Blockchain, IoT, and Cyber Security

Presented by Ahmed Lekssays
University of Insubria in Varese, Italy

RAIS Online Seminars - May 21, 2020

Outline

1. Introduction to Blockchain
2. Blockchain and IoT
3. Applications of Blockchain in Security
    a. Access Control
    b. Data Privacy
    c. Malware Detection
4. Final Thoughts

Introduction to Blockchain

Overview

“To understand the power of blockchain systems, and the things they can do, it is important to distinguish between three things that are commonly muddled up, namely the ***bitcoin currency***, the ***specific blockchain that underpins it*** and ***the idea of blockchains in general***.”

- The Trust Machine, THE ECONOMIST, Oct. 31, 2015

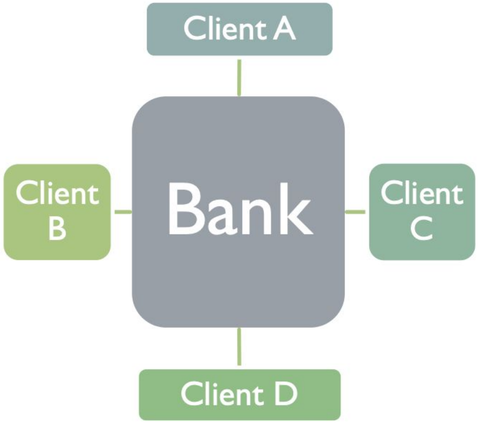
What is Blockchain?

It is a distributed ledger that:

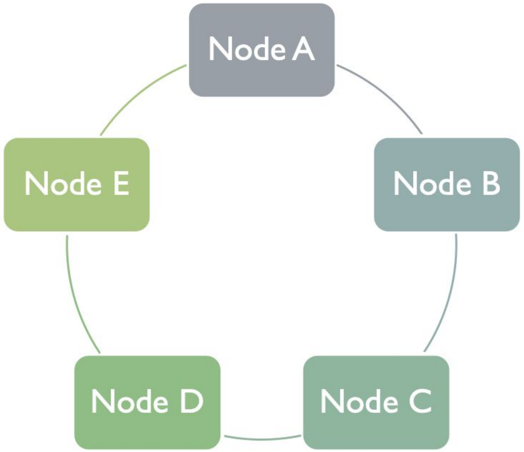
- *permits* transactions to be gathered into blocks and recorded;
- *cryptographically chains* blocks in chronological order; and
- *allows* the resulting ledger to be accessed by different servers.

What is a Distributed Ledger?

Centralized Ledger



Distributed Ledger



What is a Distributed Ledger? (Cont'd)

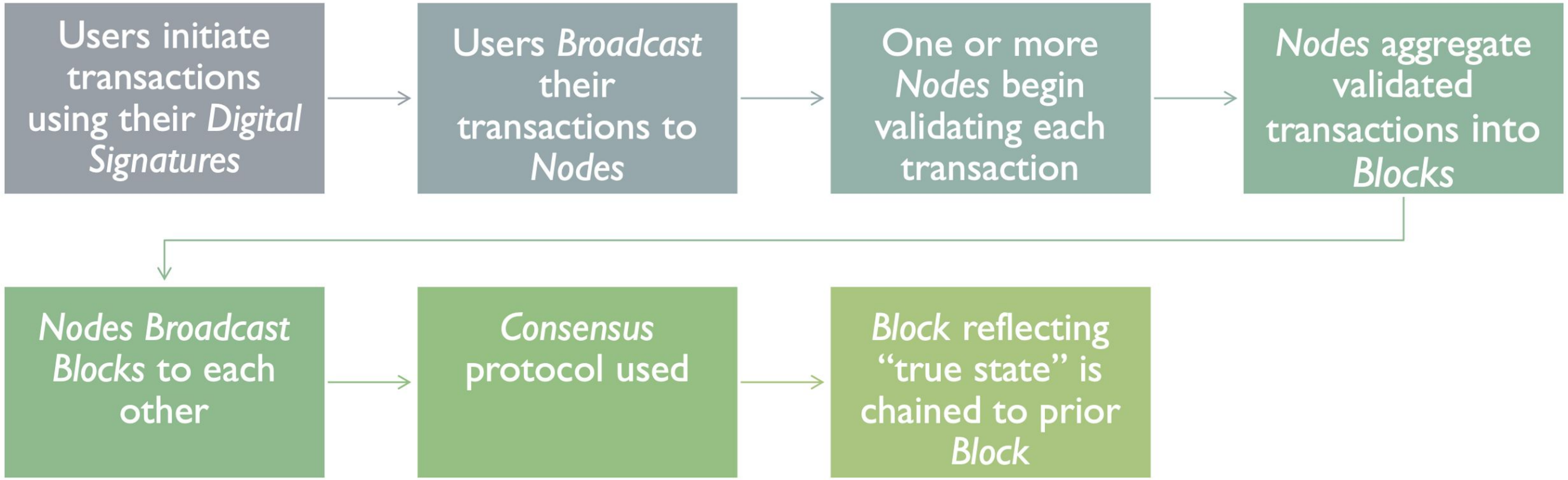
Centralized Ledger:

- There are multiple ledgers, but Bank holds the "golden record"
- Client B must reconcile its own ledger against that of Bank, and must convince Bank of the "true state" of the Bank ledger if conflicts arise

Decentralized Ledger:

- There is one ledger. All Nodes have some level of access to that ledger.
- All Nodes agree to a protocol that determines the "true state" of the ledger at any point in time. The application of this protocol is sometimes called "achieving consensus."

How does a Distributed Ledger Work?



How does Cryptography relate to Blockchain?

Initiation and Broadcasting of Transaction
(Digital Signatures, Public/Private keys)

Validation of Transactions
(Proof of Work, BFT...)

Chaining Blocks
(hash functions)

Types of Blockchain

Public

bitcoin

ethereum

Permissioned

HYPERLEDGER FABRIC

Consensus in Blockchain

Proof of Work

Proof of Stake

Byzantine Fault Tolerance

Transaction validation is reached through a distributed consensus protocol that, in general, is considered secure if the majority of network participants are honest.

Block Validation Transactions are inserted into blocks only if they are considered valid by the network participants

Smart Contracts

Smart contracts are autonomously-executed programs that encode predefined actions to validate a transaction

- Example: Assuming entity A has money, if it sends an amount of cryptocurrency to entity B, a smart contract is executed to deduct the amount from entity A and add it to entity B

Benefits of Blockchain

- **Decentralisation**: distributed network and the ledger is replicated in all the participating nodes.
- **Transparency**: blockchain transactions are completely transparent. Blockchain made verification of transaction further effortless through the application of Merkle Tree.
- **Security**: consensus approach, such as PoW, and longest chain rule makes the blockchain network protected from DDoS by capturing 51% or more nodes.
- **Immutability**: replica of the chain is distributed on all the nodes of the network which provides verifiability – making the chain completely immutable.

Benefits of Blockchain (Cont’d)

- **Cost:** For large scale applications, deploying blockchain could be well of legacy technologies and will need less maintenance – making blockchain an economical and affordable solution in the long run.

Blockchain and IoT

IoT Applications

7: Applications	Large pool of IoT applications	In-layer Security Blockchains Authentication & Authorization Encryption & Key Management Trust & Identity Management
6: Data Analytics & Storage	(Medical) (Institutional) Engine; Cloud (Medical) SaaS/Big Data; Internet & App Store (Medical/health Apps); Cloud Storage	In-layer Security Blockchains Authentication & Authorization Encryption & Key Management Trust & Identity Management
5: Data Centralization	Firm's Intranet; Extranet; Public Cloud; Private Cloud; Hybrid Cloud; Internet (protocols such as but not limited to IPv4, IPv6, MIPv6, PMIPv6, 6LowPAN, 4G/5G, Satellite/LEO/HTS)	In-layer Security Authentication & Authorization Encryption & Key Management Trust & Identity Management
4: Data Aggregation	Edge Networking; Edge Gateway	In-layer Security Blockchains Authentication & Authorization Encryption & Key Management Trust & Identity Management
3: Fog Networking	Wired (e.g., LAN); Wireless (e.g., BAN, PAN, ZigBee 3.0, Bluetooth 4.0, LAN); Wireless (LPWAN, Sigfox, LoRa, Weightless, 4G/5G, Satellite)	In-layer Security Authentication & Authorization Encryption & Key Management Trust & Identity Management
2: Data Acquisition	Hub; Hub; Hub; Hub	In-layer Security Blockchains Authentication & Authorization Encryption & Key Management Trust & Identity Management
1: Things (medical devices example)	ECG/EKG Sensor; Blood Pressure Sensor; Medicine Pump; Video Surveillance; Inertial Sensor; Pulse Oximetry Sensor; Fitness/exercise Sensor; Punic Button (partial list)	In-layer Security Blockchains Authentication & Authorization Encryption & Key Management Trust & Identity Management

