A blockchain-based decentralized efficient investigation framework for IOT digital forensics

Ramesh Adhikari

School of Computer and Cyber Sciences
Augusta University
Augusta, GA, USA

August 12, 2023

IOT digital forensics

- IoT forensics is the practice of analyzing IoT devices to investigate crimes
- Devices includes: Sensors, Smart home, smart car, smart phone computers
- Goal is to investigating whether
  - hackers used internet-connected devices to commit cybercrimes
  - or examining the source of a security breach

Problem statement

- Existing digital forensic tools, frameworks, and processes fail to address the heterogenous and distributed nature of the IoT ecosystem.

- Challenge for digital forensic investigators and law enforcement agencies

- Centralized data storage

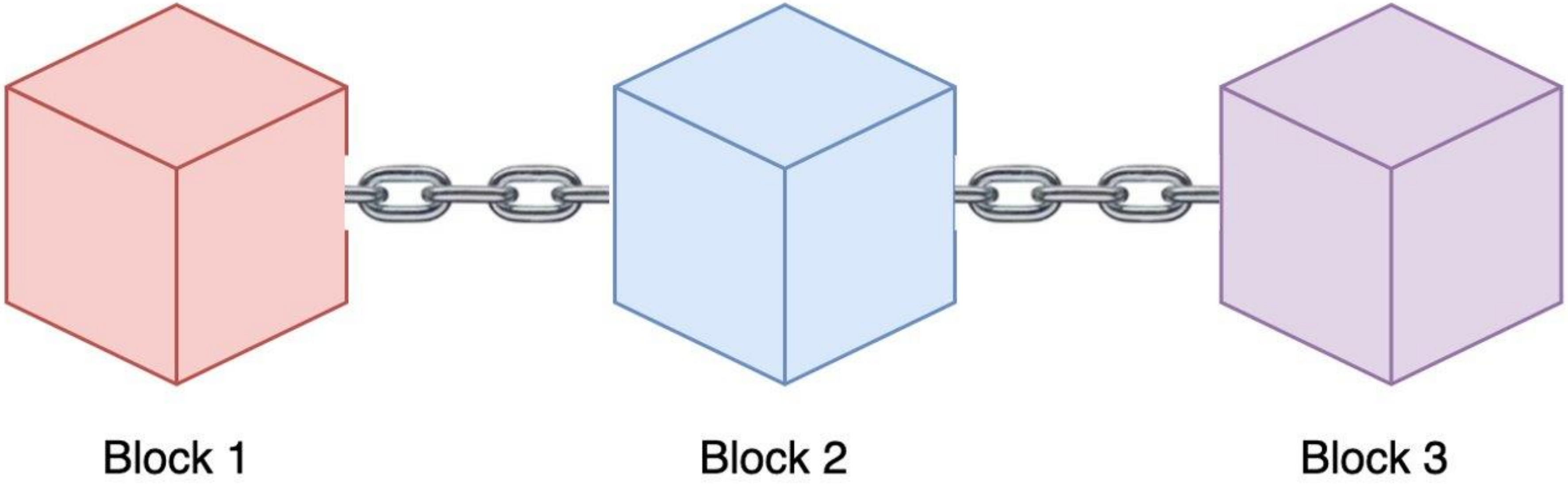
- Risk of data bridge through various networks, devices, and communication routes.

