Using Blockchain to Improve Security of the Internet of Things

Josh Quist
University of Minnesota, Morris
April 14, 2022

Introduction

- Alarm clock data wipe

  More sinister example:

- Intentional alarm data manipulation

https://www.bestbuy.com/site/amazon-echo-spot-smart-alarm-clock-with-alexa-black

Internet of Things Example Cont.

- Clearly important security risk
- Peloton Data breach
  - User info was exposed
  - Joe Biden Peloton Data was viewable
  - Weight is a socially sensitive issue, while birthdays are commonly used in passwords
- Devices like this need to be secure

https://www.npr.org/2022/01/24/1075326738/the-ins-and-out-of-peloton-culture

Talk Outline

1. Background Information
    a. Introduction to Internet of Things
    b. Discussion of current IoT implementations
    c. Introduction to blockchain
2. Blockchain IoT example 1
3. Blockchain IoT example 2
4. Blockchain Implementation Difficulties
5. Conclusion

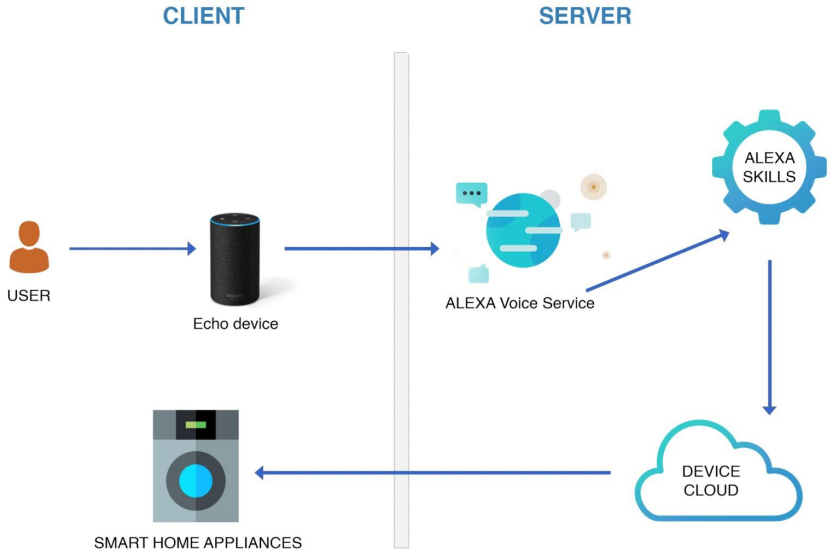
Internet of Things Introduction

- Internet of Things (IoT) definition
- Examples: Smart home security system, wearable health monitors, smart appliances.
- Automate tasks for convenience

https://builtin.com/internet-things/iot-internet-of-things-companies

Current IoT Implementation

- Alexa system design
  - Always-online
  - Amazon uses its servers for software functionality
  - Stores all data on its own cloud server
  - Typical of most IoT systems; data sometimes stored by third parties



https://www.qsstechnosoft.com/how-does-amazon-alexa-works

IoT Implementation Security Concerns

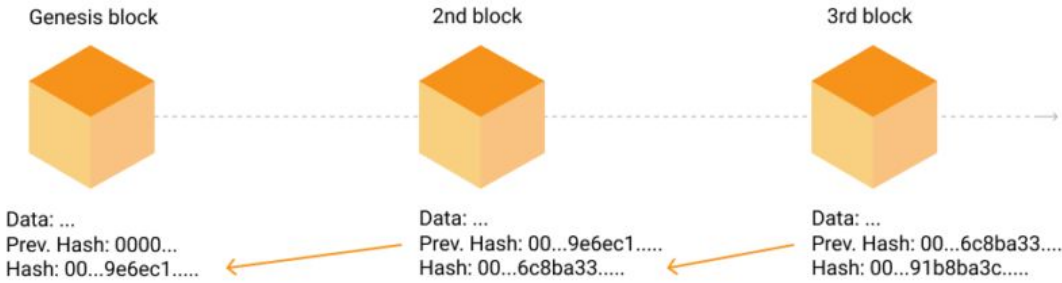
- Complete separation from your data
- Devices communicating with system not monitored
- Third parties often trusted with data
- Blockchain can help with these concerns