IoT Factors Impacting Security

- IoT technology and systems are relatively *new and are, therefore, less well understood than traditional IT systems.*
- IoT systems are almost invariably *distributed over a wide (regional) geography*, typically in uncontrolled open environments.
- IoT systems are currently *deployed insularly across vendor-specific vertical applications*, creating fragmented technology and administrative silos.
- IoT endpoint systems have *limited electrical power* (typically being battery-driven).
- IoT devices are usually *deployed with low security measures in place*.

How can IoT use Blockchain?

Vendors are already working to make the IoT-blockchain connection in multiple ways such as:

- Trust building
- Cost reduction
- Accelerated data exchanges
- Scaled security

Applications of Blockchain in Security

Access Control

Example: *"Blockchain meets IoT: An architecture for scalable access management in IoT" by Oscar Novo*

Benefits of the proposed solution:

- *Mobility*: every administrative domain has its own freedom to manage the IoT devices while the access control policies are still enforced by the rules in the blockchain;
- *Accessibility*: This solution makes the access control rules available at any time. In addition, failures in some administrative servers do not ruin access to the information; all access control information is distributed.

Novo, Oscar. "Blockchain meets IoT: An architecture for scalable access management in IoT." *IEEE Internet of Things Journal* 5.2 (2018): 1184-1195.

Access Control (Cont'd)

- *Concurrency*: a constrained device can have multiple managers at the same time, and all of them can access or modify the access control policies concurrently.
- *Lightweight*: the IoT devices do not need any modification to adopt our solution.
- *Scalability*: this solution supports numerous IoT devices connected through dif- ferent constrained networks to a single blockchain.
- *Transparency*: the system hides the location of the IoT devices and how a resource is accessed.

Novo, Oscar. "Blockchain meets IoT: An architecture for scalable access management in IoT." *IEEE Internet of Things Journal* 5.2 (2018): 1184-1195.

Access Control (Cont'd)

Use Case Scenario

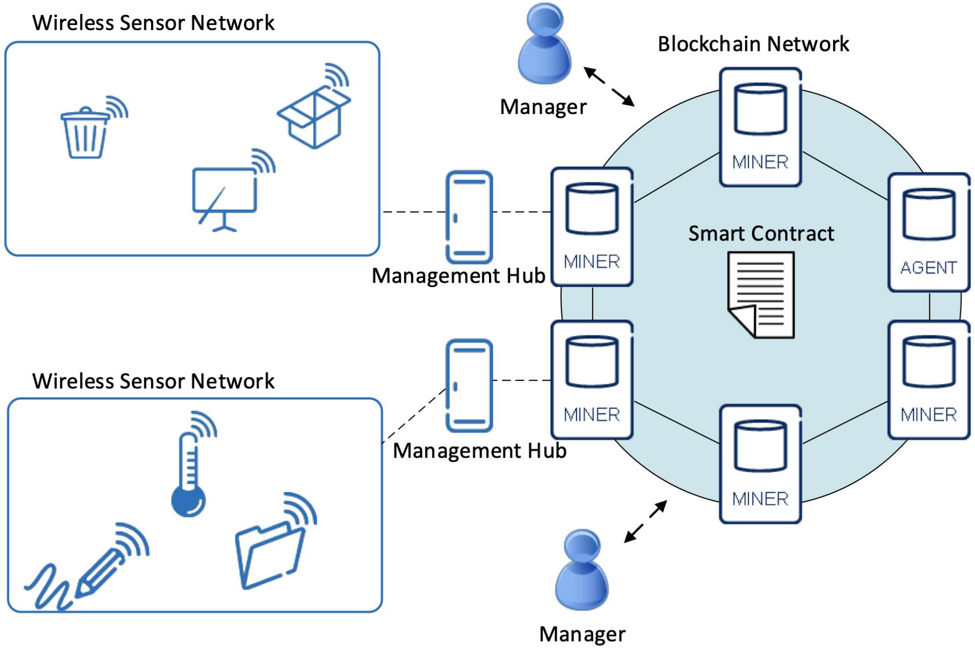


Figure 1: Access Control Use Case Scenario

Novo, Oscar. "Blockchain meets IoT: An architecture for scalable access management in IoT." *IEEE Internet of Things Journal* 5.2 (2018): 1184-1195.