Proposed Solution

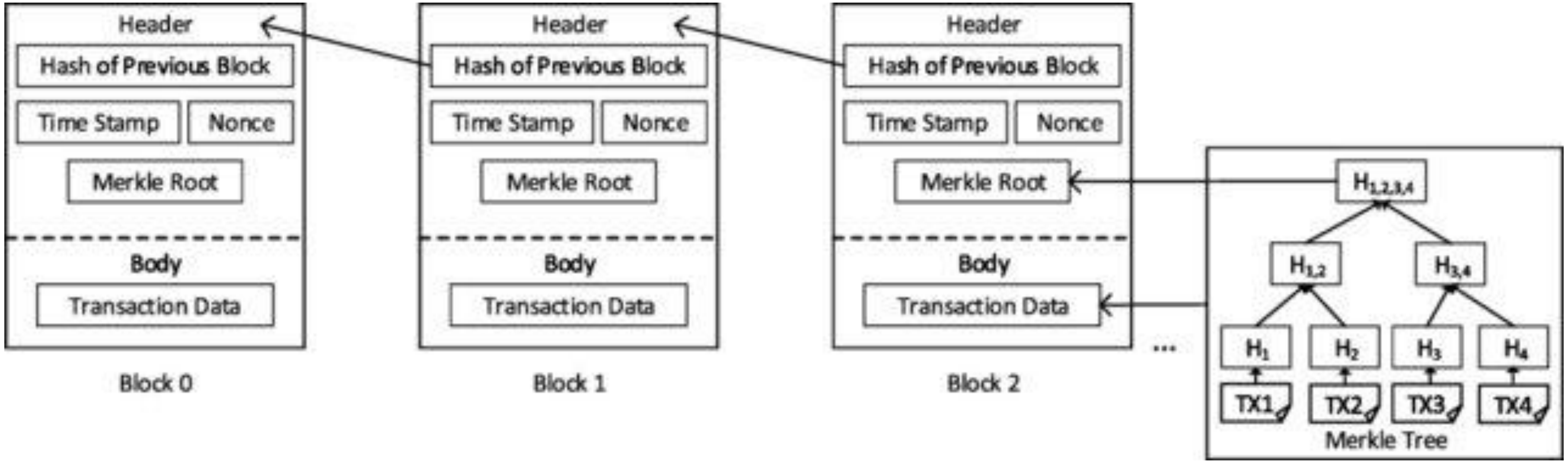
- Digital forensics framework based on the blockchain technology
- All communications of IoT devices are stored in the blockchain as transactions
- Blockchain ensures data integrity, security, immutability, and decentralization
- Blockchain enable transparent confirmation of forensic investigation processes

Blockchain

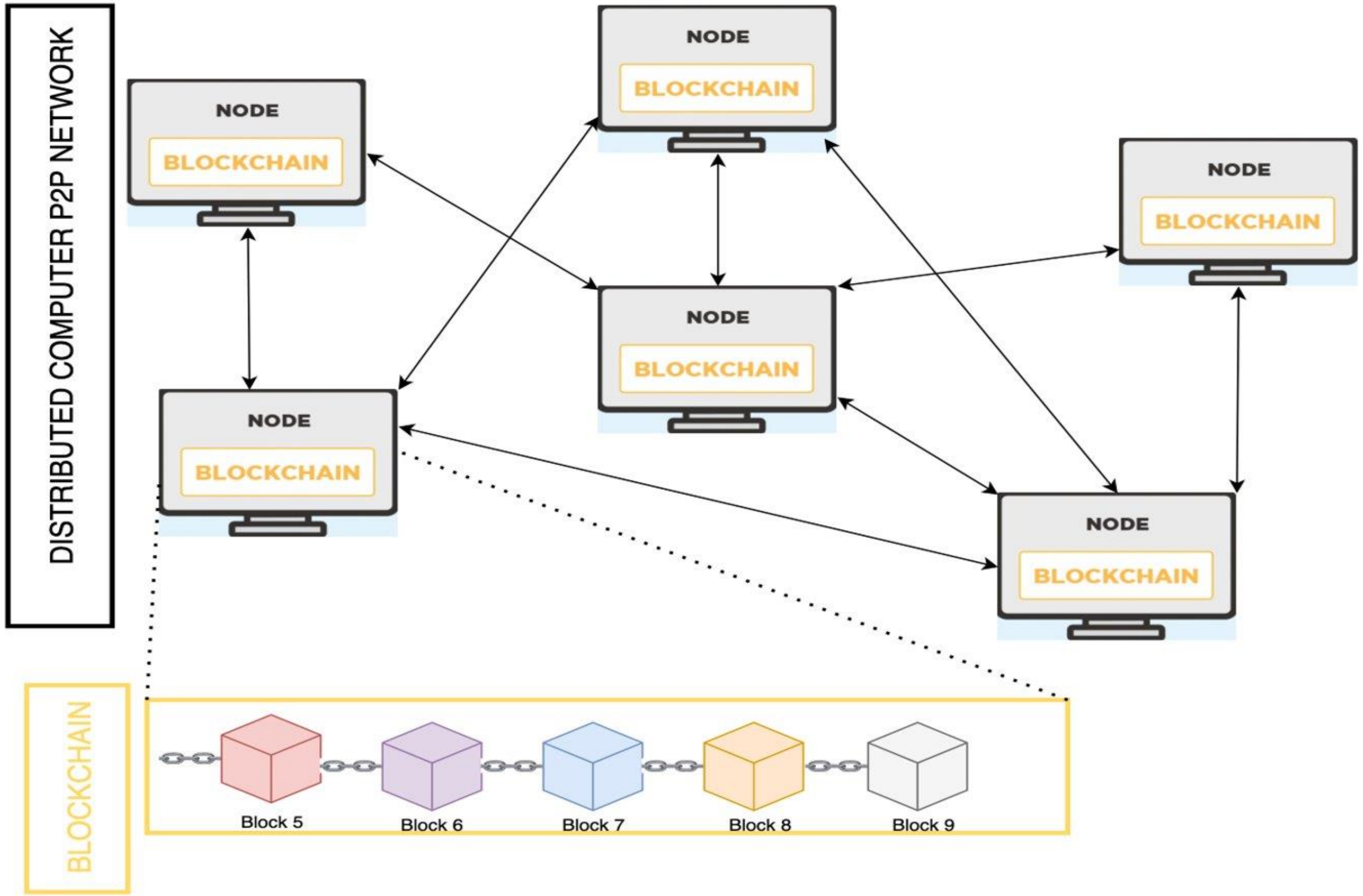
- Blockchain is a chain of Block which records transactions
- It is decentralized and unchangeable public ledger



