoA
  - Unique Record (block) Name: /dledger/<creator prefix>/<record hash digest>
  - E.g., /dledger/solar-gtw-001/23c7a46e2d2abb2333bc491957c8be0320d5c876
- When a record gains enough number of approvals, it is confirmed. If not, record and following records will be **abandoned (incentives).**



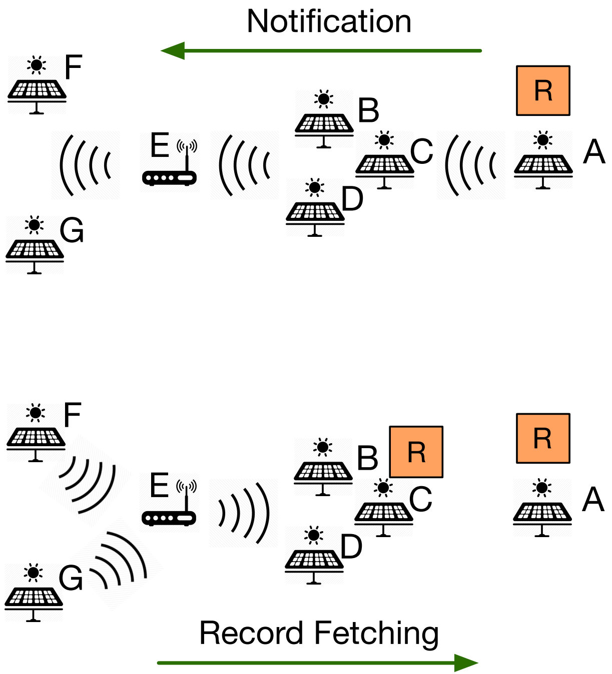


Each block is an NDN Data Packet

- Block Name becomes NDN packet name
- Approvals and content (energy usage, cert management) is the Data content
- Proof-of-Authentication is simply NDN Data packet signature

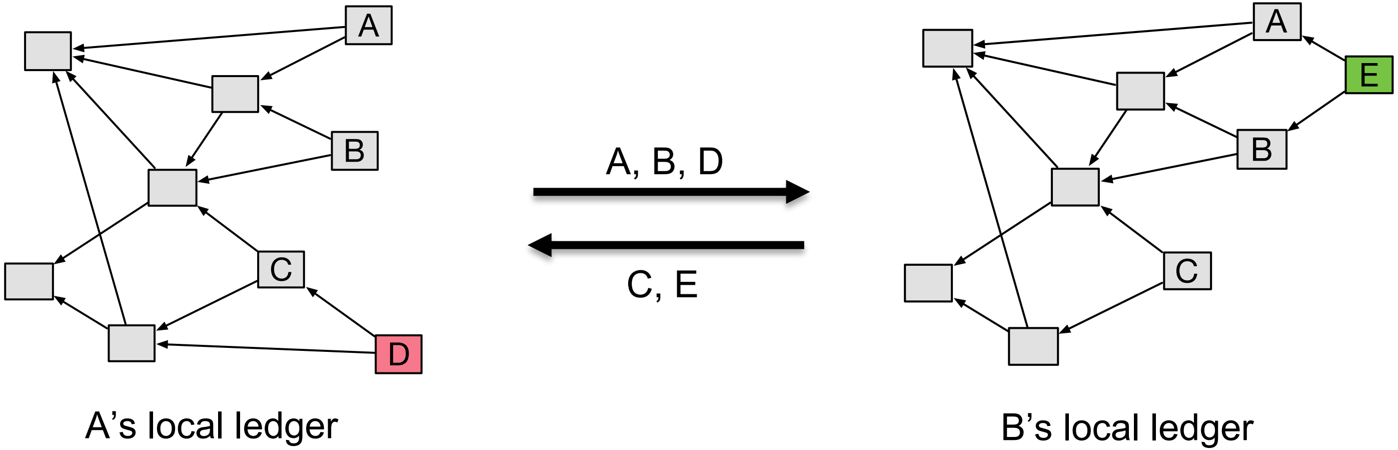
DLedger: New Record Notification

- Each node has registered two NDN prefixes to receive DLedger Interests
  - /dledger : receive multicast Interest
  - /dledger/<creator prefix>: receive unicast Interest
- Peer multicasts new record Notification Interest (Notif) to the whole system
  - /dledger/NOTIF/<creator prefix>/<record-digest>
  - Notif bears hints to construct the new record's name -- being able to fetch it from NDN by dropping the <NOTIF> component



