B-IoT: Blockchain Driven Internet of Things with Credit-Based Consensus Mechanism

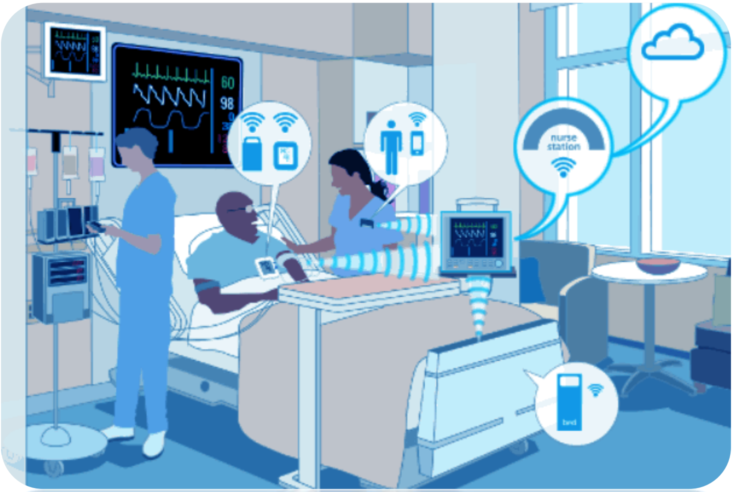
ICDCS 2019, Dallas, Texas

Junqin Huang, Linghe Kong, Guihai Chen, Long Cheng, Kaishun Wu and Xue Liu

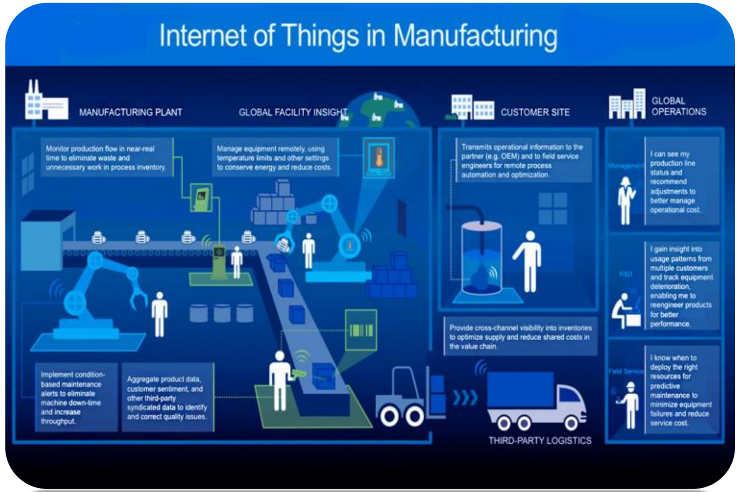
Shanghai Jiao Tong University

Internet of Things Systems

Transportation



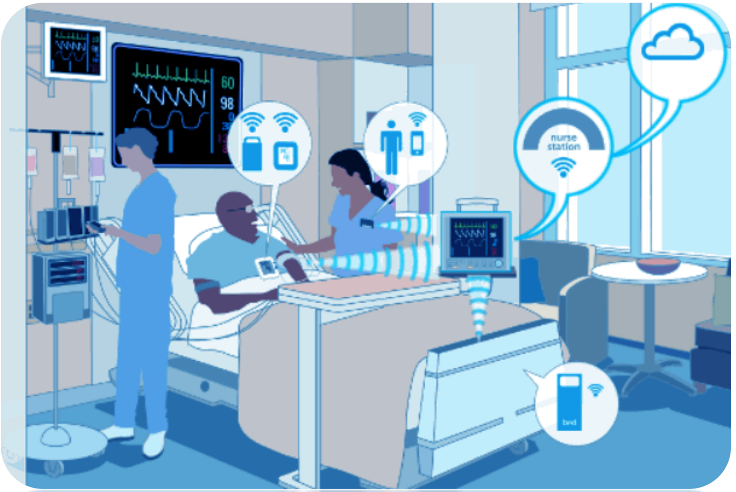
Healthcare



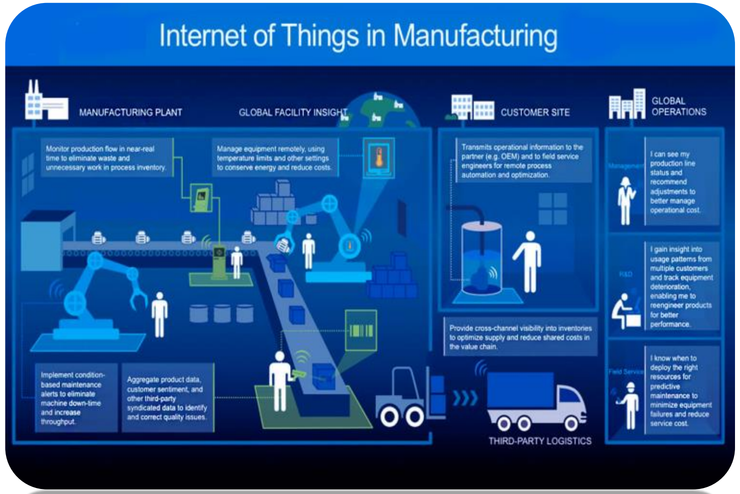
Industrial/Manufacturing Field

Internet of Things Systems

Transportation



Healthcare

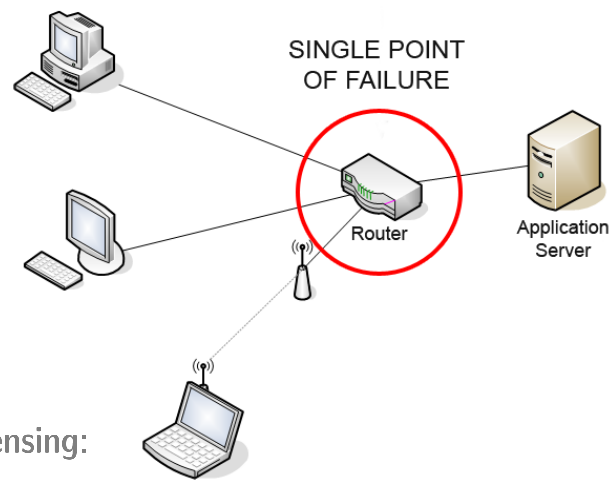


Industrial/Manufacturing Field

IoT smart objects are expected to reach 212 billion entities deployed globally by the end of 2020

Open Issues in IoT Systems

- Single point of failure [1]
- Malicious attacks such as DDoS, Sybil attack [2], [3]
- Data disclosure & credibility [4]
- System scalability [5]



[1] I. J. Vergara-Laurens, L. G. Jaimes, and M. A. Labrador, "Privacy-preserving mechanisms for crowdsensing: Survey and research challenges," IEEE Internet of Things Journal, vol. 4, no. 4, pp. 855–869, 2017.
[2] H. Yu, P. B. Gibbons, M. Kaminsky, and F. Xiao, "Sybillimit: A near-optimal social network defense against sybil attacks," in IEEE Symposium on Security and Privacy (S&P), May 2008, pp. 3–17.
[3] Y. Lu and L. D. Xu, "Internet of things (iot) cybersecurity research: A review of current research topics," IEEE Internet of Things Journal, pp. 1–1, 2018.
[4] IoTeX, "Blockchain & iot: What's it all about?" Oct 2018. [Online]. Available: https://hackernoon.com/blockchain-iot-whats-it-all-about-f594b3f0da1e
[5] K. Iwanicki, "A distributed systems perspective on industrial iot," in IEEE 38th International Conference on Distributed Computing Systems (ICDCS), July 2018, pp. 1164–1170.

Combine Blockchain with IoT?

- Why Blockchain in IoT
  - non-manipulated source of data
  - break down monolithic data silos and enable trust across parties
- Related Work
  - A scalable access management system in IoT [IOTJ'18]
    - vulnerable to the single point failure and attacks
  - Consortium blockchain for secure energy trading in IIoT [TII'18]
    - data disclosure risk
  - A blockchain platform for clinical trial and precision medicine [ICDCS'17]
    - stuck in the concept stage
  - Integrating low power IoT devices to a blockchain-based infrastructure [EMSOFT'17]
    - bring too much overloads in IoT systems

Main Challenges

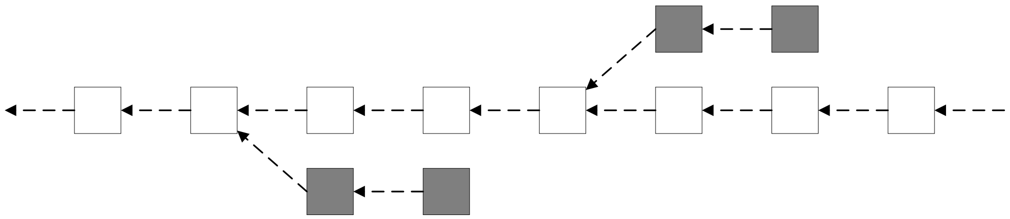
- The conflicts between high concurrency and low throughput
- The trade-off between efficiency and security
- The coexistence of transparency and privacy

Main Challenges

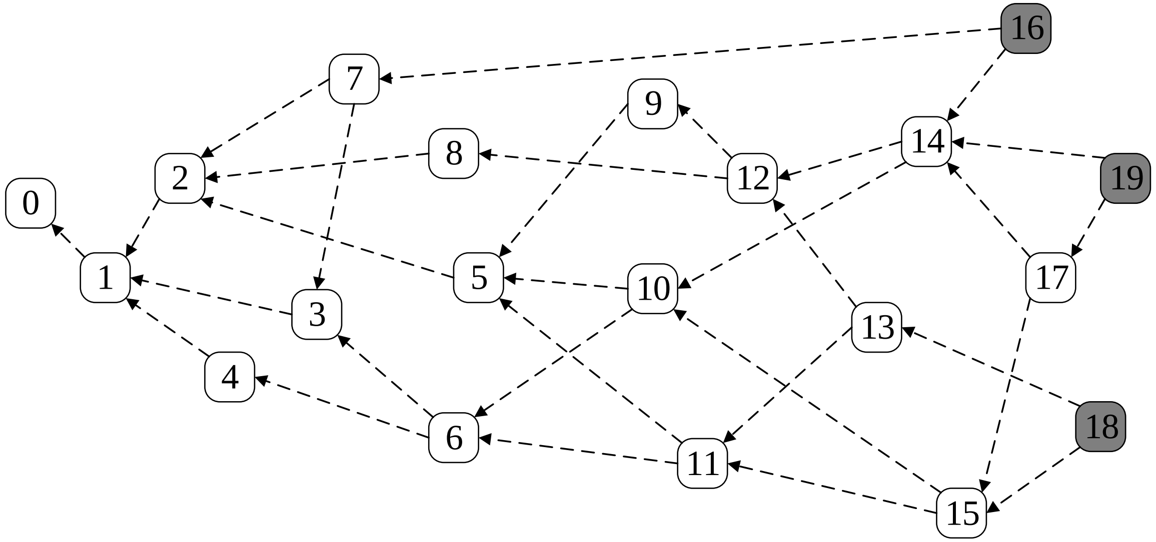
- The conflicts between high concurrency and low throughput
  - We explore a DAG-structured blockchain based solution
- The trade-off between efficiency and security
- The coexistence of transparency and privacy

Blockchains

- Distributed ledgers or databases that enable parties which do not fully trust each other to form and maintain consensus



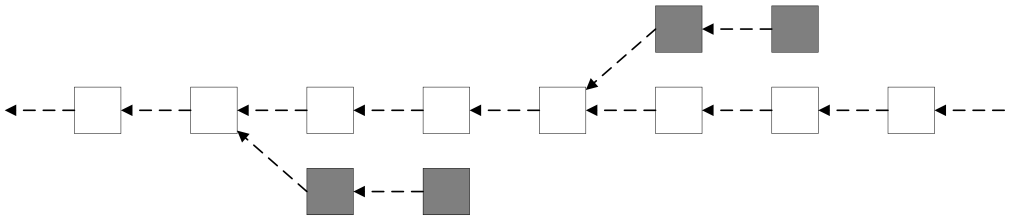
Chain-structured blockchain
(bitcoin, Ethereum, Hyperledger, etc.)