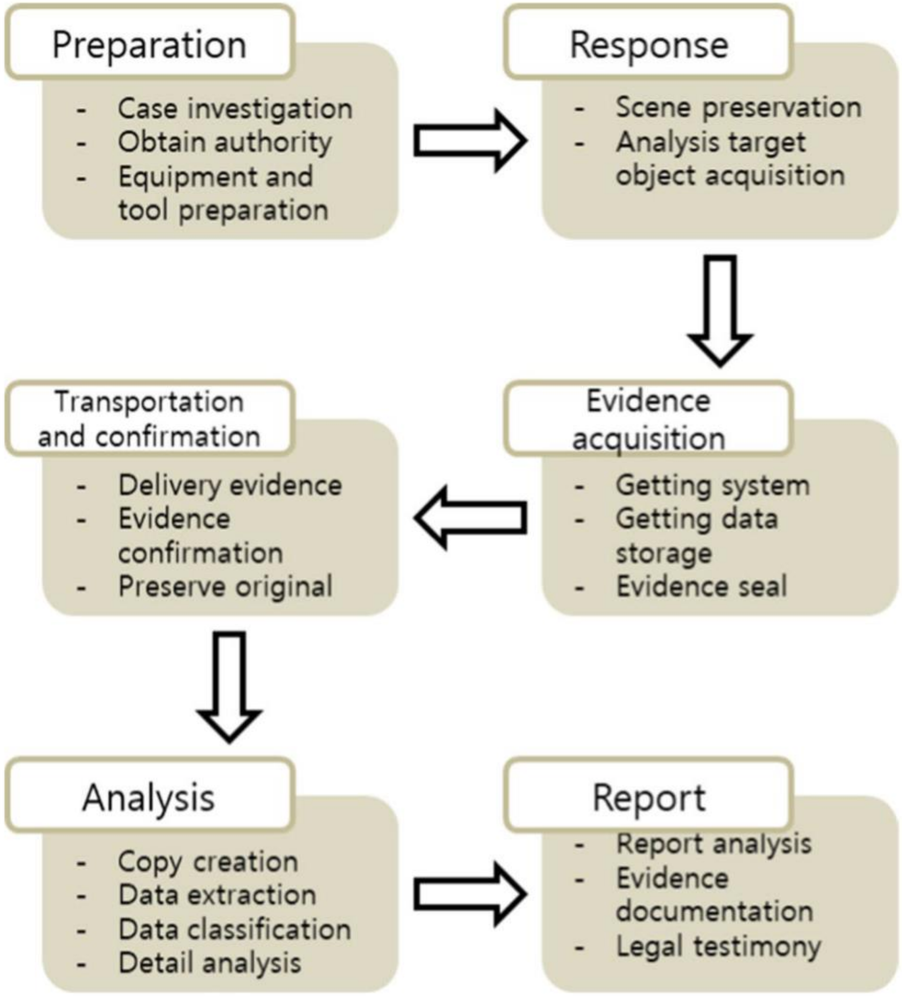
Blockchain structure



Blockchain Architecture



Existing digital forensic process



Preparation

- Case investigation
- Obtain authority
- Equipment and tool preparation

Response

- Scene preservation
- Analysis target object acquisition

Evidence acquisition

- Getting system
- Getting data storage
- Evidence seal

Transportation and confirmation

- Delivery evidence
- Evidence confirmation
- Preserve original

Analysis

- Copy creation
- Data extraction
- Data classification
- Detail analysis

Report

- Report analysis
- Evidence documentation
- Legal testimony

Category of Digital forensic in IoT

- **Cloud Forensics:** Focuses on cloud-based devices sharing data, often targeted by cybercrime due to data centralization.