Talk Outline

1. Background Information
    a. Introduction to Internet of Things
    b. Discussion of current IoT implementations
    c. Introduction to blockchain
2. Blockchain IoT example 1
3. Blockchain IoT example 2
4. Blockchain Implementation Difficulties
5. Conclusion

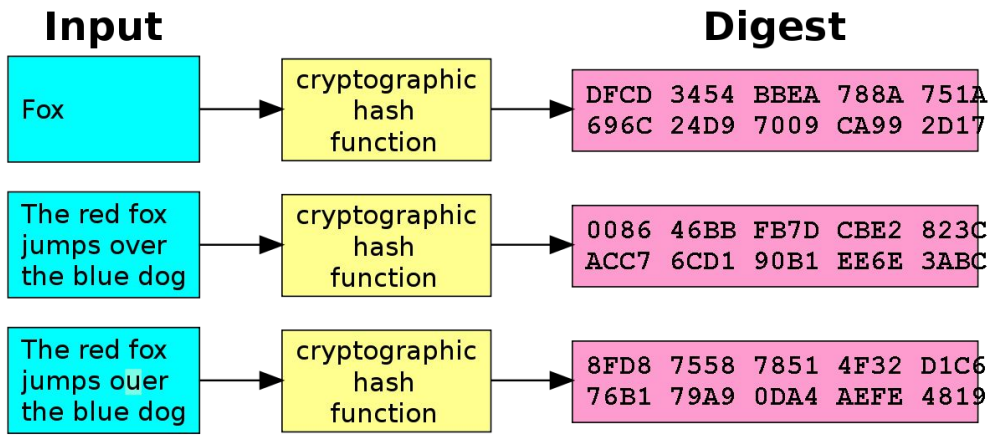
Introduction to Blockchain

- What is a blockchain?
  - Database containing records, or “Blocks”
  - Each block contains hash of previous block, hash of next block, timestamp, and data contained within
  - Blocks are “chained” because each contains information about the previous block



Hashing

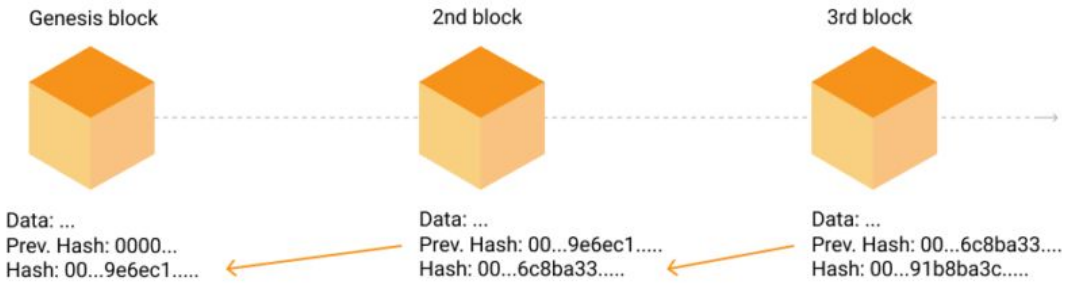
- Mathematical function, converts input to fixed length digest, or output
- One change alters entire output
- “One-way” - simple example



https://en.wikipedia.org/wiki/Cryptographic_hash_function

Hashing in Blockchain

- All information in the block hashed, points to the next block
- Data unable to be altered without breaking the chain
- One way functionality means data is secure