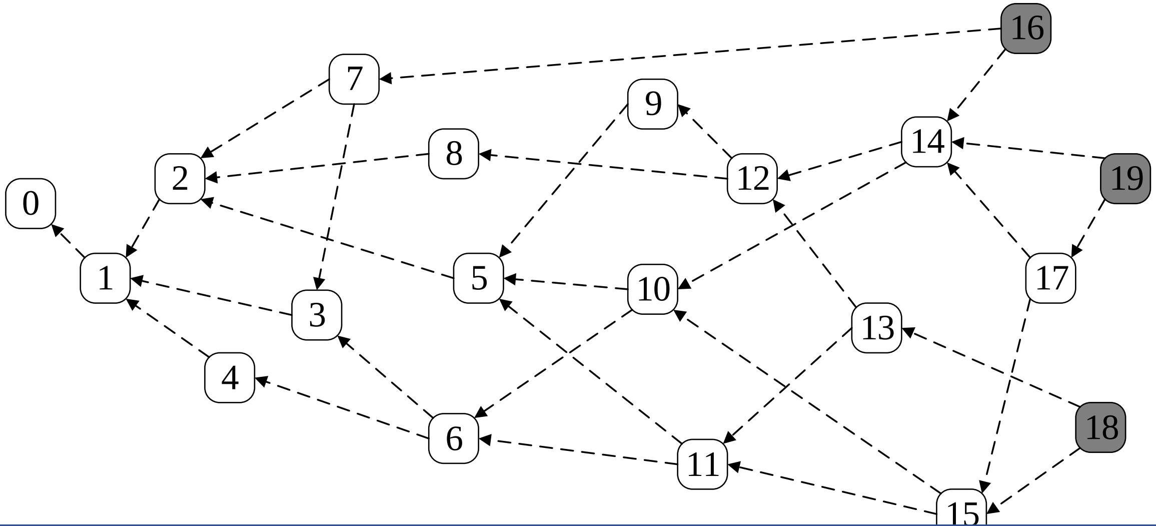


Directed acyclic graph (DAG)-structured blockchain
(IOTA, Byteball, NANO, etc.)

Blockchains

- Distributed ledgers or databases that enable parties which do not fully trust each other to form and maintain consensus

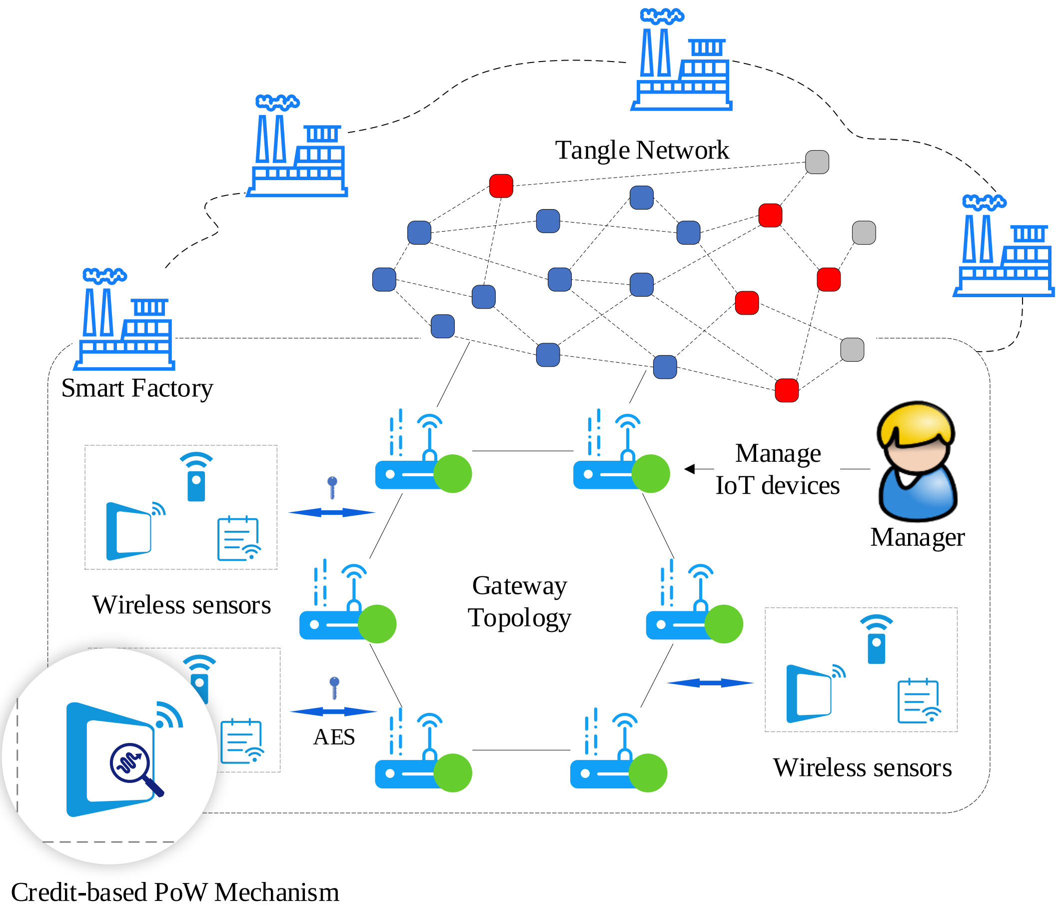




DAG-structured blockchains have a higher throughput than chain-structured blockchains

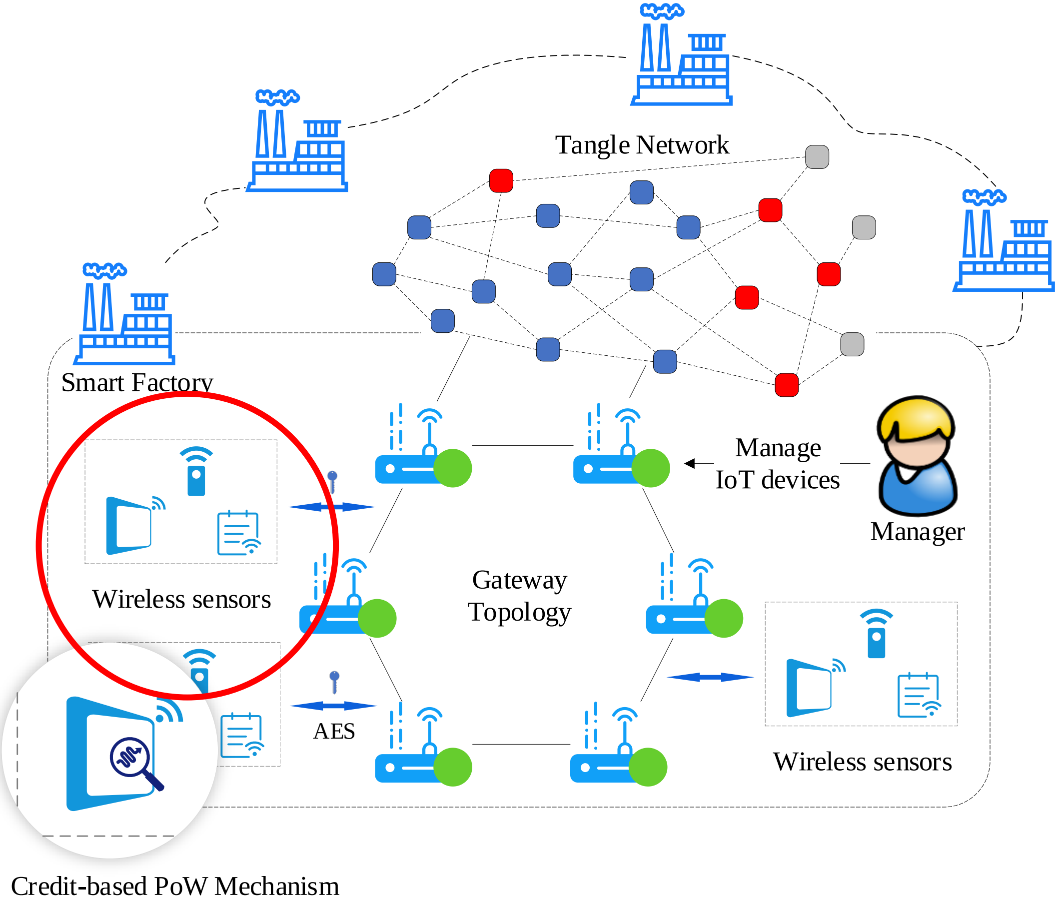
B-IoT: System Overview

- Node type:
  - Light nodes
  - Full nodes
- A case study of smart factory:
  - Wireless sensors
  - Gateways
  - Manager
  - Tangle network



B-IoT: System Overview

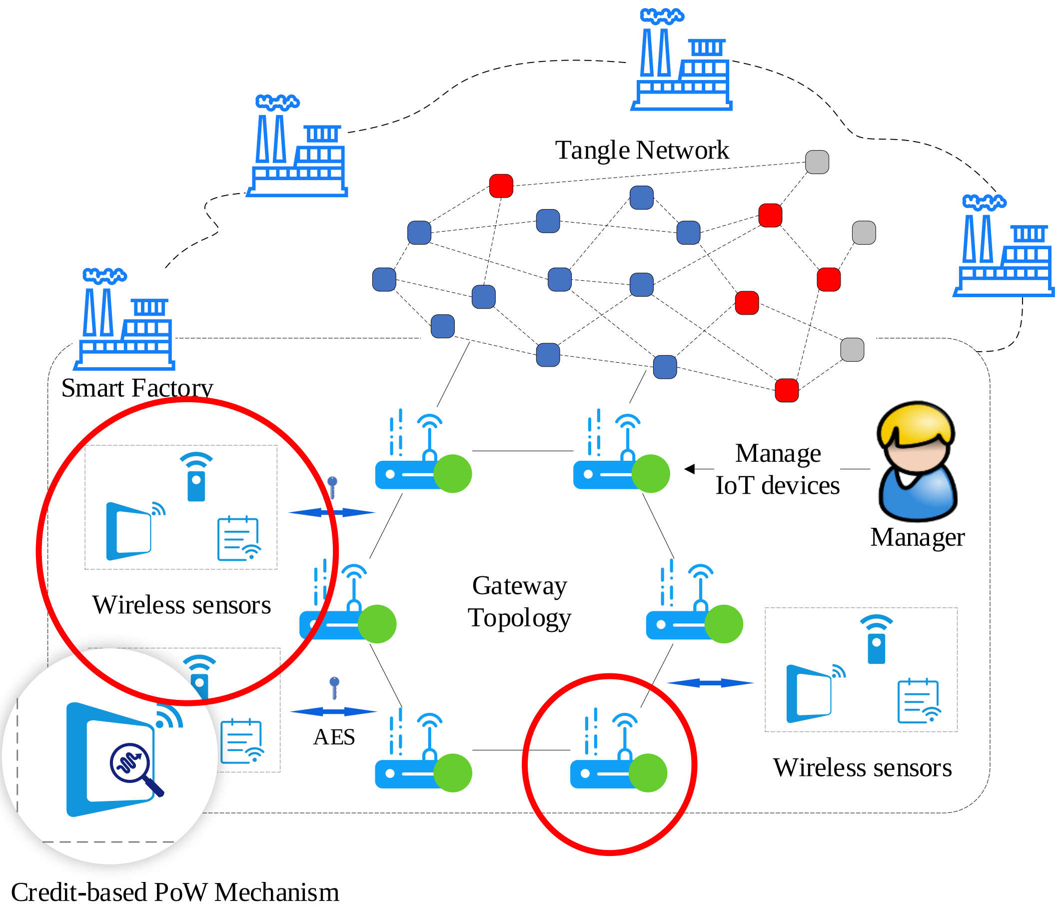
- Node type:
  - Light nodes
  - Full nodes
- A case study of smart factory:
  - Wireless sensors
  - Gateways
  - Manager
  - Tangle network