- **Network Forensics:** Investigates abnormal attack logs across various networks (home, industrial, LAN, Internet).

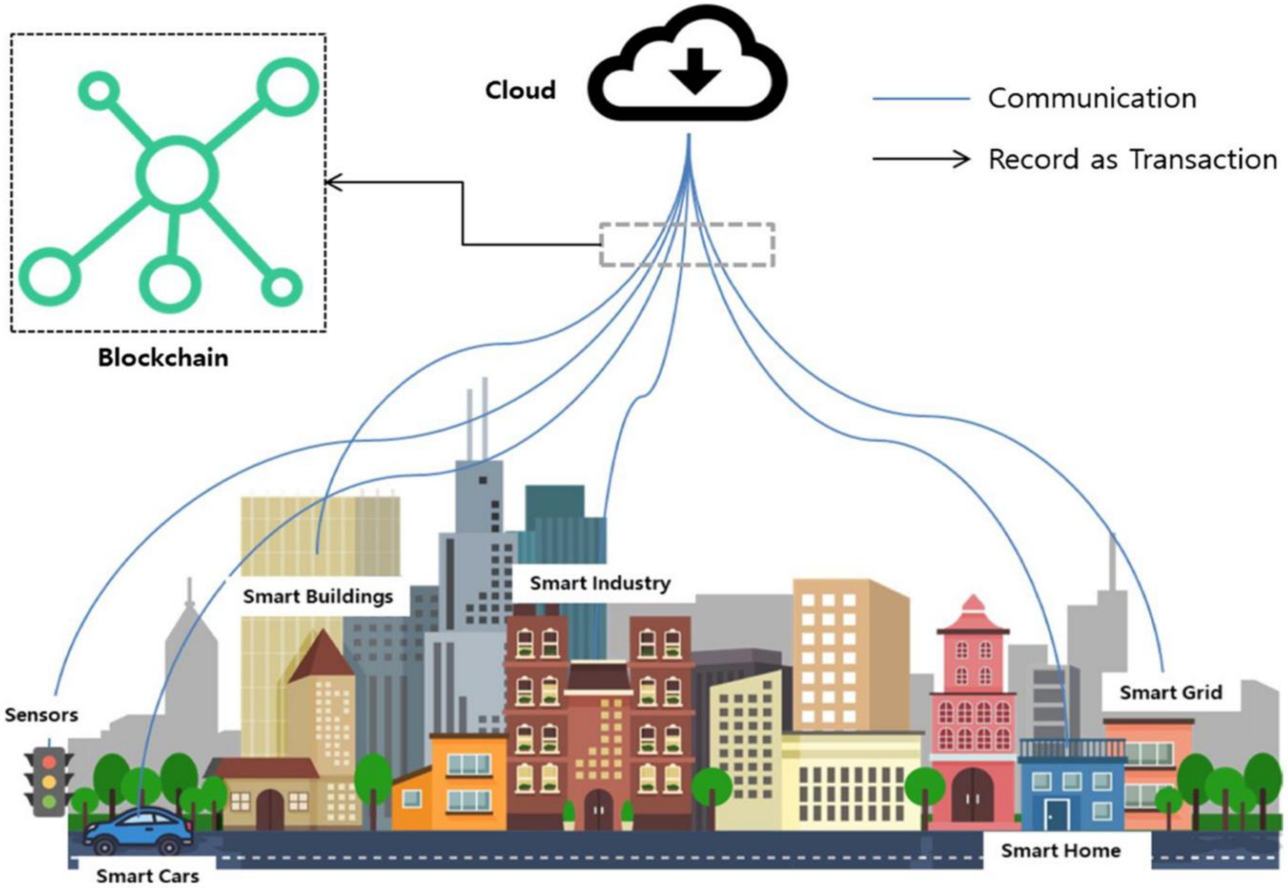
- **Device Forensics:** Collects digital evidence (video, audio, memory) from physical IoT devices.