Access Control (Cont'd)

Work Flow

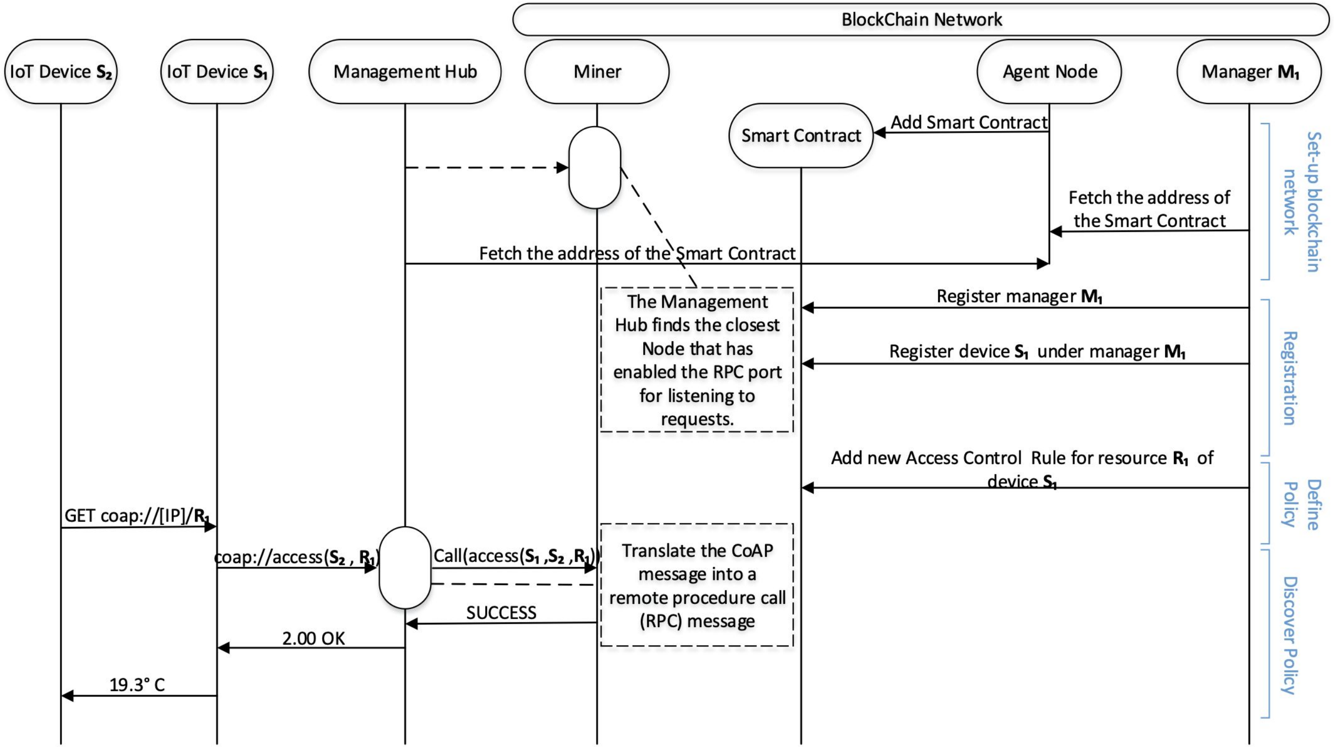


Figure 2: Proposed Solution Work Flow

Novo, Oscar. "Blockchain meets IoT: An architecture for scalable access management in IoT." *IEEE Internet of Things Journal* 5.2 (2018): 1184-1195.

Data Privacy

Example: *"Leveraging Blockchain to Enhance Data Privacy in IoT-Based Applications" by Truc Nguyen et al.*

Contributions:

- Developed a system model featuring a trustless access control management mechanism to ensure that users have full control over their data and can track how data are accessed by thirdparty services.
- Propose a firmware update scheme using blockchain that helps prevent fraudulent data caused by IoT device tampering.