B-IoT: System Overview

- Node type:
  - Light nodes
  - Full nodes

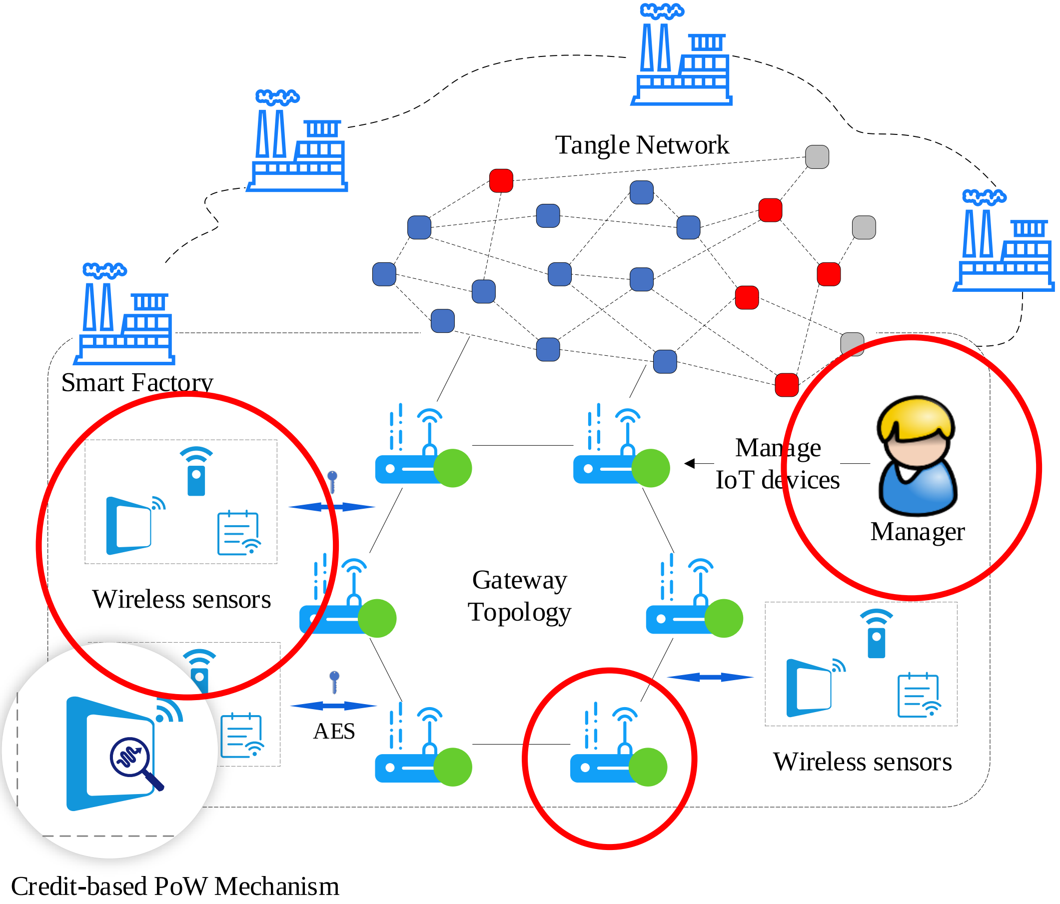
- A case study of smart factory:
  - Wireless sensors
  - Gateways
  - Manager
  - Tangle network



B-IoT: System Overview

- Node type:
  - Light nodes
  - Full nodes

- A case study of smart factory:
  - Wireless sensors
  - Gateways
  - Manager
  - Tangle network



Main Challenges

- The conflicts between high concurrency and low throughput
  - We explore a DAG-structured blockchain based solution
- The trade-off between efficiency and security

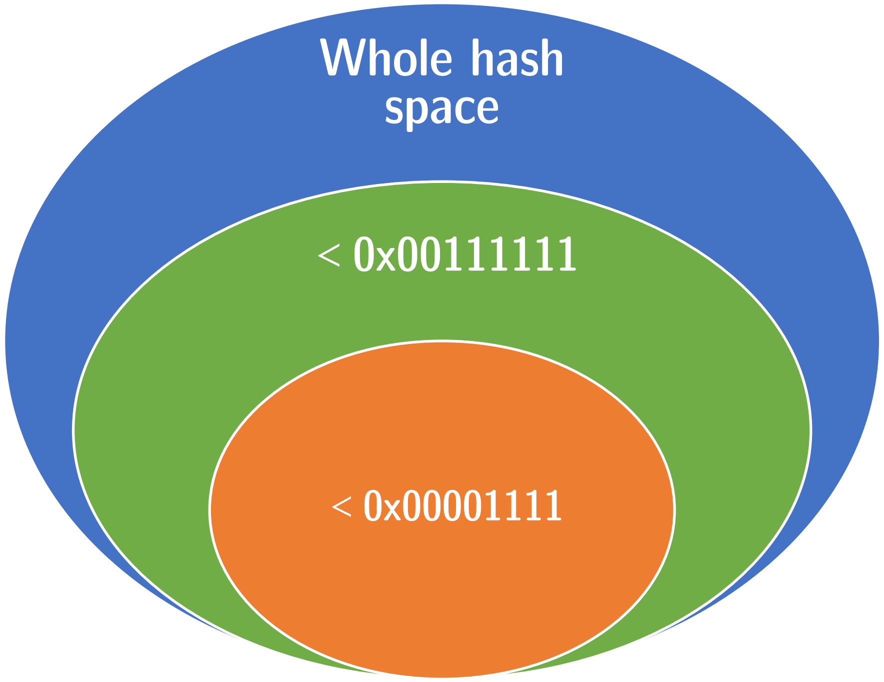
- The coexistence of transparency and privacy

Main Challenges

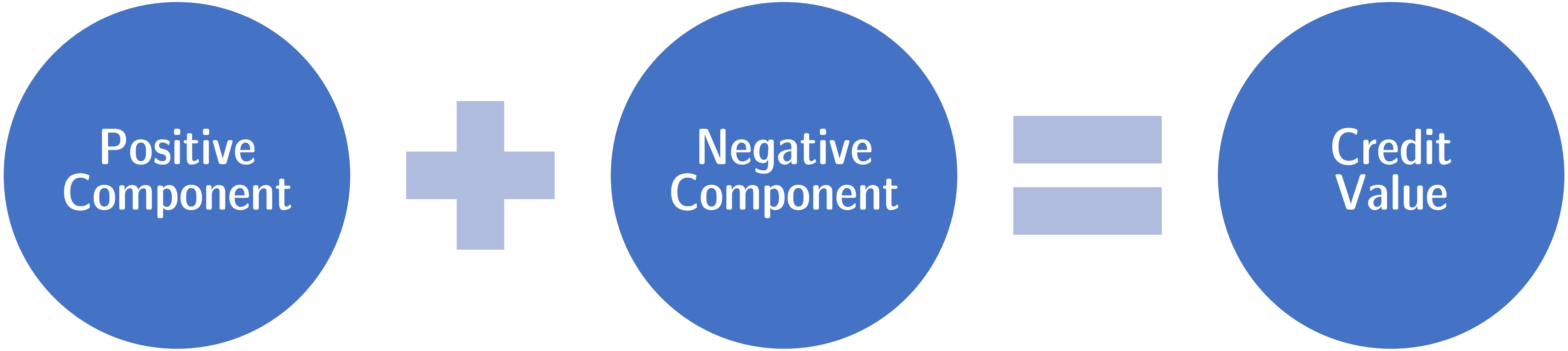
- The conflicts between high concurrency and low throughput
  - We explore a DAG-structured blockchain based solution
- The trade-off between efficiency and security
  - We design a moderate-cost credit-based PoW mechanism
- The coexistence of transparency and privacy

Tuning the difficulty of PoW algorithm

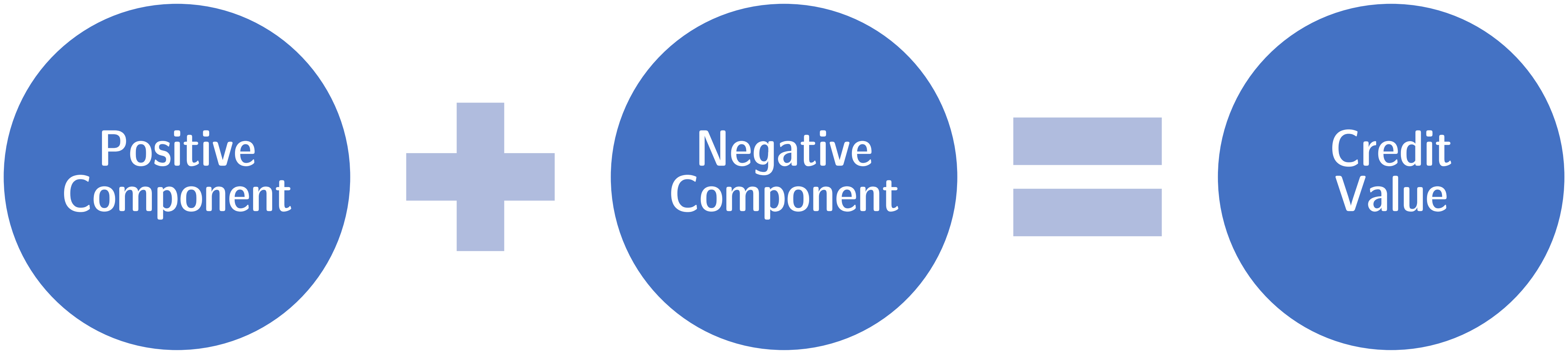
- Less than the target hash value, i.e. the length of prefix zero
- E.g. hash space is 0x00000000~0xffffffff



Credit-Based PoW Mechanism

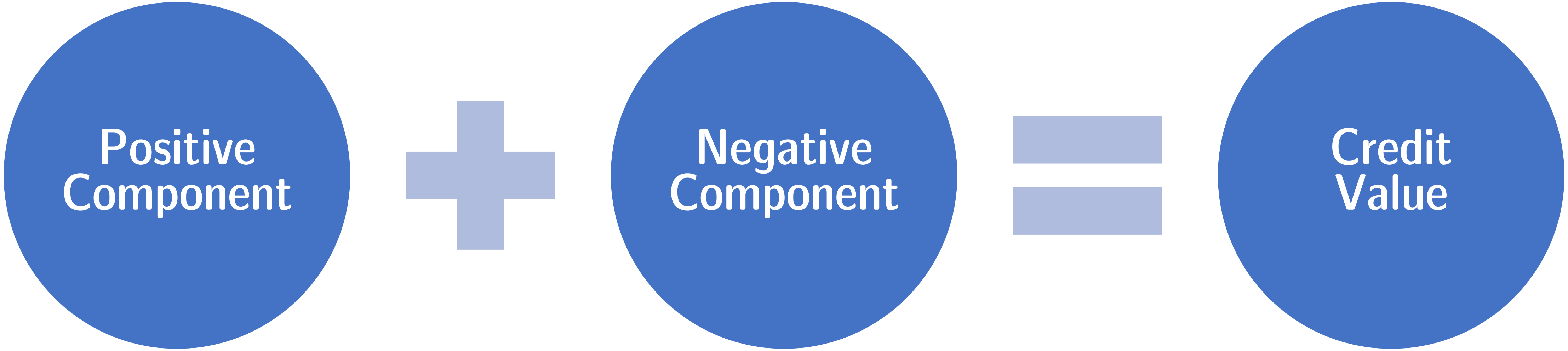


Credit-Based PoW Mechanism



$$Cr_i^P = \frac{\sum_{k=1}^{n_i} w_k}{\Delta T}$$

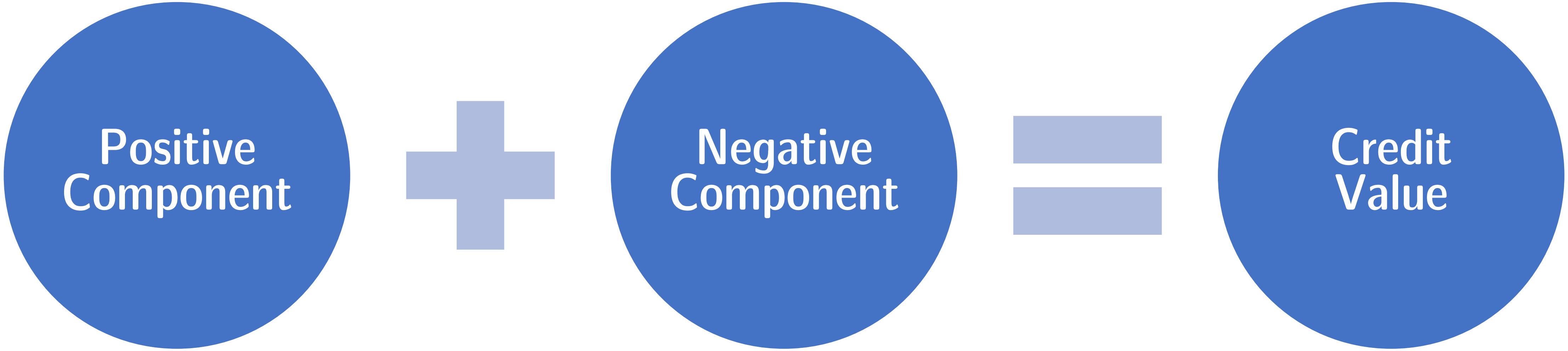
Credit-Based PoW Mechanism



$$Cr_i^P = \frac{\sum_{k=1}^{n_i} w_k}{\Delta T}$$

$$Cr_i^N = -\sum_{k=1}^{m_i} \alpha(\mathcal{B}) \cdot \frac{\Delta T}{t - t_k}$$