Proposed framework

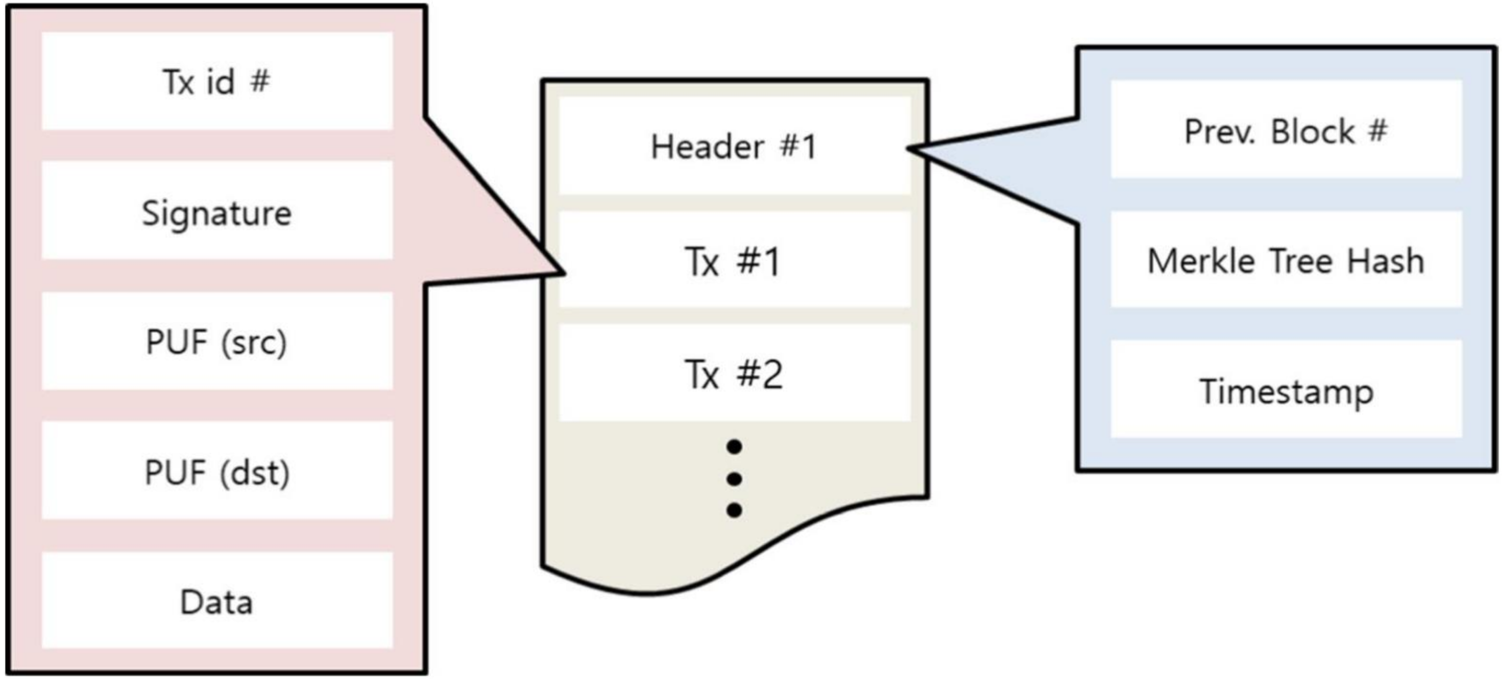
IoT devices store generated and communicated data in blockchain as transactions.

Divided into three layers:

1. Cloud
2. Blockchain
3. IoT devices



Block structure of proposed framework



Blocks are divided into two sections: **block header** and **transaction**

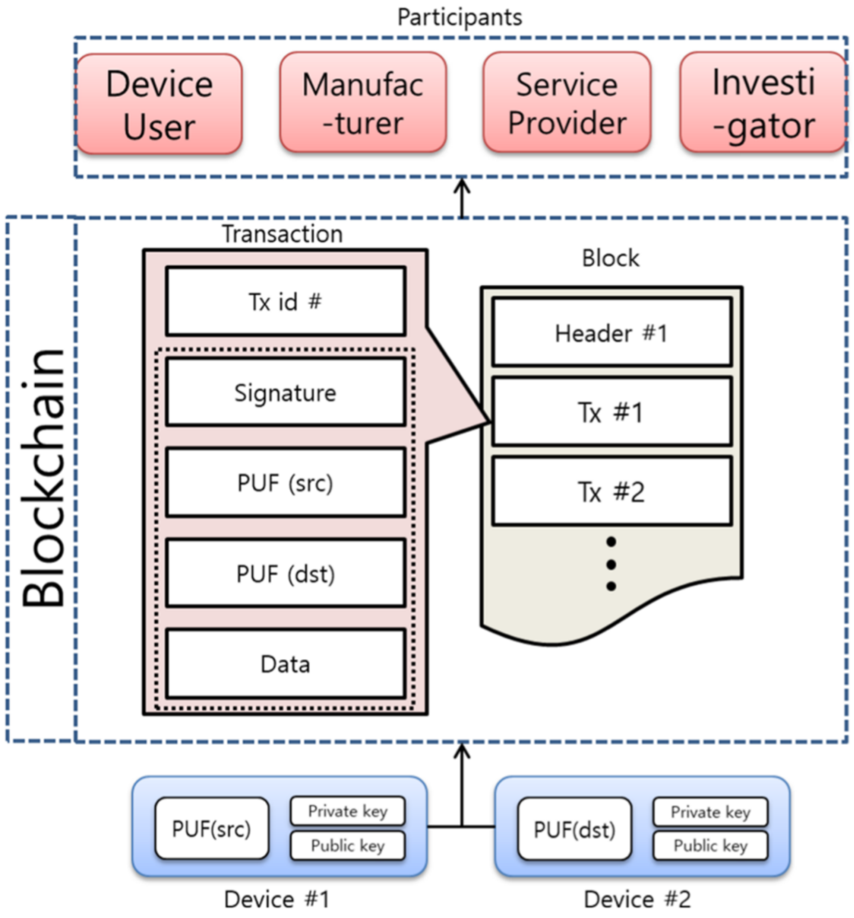
Participants of blockchain

proposed digital forensics framework is divided into four categories

- IoT device user
- IoT device manufacturer
- Service provider.
- Investigator

Workflow of proposed framework

- **Device Layer:**
  - IoT devices communicate and exchange data.
- **Blockchain Layer:**
  - Blocks generated from communication data of IoT devices.
  - Transaction details: sender/receiver PUF IDs, data, digital signature.
- **Participants' Layer:**
  - Device users, manufacturers, service providers, investigators.
  - Open ledger allows verification of data integrity.



Benefits of Proposed system

- Distributed and Secure

- Enhances integrity and transparency of transmitted IoT data.

- Reduces resources for demonstrating data integrity and transparency.

Experimental evaluation

- Ethereum private blockchain used for experiment

- Figure shows gas consumption with respect to the size of the blocks and number of transactions.