Nguyen, Truc DT, Hoang-Anh Pham, and My T. Thai. "Leveraging blockchain to enhance data privacy in iot-based applications." *International Conference on Computational Social Networks*. Springer, Cham, 2018.

Data Privacy

Use Case

- **Aggregators**: categorize data from IoT devices into slots so that it can permit third-party services to access only a subset of data and issue transactions to the blockchain for granting permissions or publishing data.

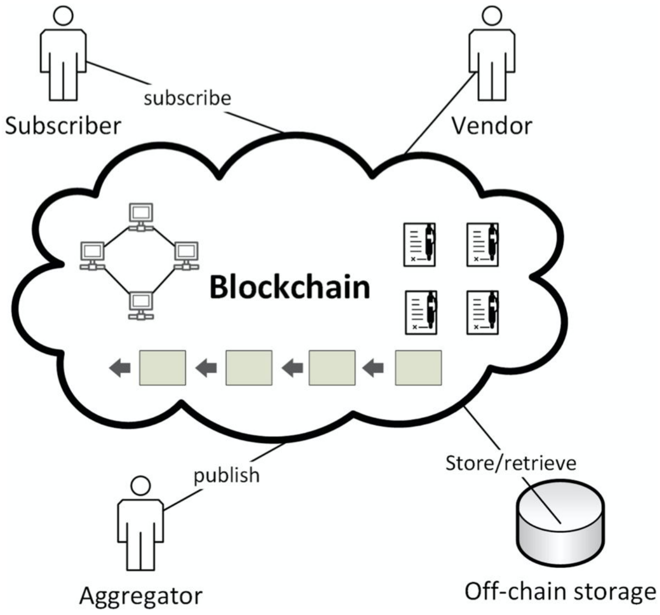


Figure 3: Data Privacy Use Case

Nguyen, Truc DT, Hoang-Anh Pham, and My T. Thai. "Leveraging blockchain to enhance data privacy in iot-based applications." *International Conference on Computational Social Networks*. Springer, Cham, 2018.

Data Privacy

- **Subscribers** represent third-party services who can issue transactions to access data published by Aggregators given appropriate permissions.
- **Vendors** represent manufacturers of IoT devices who are responsible for publishing official firmware images.

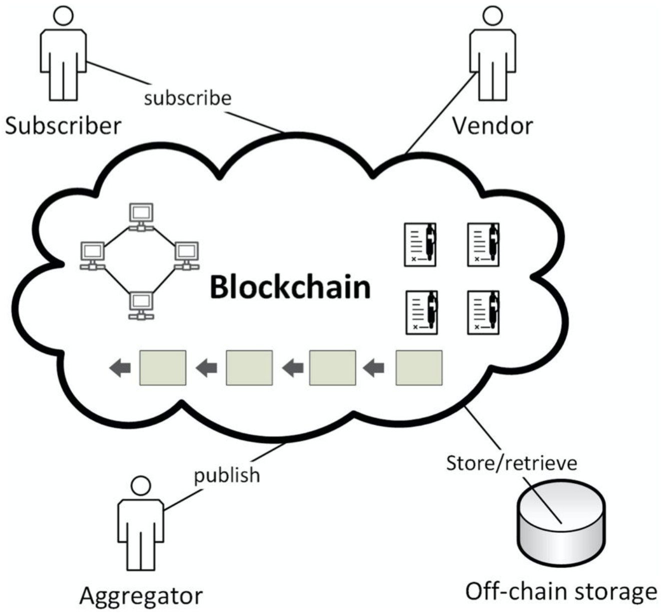


Figure 3: Data Privacy Use Case

Nguyen, Truc DT, Hoang-Anh Pham, and My T. Thai. "Leveraging blockchain to enhance data privacy in iot-based applications." *International Conference on Computational Social Networks*. Springer, Cham, 2018.

Data Privacy

- **Blockchain network** is deployed with two smart contracts:
    - *AccessControl*: used for managing access permissions.
        - Manages information sharing between subscribers and aggregators.
    - *FirmwareUpdate*: used for updating new firmwares.
        - Vendors publish hashes of their latest software updates.
        - Aggregators check the software versions of their IoT devices and update them if hashes are different than the ones in blockchain.