Credit-Based PoW Mechanism

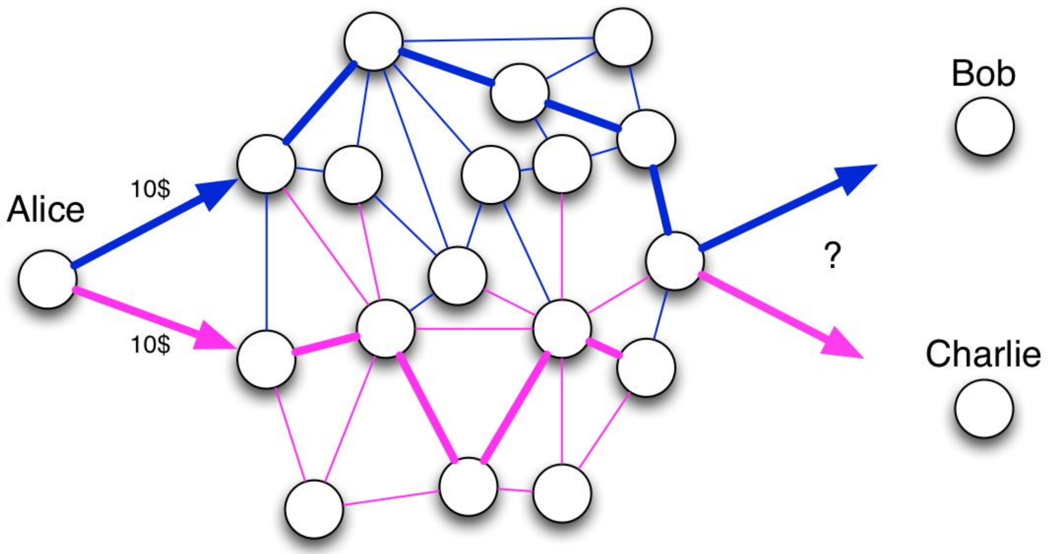


$$Cr_i^P = \frac{\sum_{k=1}^{n_i} w_k}{\Delta T}$$

$$Cr_i^N = -\sum_{k=1}^{m_i} \alpha(\mathcal{B}) \cdot \frac{\Delta T}{t - t_k}$$

Malicious Behaviours

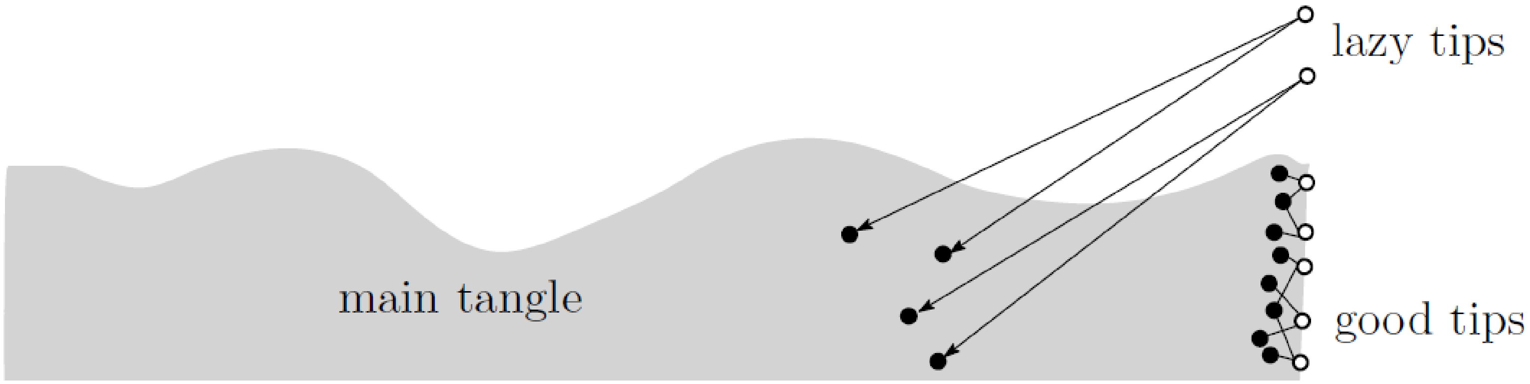
- Double-spending
- Lazy-tips



$$\alpha(\mathcal{B}) = \begin{cases} \alpha_l & \text{if } \mathcal{B} \text{ is lazy tips behaviour;} \\ \alpha_d & \text{if } \mathcal{B} \text{ is double-spending behaviour,} \end{cases}$$

Malicious Behaviours

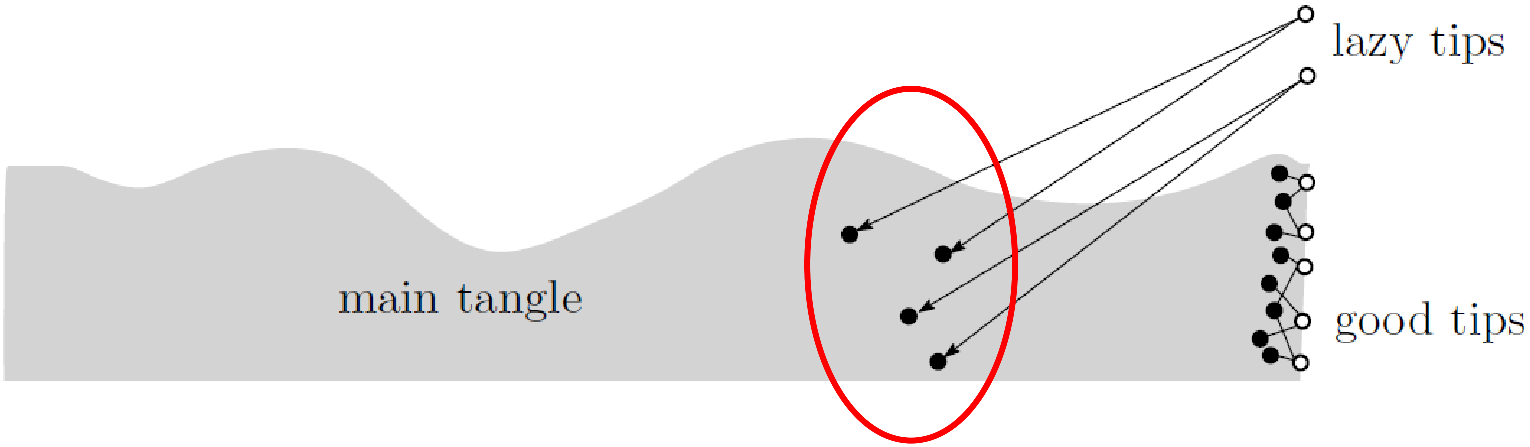
- Double-spending
- Lazy-tips



$$\alpha(\mathcal{B}) = \begin{cases} \alpha_l & \textit{if } \mathcal{B} \textit{ is lazy tips behaviour;} \\ \alpha_d & \textit{if } \mathcal{B} \textit{ is double-spending behaviour,} \end{cases}$$

Malicious Behaviours

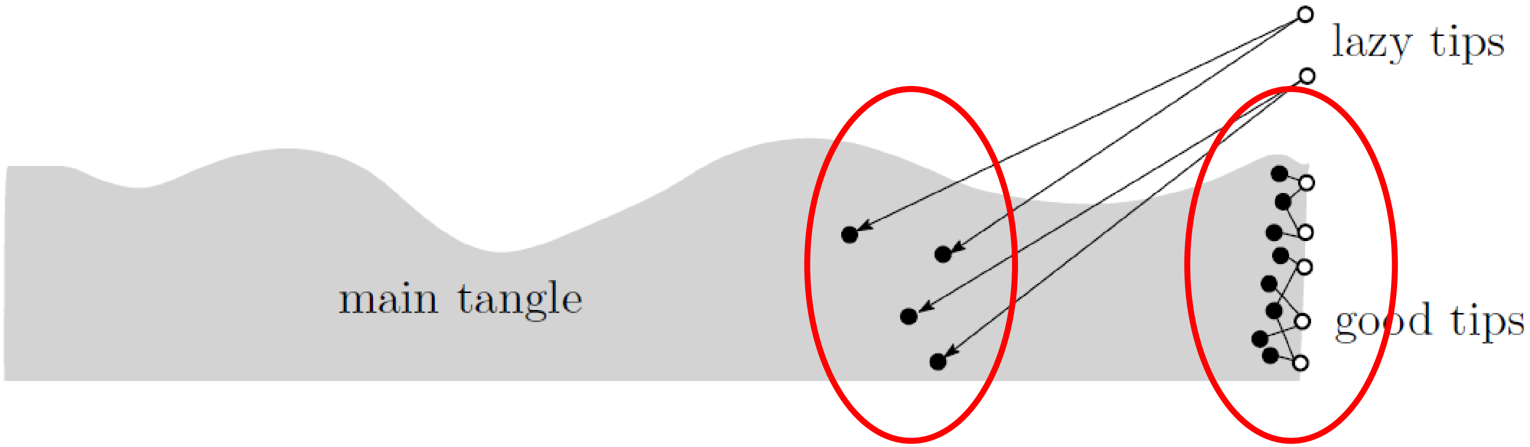
- Double-spending
- Lazy-tips



$$\alpha(\mathcal{B}) = \begin{cases} \alpha_l & \textit{if } \mathcal{B} \textit{ is lazy tips behaviour;} \\ \alpha_d & \textit{if } \mathcal{B} \textit{ is double-spending behaviour,} \end{cases}$$

Malicious Behaviours

- Double-spending
- Lazy-tips



$$\alpha(\mathcal{B}) = \begin{cases} \alpha_l & \textit{if } \mathcal{B} \textit{ is lazy tips behaviour;} \\ \alpha_d & \textit{if } \mathcal{B} \textit{ is double-spending behaviour,} \end{cases}$$

Credit-Based PoW Mechanism

Positive Component + Negative Component = Credit Value

$$Cr_i^P = \frac{\sum_{k=1}^{n_i} w_k}{\Delta T}$$

$$Cr_i^N = -\sum_{k=1}^{m_i} \alpha(\mathcal{B}) \cdot \frac{\Delta T}{t - t_k}$$

$$Cr_i = \lambda_1 Cr_i^P + \lambda_2 Cr_i^N$$

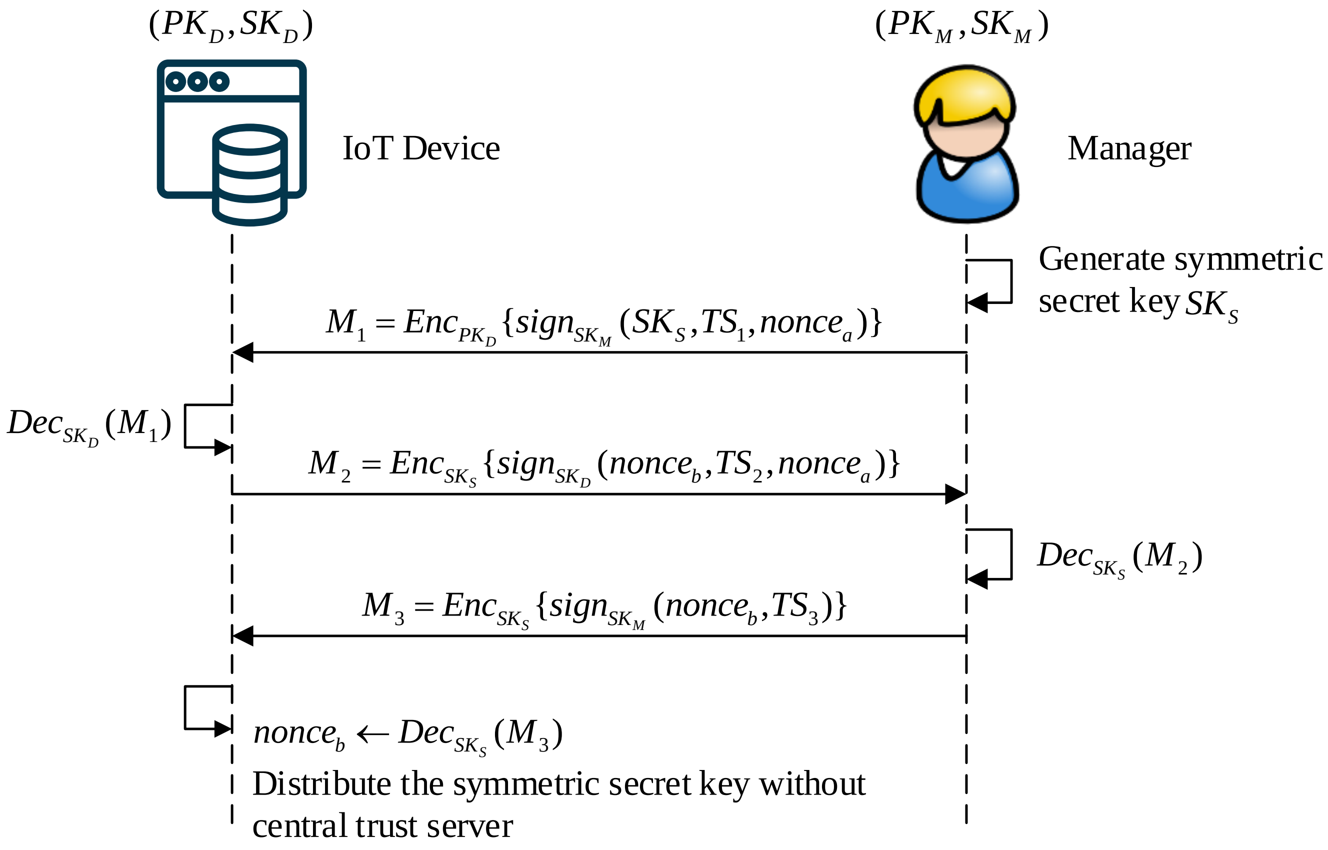
Main Challenges

- The conflicts between high concurrency and low throughput
  - We explore a DAG-structured blockchain based solution
- The trade-off between efficiency and security
  - We design a moderate-cost credit-based PoW mechanism
- The coexistence of transparency and privacy