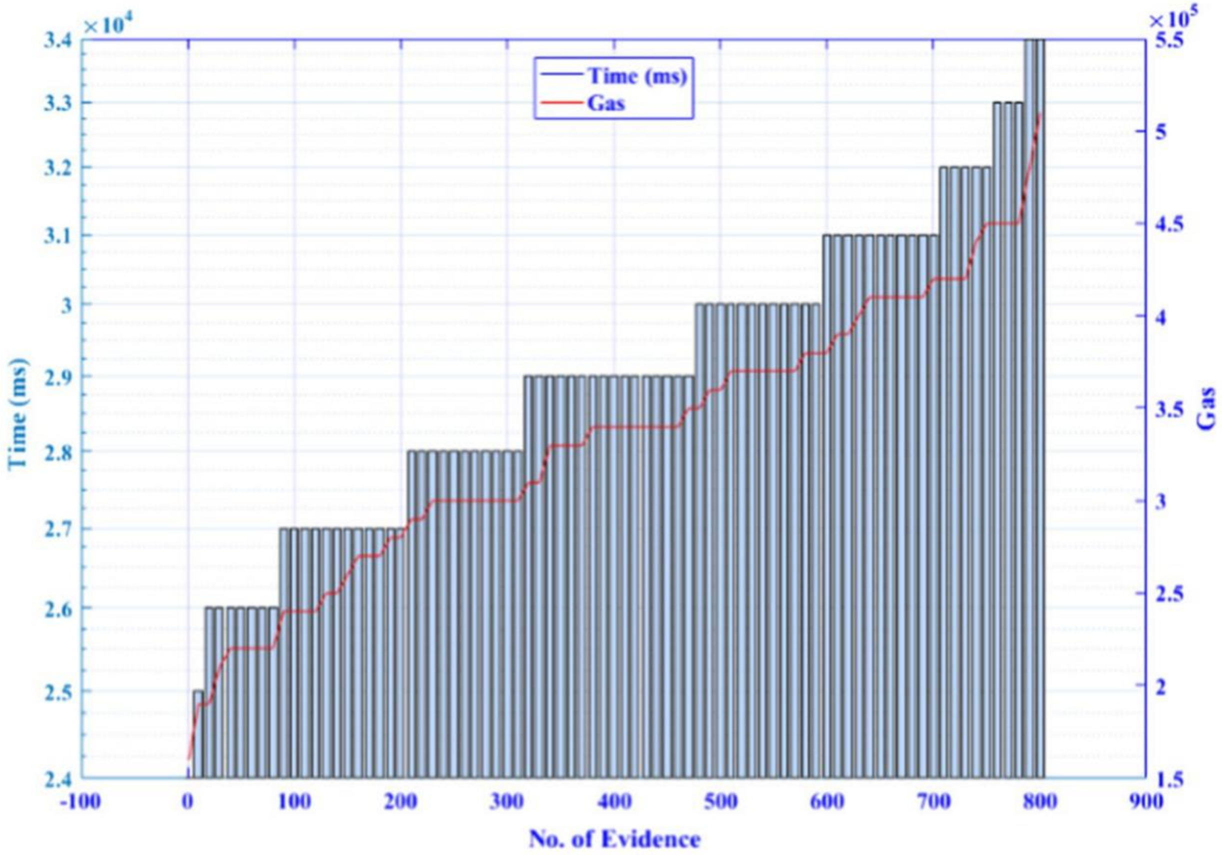


Fig. 5 Gas consumption with respect to execution time and number of transactions

Experimental evaluation

Figure 6 shows the relationship between throughput and the number of evidence generated.