DLedger: Synchronization

- Peers synchronize their ledgers by exchanging a list of tailing records through **Sync Interest**
  - /dledger/SYNC/<creator prefix>/<tailing-record-list-digest>
- Peers compare the received tailing record list with the local list.
  - Starting from missing tailing record, e.g., D, recursively fetch all the missing records
  - Notify the sender if a received tailing record is not longer a tail in local ledger, e.g., A, B



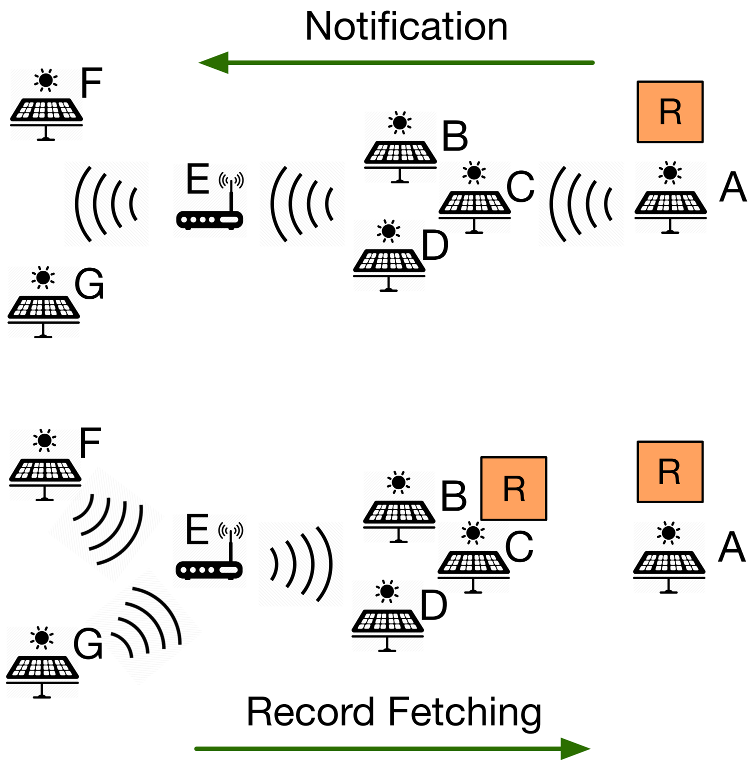
NDN-based Protocols v.s. Gossip Protocol

Efficient Data Dissemination by NDN:

- Packet Suppression:
  - B, C don't need to broadcast if C has already done it
- Interest Aggregation:
  - Interest sent from F and G merge
- Record Cache:
  - E fetches record from C
  - Efficient retransmission

Gossip Protocol

- Runs at application layer
- Don't have such benefits



Conclusion and Future Work

- A distributed ledger for private IoT business model
  - Ledger design: DAG tolerates the network partition; PoA enables IoT devices to function in the system.
  - Network design: NDN-based protocols for efficient data dissemination.
  - **The power of openness: Any malicious attempts will leave the footprint because of the PoA**
- Future work
  - Size of Tangle
    - DAG keep growing in its size.
    - Future solution: decentralized backup and snapshot mechanism
  - Tip Selection Algorithm Efficiency
    - MCMC is costly: app needs to parse entire DAG into memory
    - Our temporarily solution: Make DAG bidirectional, which requires frequent database update
    - Future solution: get rids of MCMC; select random tips for approval from tip list without any walk
  - Potential Attack Scenarios and Abuse
    - Attacks such as spam record flooding, collusion of peers, and self-approvals expanding graph depth indefinitely
    - Possible future solution: Introduce security policies to deny such attacks from happening rationally

Thank You

zhiyi@cs.ucla.edu