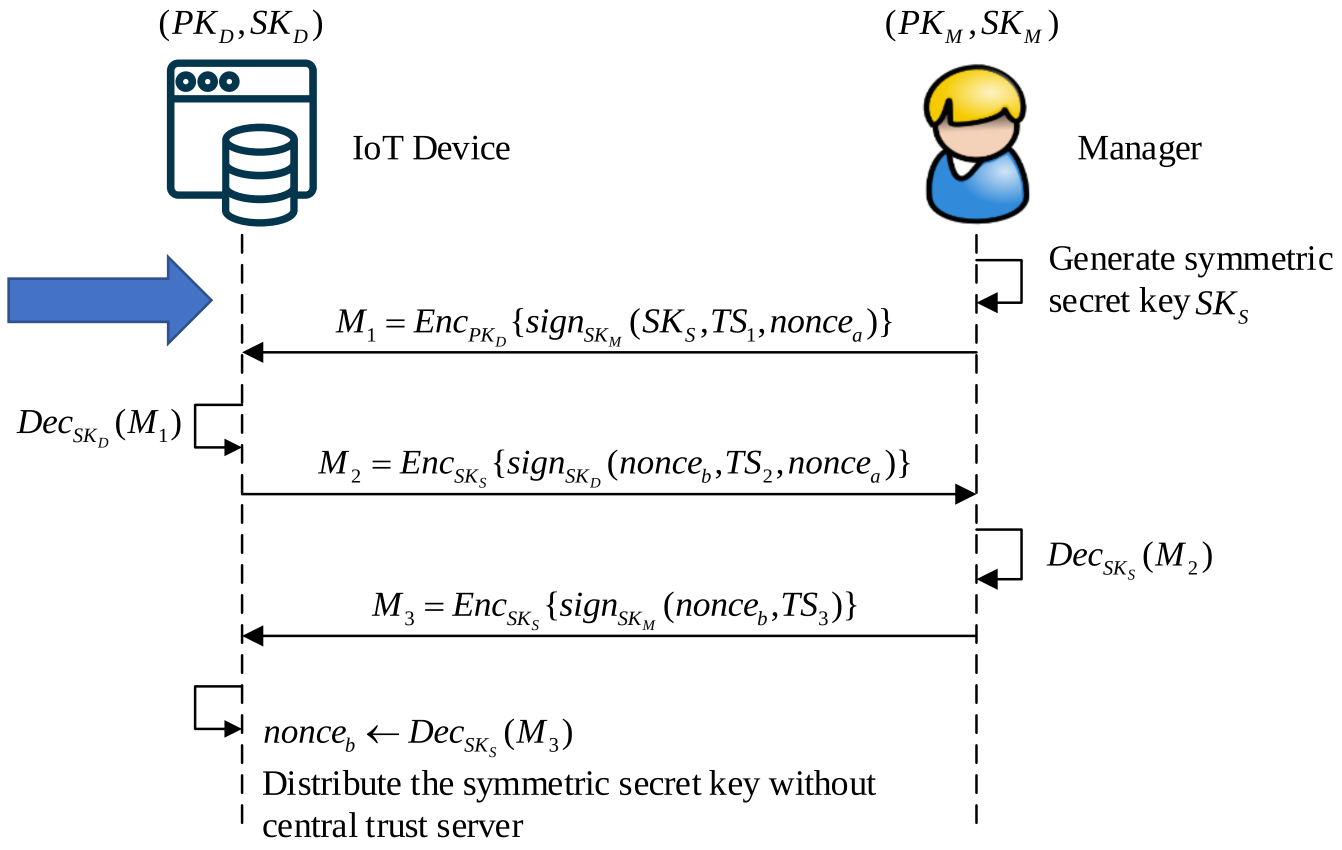
Main Challenges

- The conflicts between high concurrency and low throughput
  - We explore a DAG-structured blockchain based solution
- The trade-off between efficiency and security
  - We design a moderate-cost credit-based PoW mechanism
- The coexistence of transparency and privacy
  - We propose an efficient data authority management method