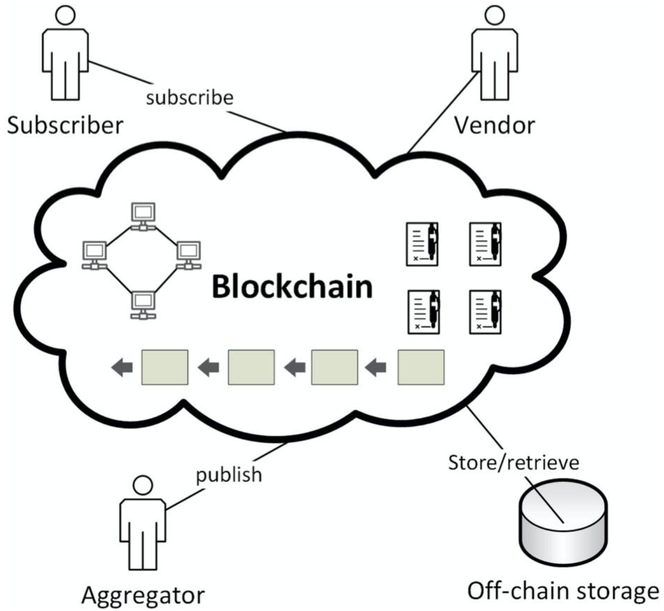


Figure 3: Data Privacy Use Case

Nguyen, Truc DT, Hoang-Anh Pham, and My T. Thai. "Leveraging blockchain to enhance data privacy in iot-based applications." *International Conference on Computational Social Networks*. Springer, Cham, 2018.

Malware Detection

Example: *“AutoBotCatcher: Blockchain-Based P2P Botnet Detection for the Internet of Things” by Gokhan Sagirlar et al.*

- AutoBotCatcher is an automatic P2P botnet detector based on the idea of botnet communities.
- It uses PeerHunter algorithm that constructs mutual contact graphs to detect P2P botnet communities.
- It exploits blockchain:
    - to **enable collaborative botnet detection** with big parties, rather than a centralized system.
    - to **validate correct execution of the botnet detection** as a collaborative process
    - to ensure **transparency** on collected snapshots of communities of IoT devices without trusted entity.

Sagirlar, G., Carminati, B., & Ferrari, E. (2018, October). AutoBotCatcher: Blockchain-Based P2P Botnet Detection for the Internet of Things. In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)(pp. 1-8). IEEE.

Malware Detection

Use Case:

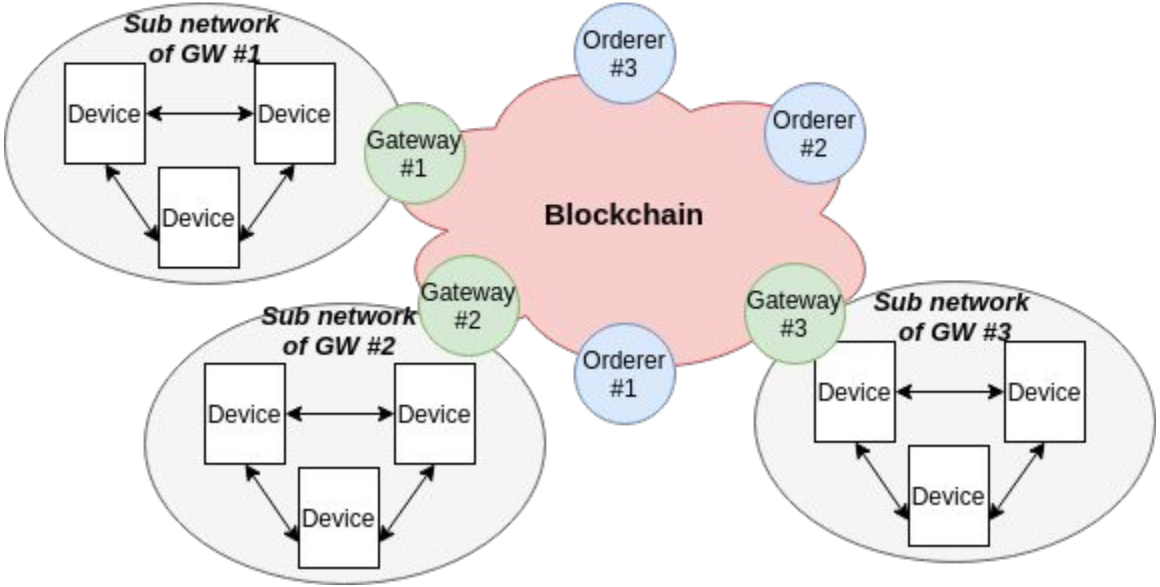


Figure 4: AutoBotCatcher Use Case

Sagirlar, G., Carminati, B., & Ferrari, E. (2018, October). AutoBotCatcher: Blockchain-Based P2P Botnet Detection for the Internet of Things. In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)(pp. 1-8). IEEE.