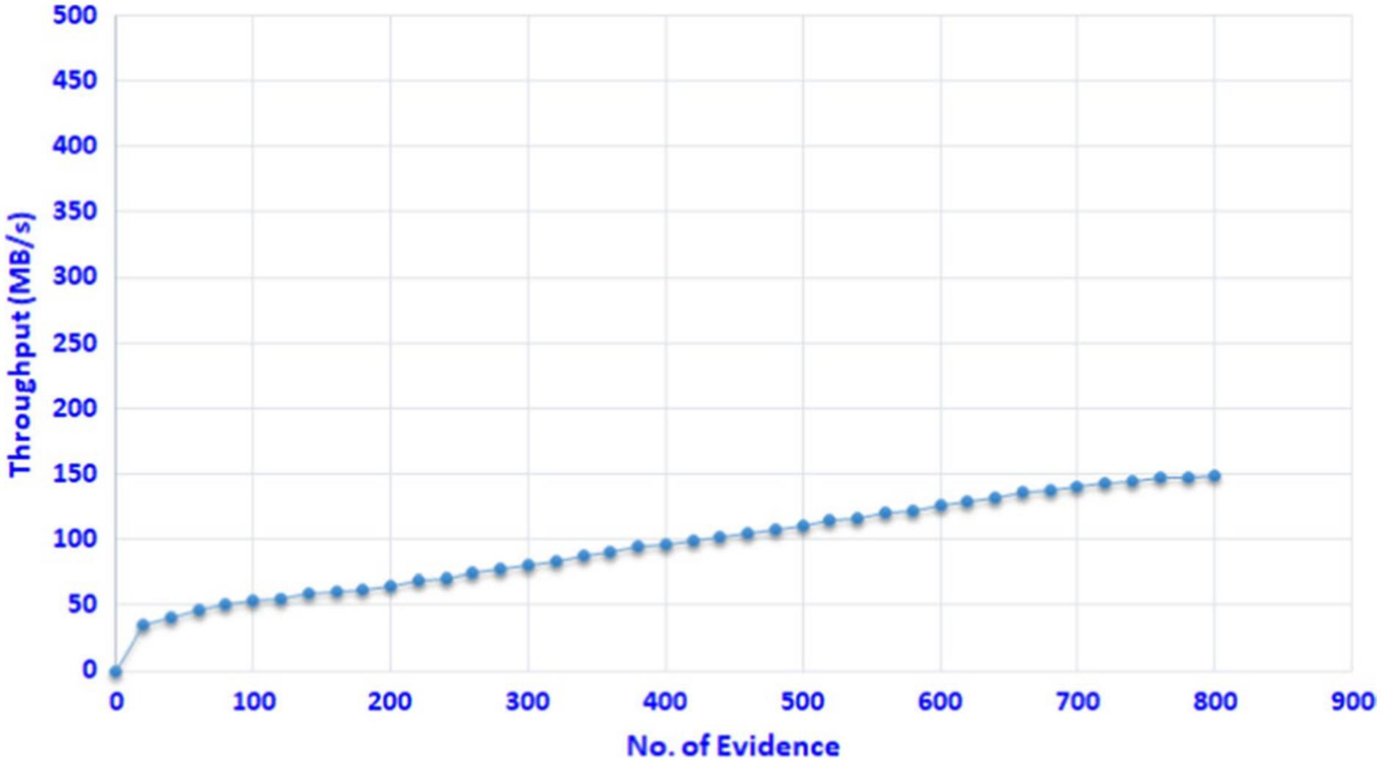


Fig. 6 Throughput with respect to the number of evidence

Experimental evaluation

Figure 7 shows the CPU utilization varies with the number of evidence generated.

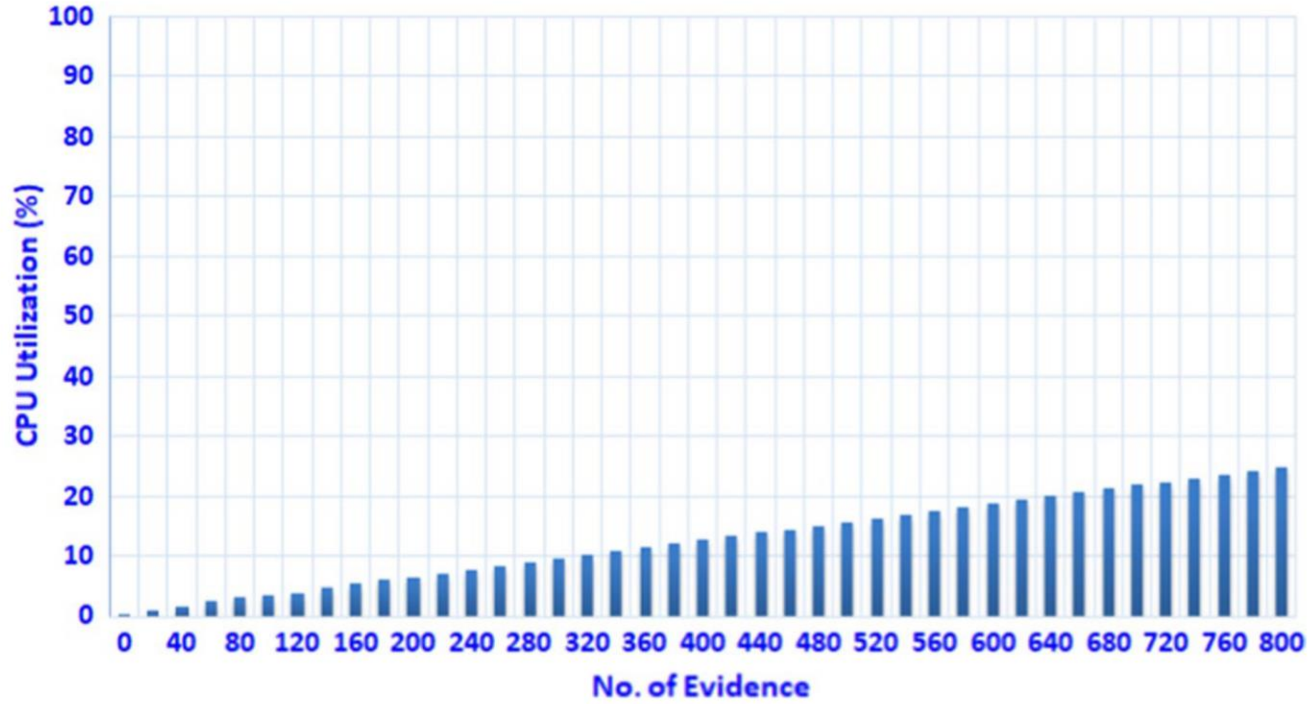


Fig. 7 CPU utilization with respect to the number of evidence

Conclusion

- Current forensics rely on central authorities (e.g., Prosecutors' Office, Police) for data integrity.
  - While efficient, this approach risks compromise due to malicious attacks.
  - Improving digital forensics in big IoT setups requires stronger protection for data security

- Proposed blockchain-based framework for IoT forensics to address IoT environment challenges and centralization issues.
  - Use Blockchain to ensure
    - Data security, decentralization, transparency and integrity

Thank you!

Questions?