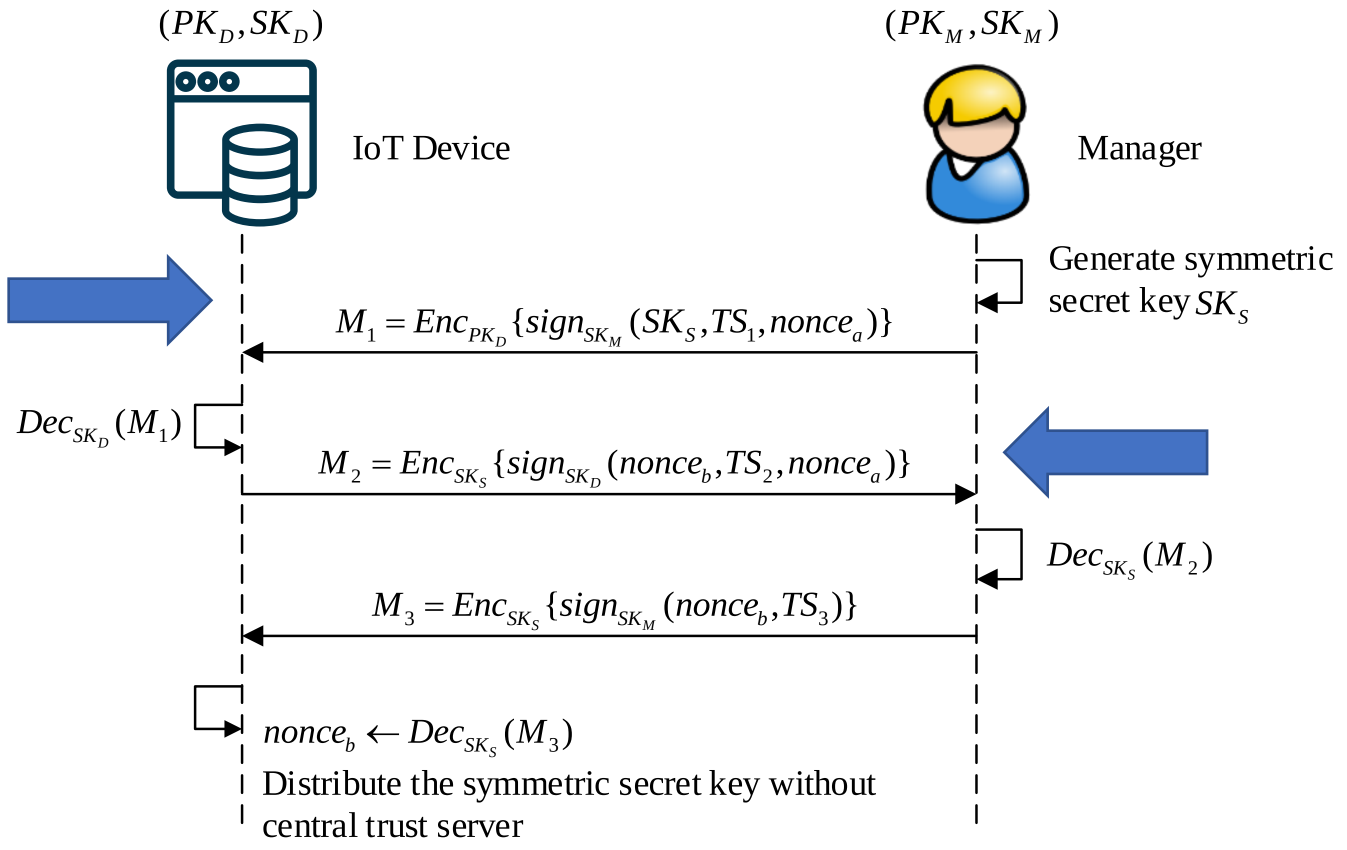
Data Authority Management Method



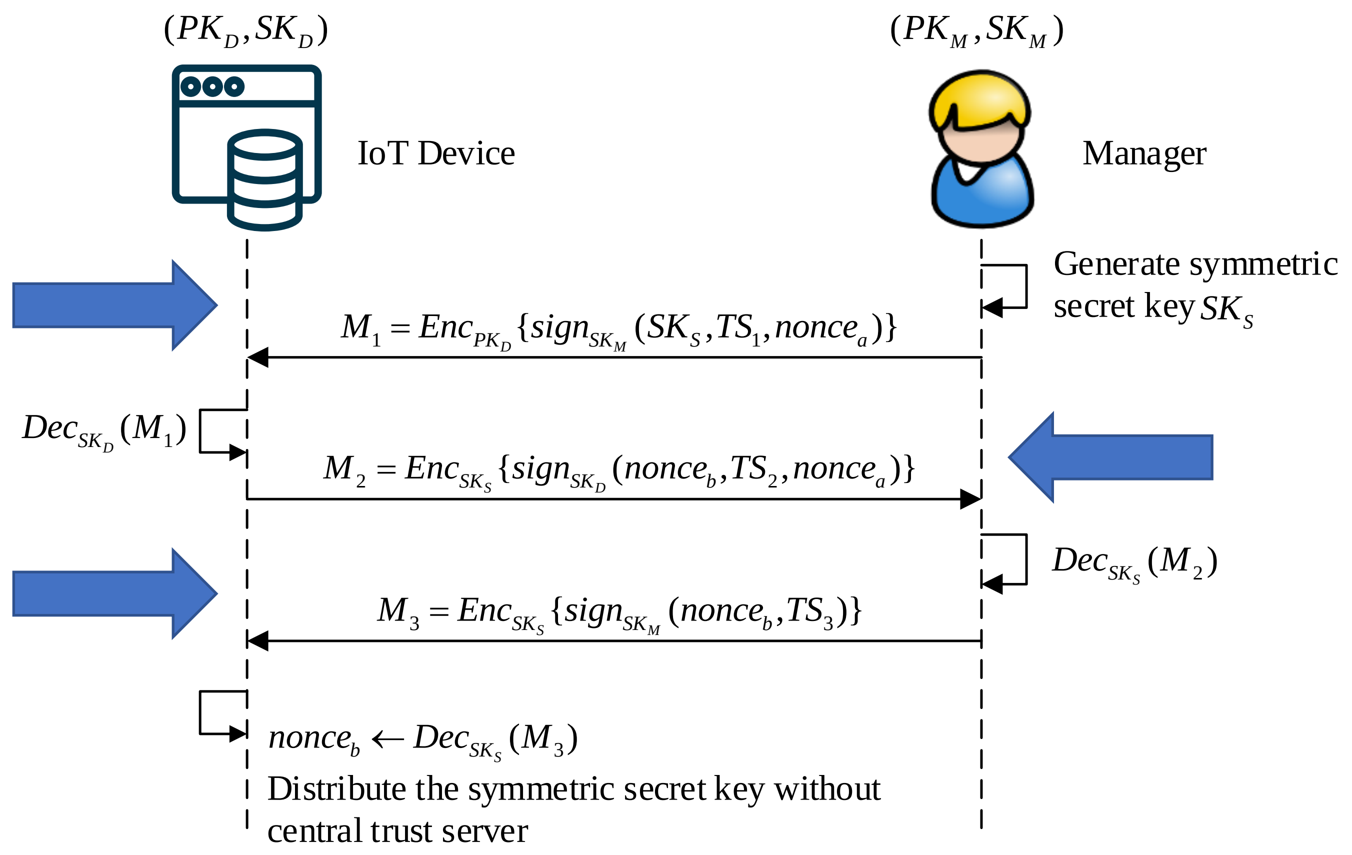
Data Authority Management Method



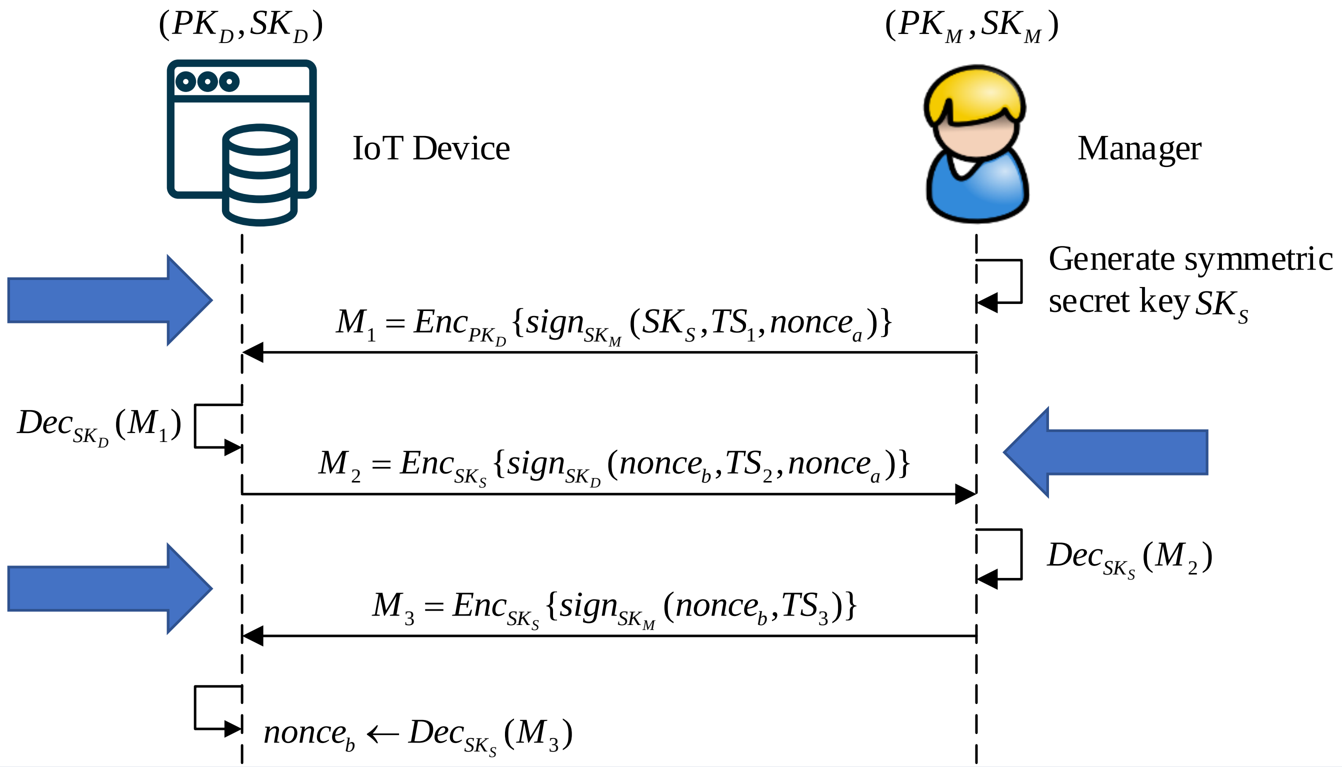
Data Authority Management Method



Data Authority Management Method



Data Authority Management Method

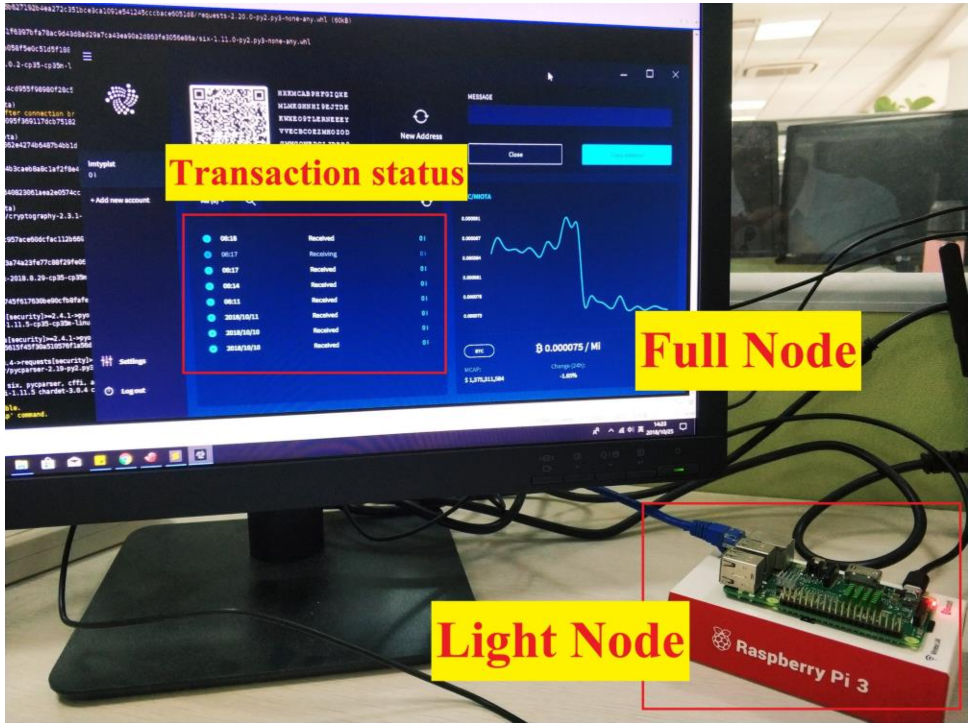


Distribute the symmetric secret key without the central trust server

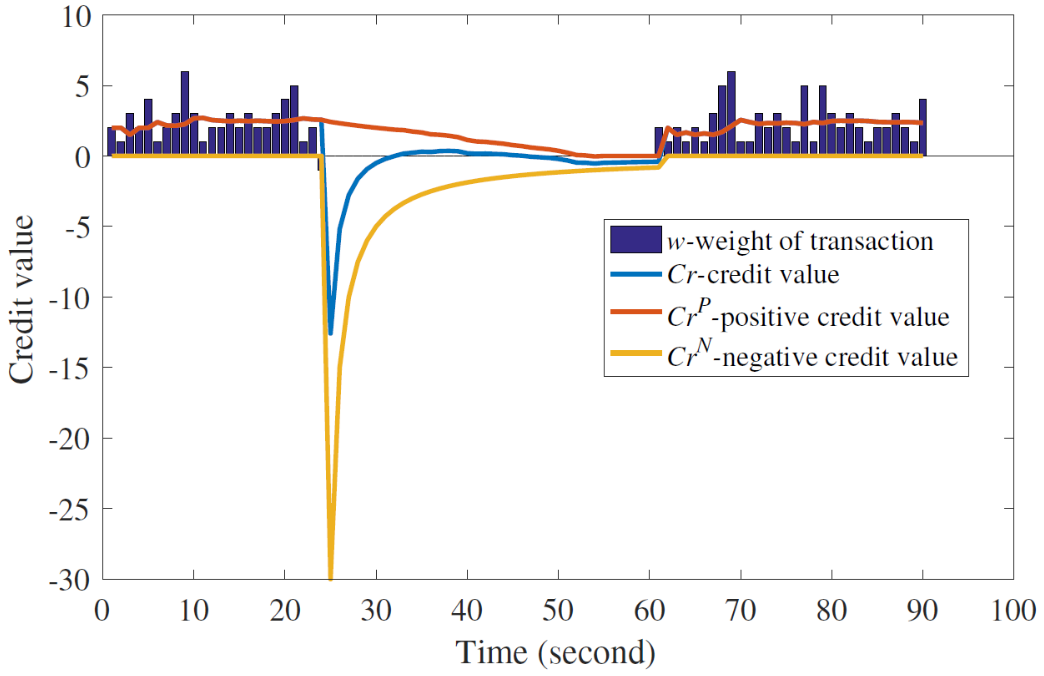
Implementation

- Full nodes: manager & gateway
  - commercial computer
  - implemented based on IRI
  - SHA-256 & AES encryption

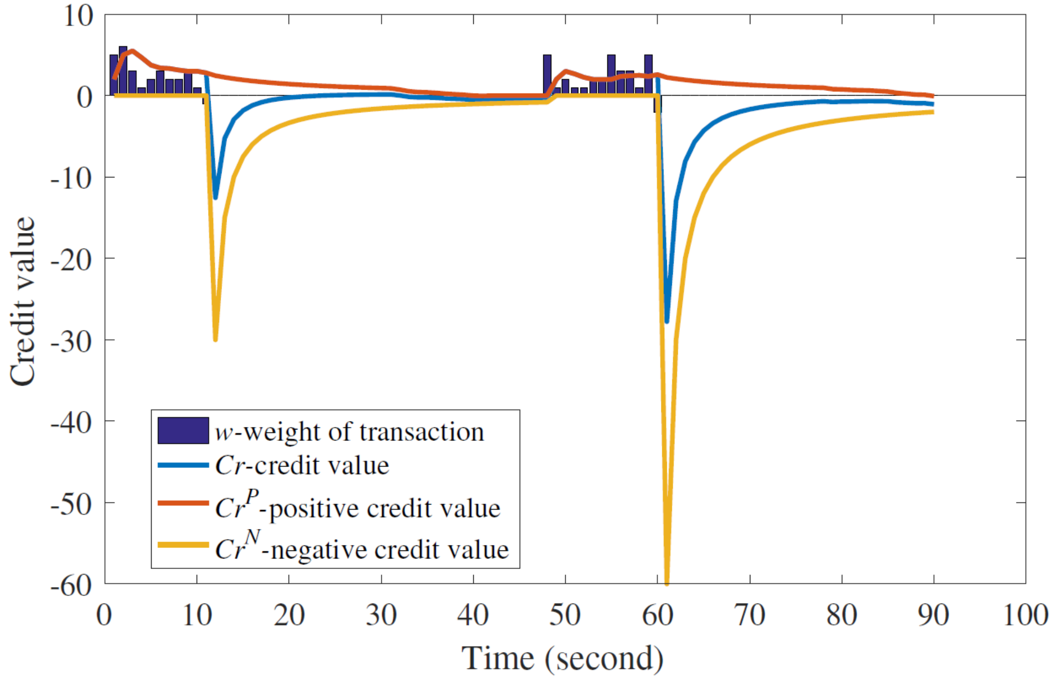
- Light nodes: IoT devices
  - Raspberry Pi Model 3B
  - implemented based on PyOTA
  - Extended with local PoW
  - AES encryption