Malware Detection

Work Flow

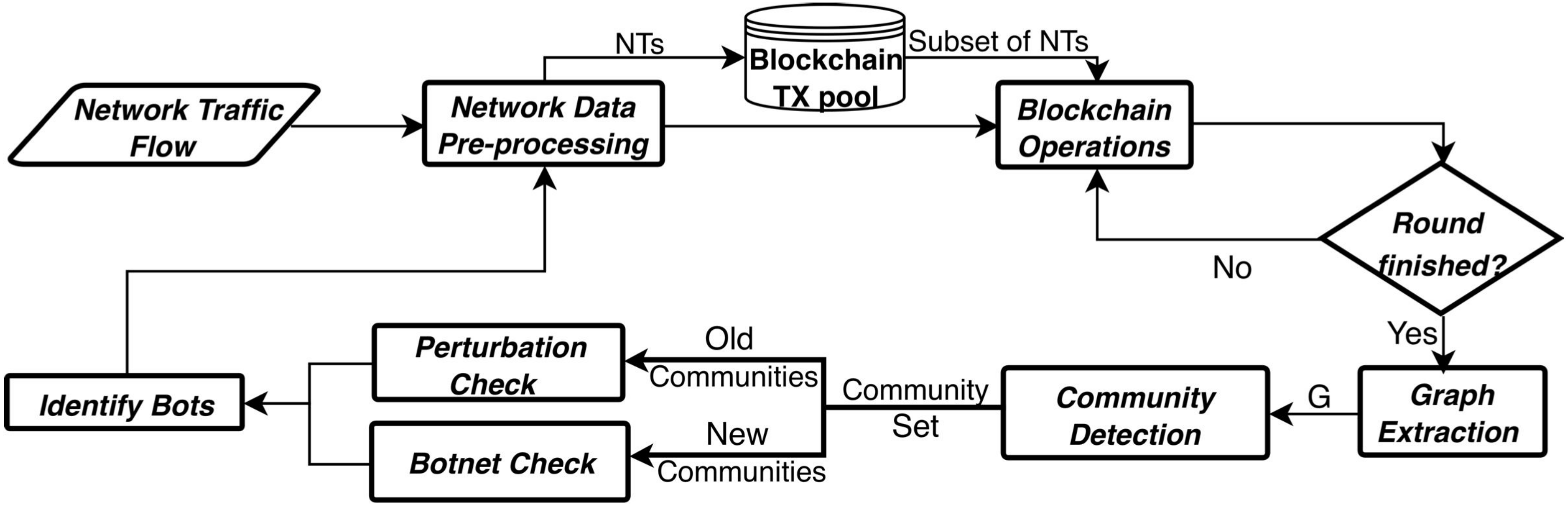


Figure 5: AutoBotCatcher Use Case

Sagirlar, G., Carminati, B., & Ferrari, E. (2018, October). AutoBotCatcher: Blockchain-Based P2P Botnet Detection for the Internet of Things. In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)(pp. 1-8). IEEE.

Final Thoughts

Final Thoughts

- Blockchain has many applications to enhance security of IoT devices such as access control, malware detection, and data privacy.
- It is a low cost solution for companies.
- The main challenges of deploying such technology in IoT devices is that the latter has limited computation and energy power.
- Some of consensus algorithms cannot work in an IoT context.
- There are emerging solutions like IOTA and Tangle transaction management.

Q&A

References

Nguyen, Truc DT, Hoang-Anh Pham, and My T. Thai. "Leveraging blockchain to enhance data privacy in iot-based applications." International Conference on Computational Social Networks. Springer, Cham, 2018.

Sagirlar, G., Carminati, B., & Ferrari, E. (2018, October). AutoBotCatcher: Blockchain-Based P2P Botnet Detection for the Internet of Things. In 2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)(pp. 1-8). IEEE.

O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," in IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195, April 2018, doi: 10.1109/JIOT.2018.2812239

.