Performance in Credit-Based PoW

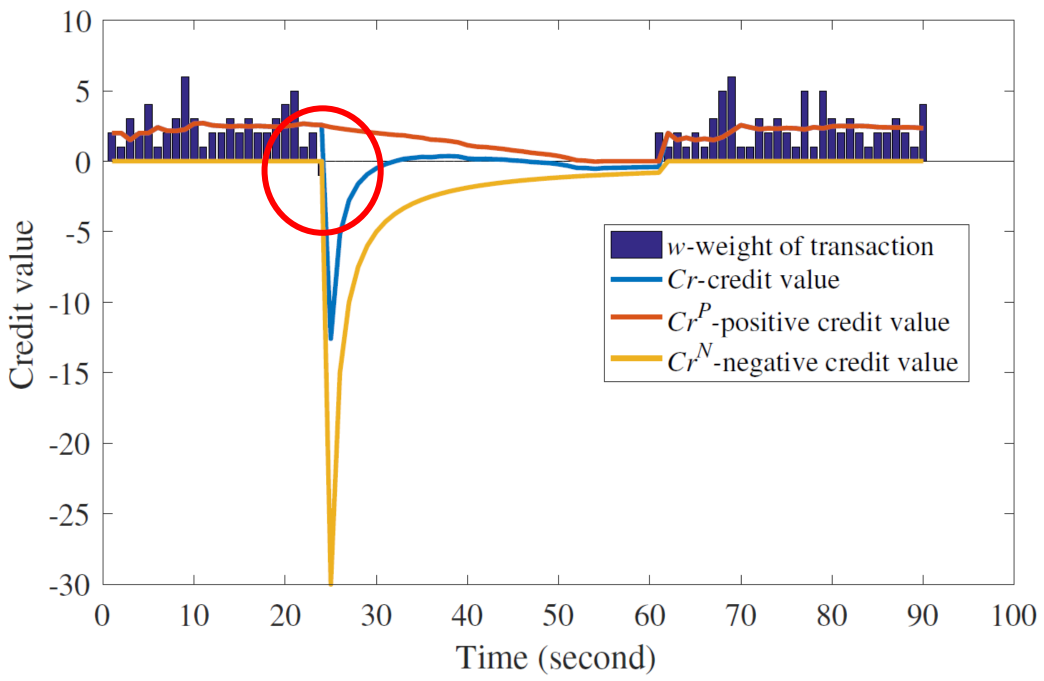


When one malicious attack happens

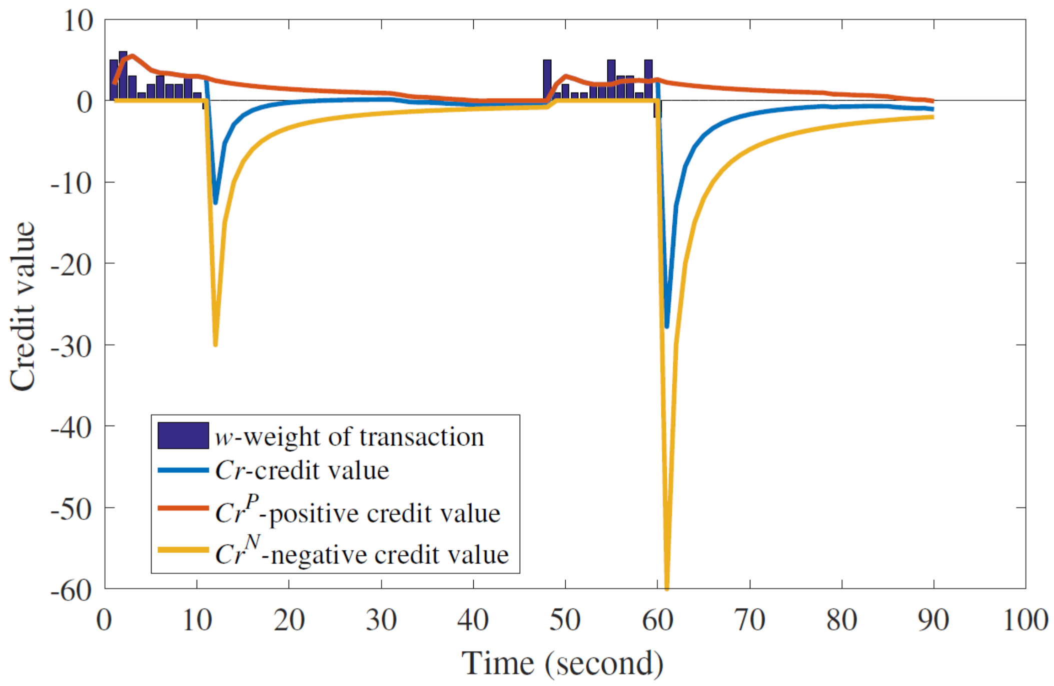


When two malicious attacks happen

Performance in Credit-Based PoW

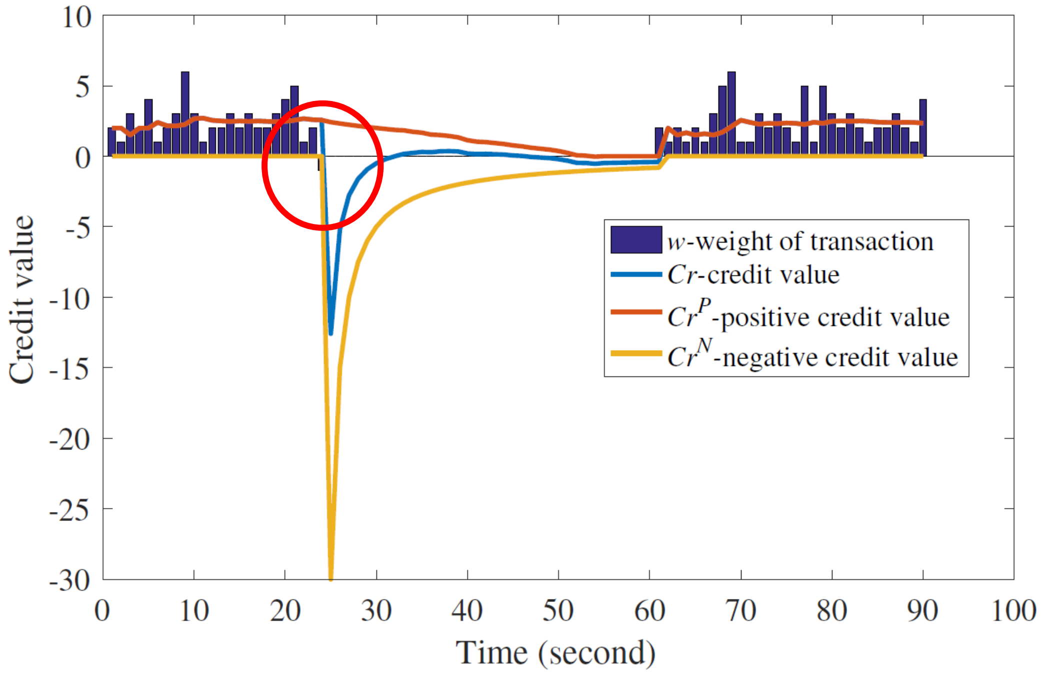


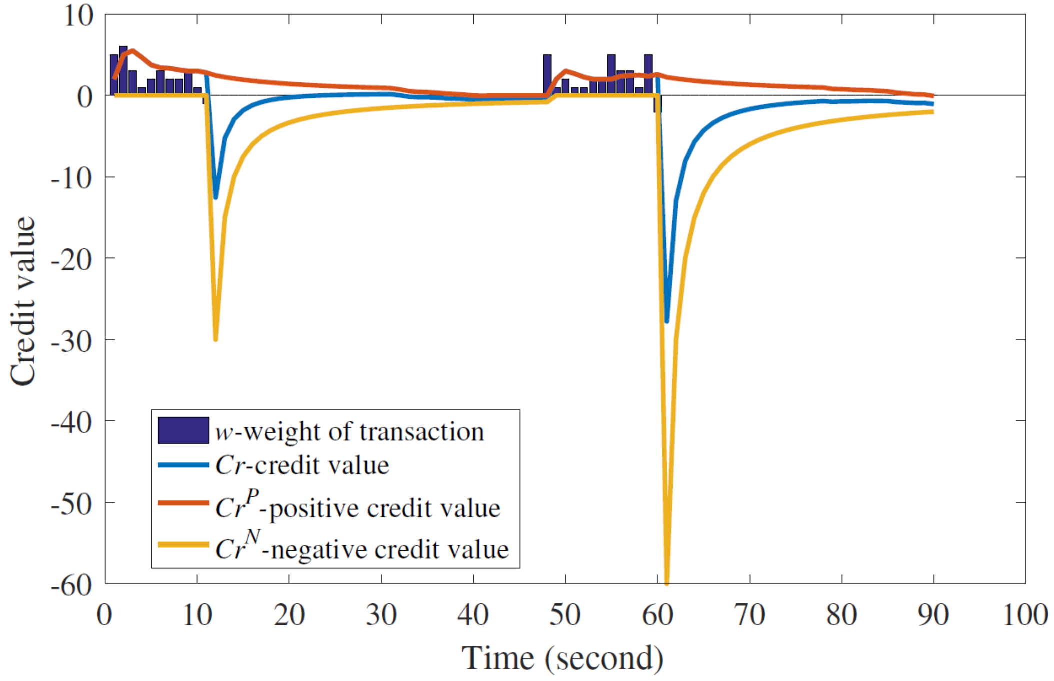
When one malicious attack happens



When two malicious attacks happen

Performance in Credit-Based PoW

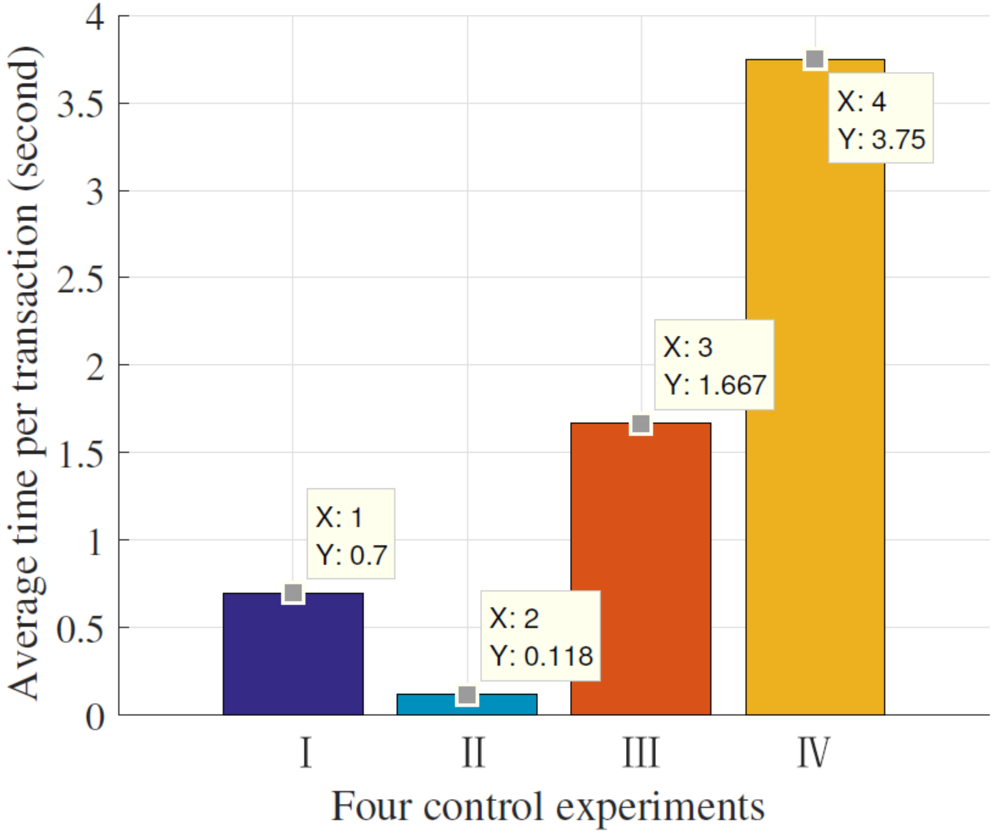




It will take longer time to recover normal transaction rate if the node conducts malicious attacks twice or more

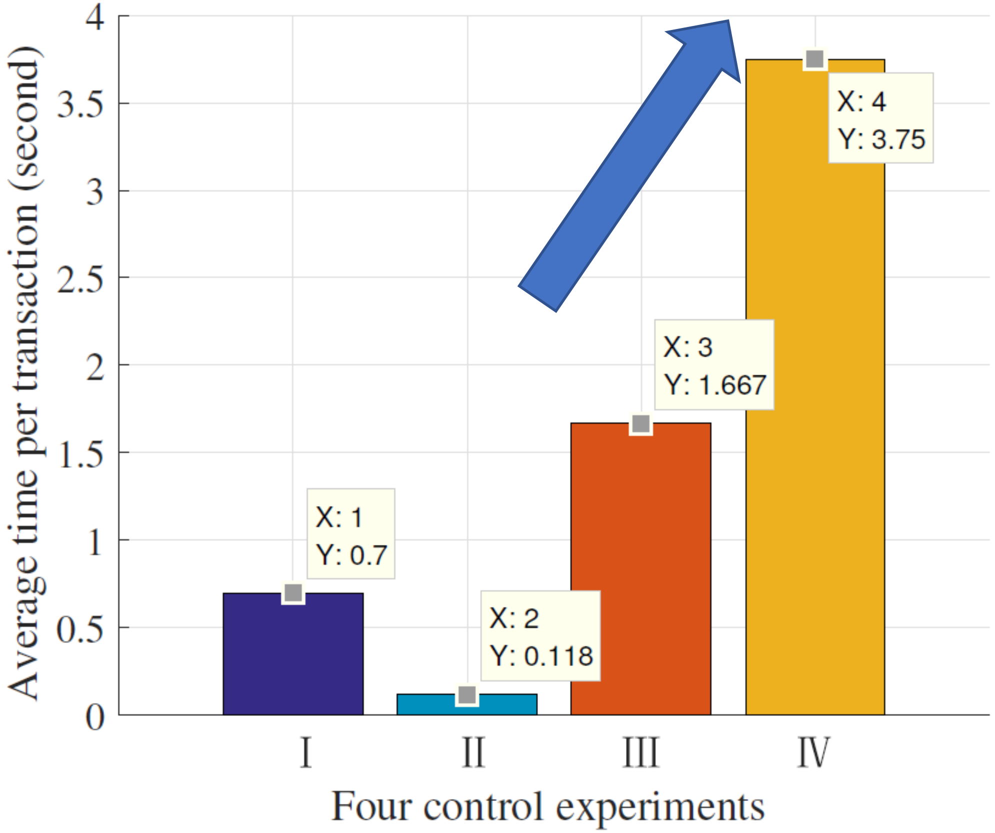
Performance in Credit-Based PoW

- Four control experiments:
  - PoW
  - Cr-PoW w/o malicious attacks
  - Cr-PoW with a malicious attack
  - Cr-PoW with two malicious attacks



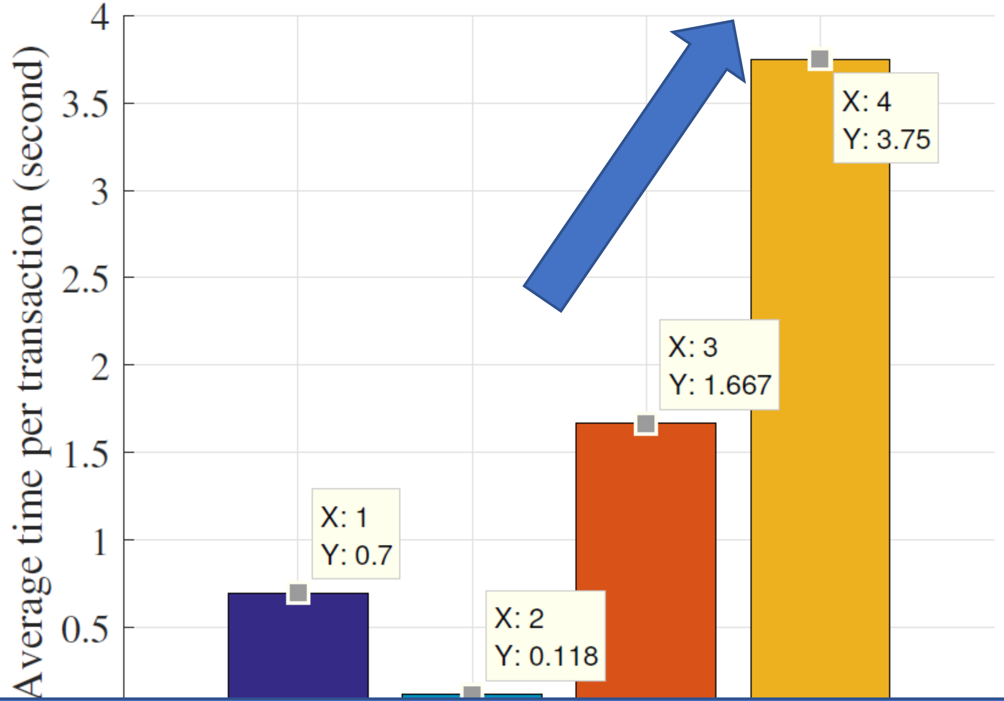
Performance in Credit-Based PoW

- Four control experiments:
  - PoW
  - Cr-PoW w/o malicious attacks
  - Cr-PoW with a malicious attack
  - Cr-PoW with two malicious attacks



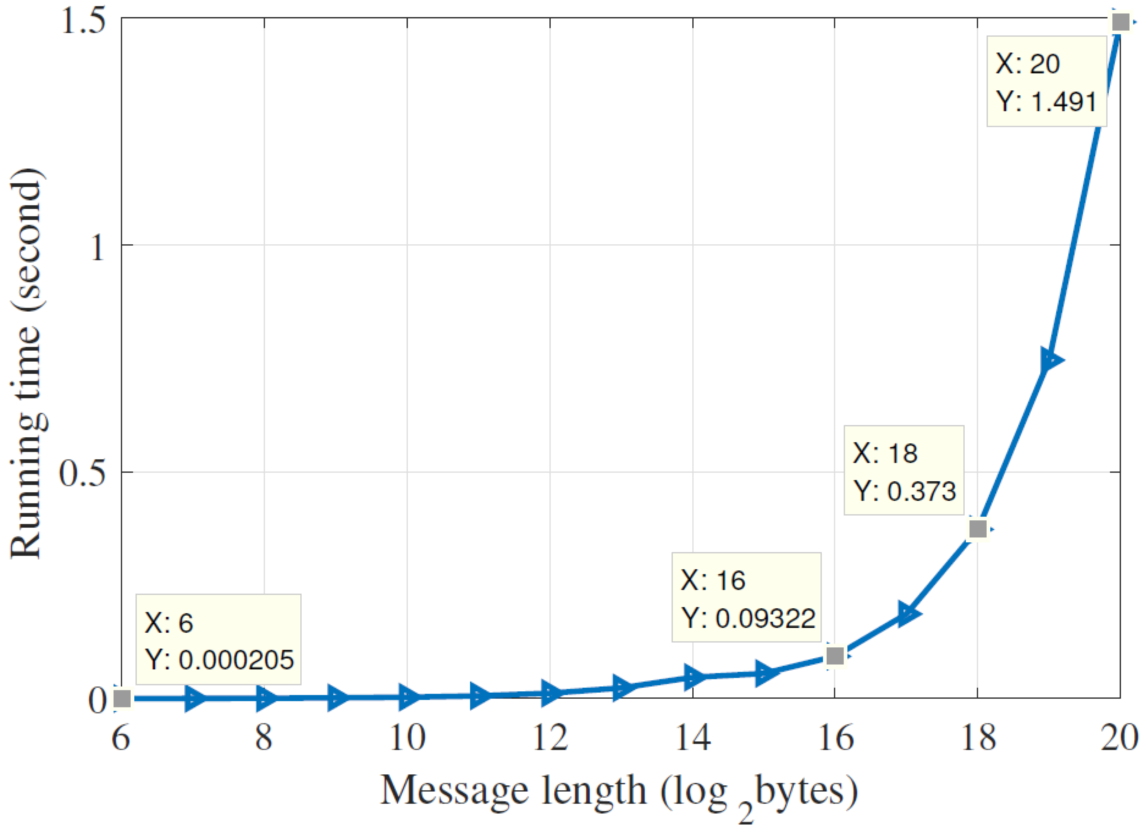
Performance in Credit-Based PoW

- Four control experiments:
  - PoW
  - Cr-PoW w/o malicious attacks
  - Cr-PoW with a malicious attack
  - Cr-PoW with two malicious attacks

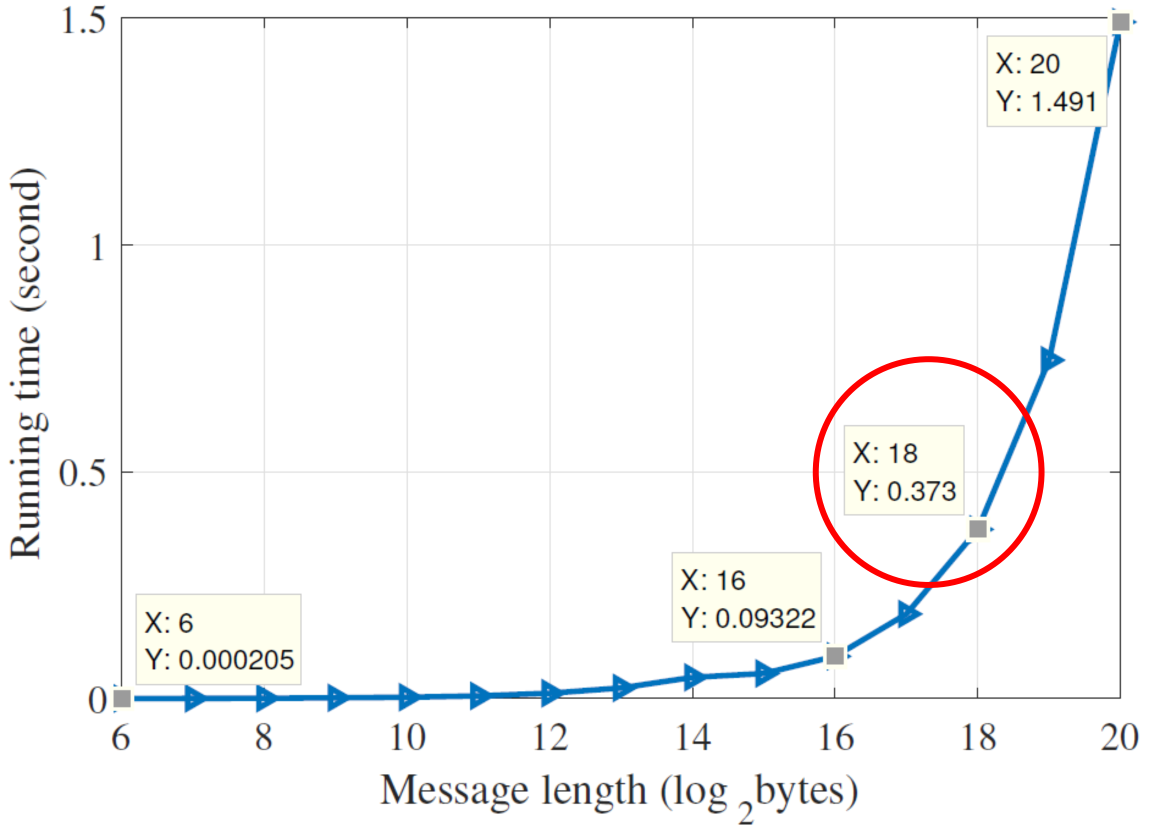


Credit-based PoW can speed up transactions for honest nodes, also can defend malicious attacks efficiently

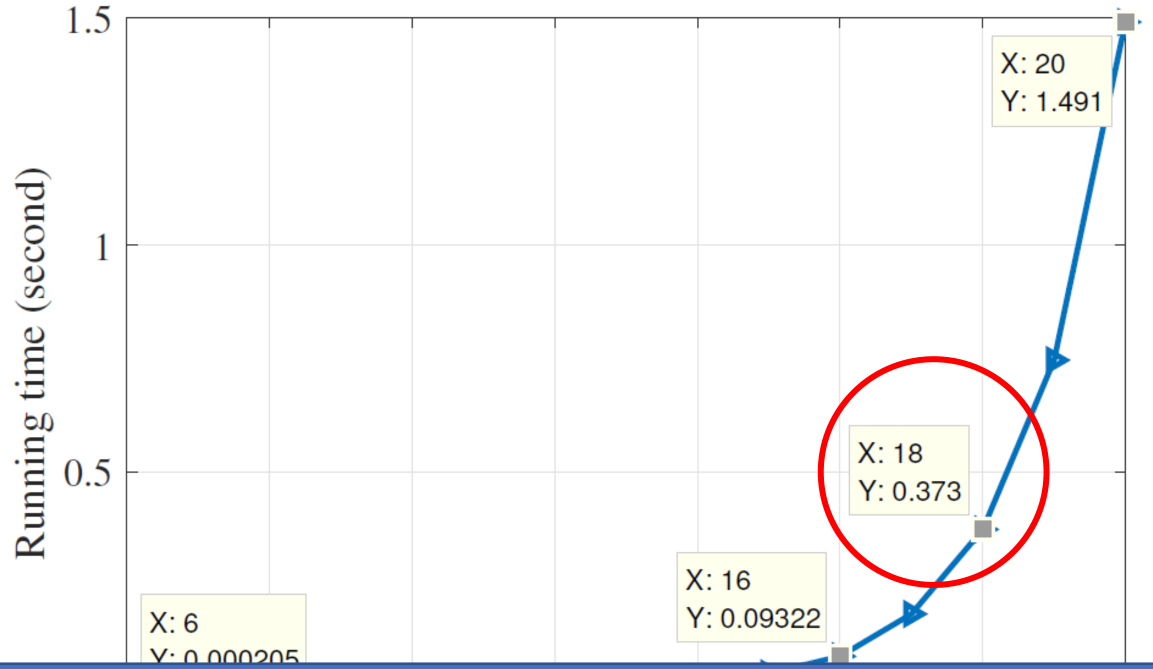
Efficiency of Data Authority Management



Efficiency of Data Authority Management



Efficiency of Data Authority Management



The data authority management method has tiny impact on the whole transaction process

Conclusion & Thank you!

- A general DAG-structured blockchain-based IoT system to address aforementioned challenges for IoT
- The credit-based PoW mechanism helps to make the blockchain more suitable for IoT systems
- The data authority management method can protect data privacy without affecting the system performance
- Future directions:
  - sensor data quality control
  - storage limitations