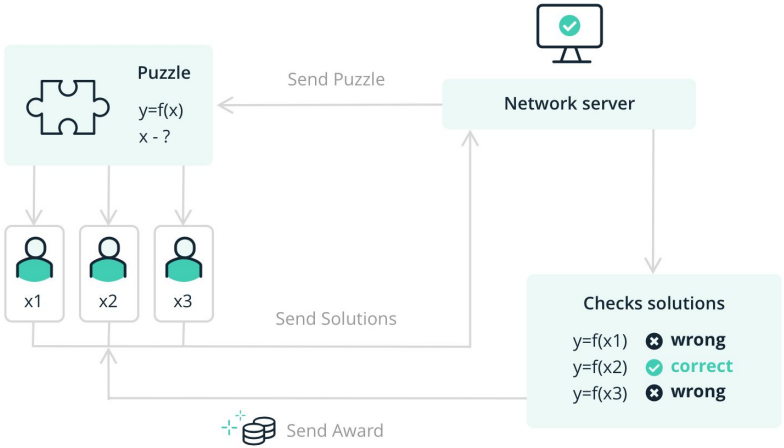
Bitcoin Blockchain Example

- Bitcoin most well-known implementation of blockchain
- Decentralized, digital currency, or Cryptocurrency
- Blockchain stores transaction information
- Anonymous way to send and receive money
- Bitcoin’s blockchain grows by incentivizing miners

https://bitcoin.org/

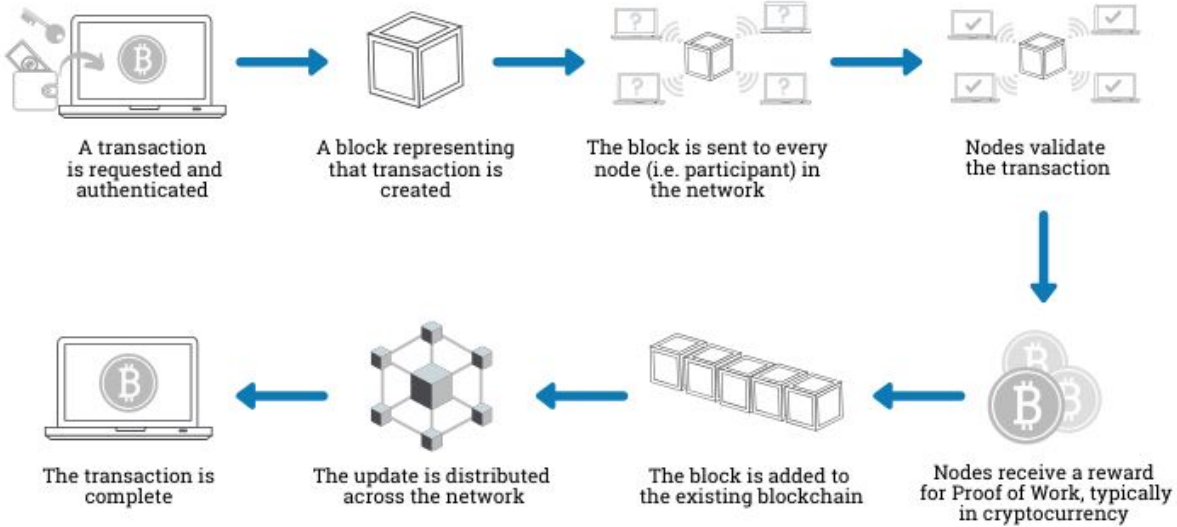
Bitcoin mining

- Bitcoin generates new block every 10 minutes, including a target digit and the hash for the next block
- Bitcoin miners calculate the hash of the next block to verify
- The solution to the hash is a mathematical problem
- Finding the solution, or “proof of work” essentially guesswork
- Reward for solving this “proof of work” is Bitcoin



https://www.ledger.com/academy/blockchain/what-is-proof-of-work

Completing Transaction



https://support.coinigy.com/hc/en-us/articles/4408831413915-What-is-Bitcoin-

Mining Ensuring Authenticity

- The mining process ensures that entries are authentic
- After a miner posts the solved hash, all other miners verify its correctness
- Data in blockchain unable to be modified

Talk Outline

1. Background Information
    a. Introduction to Internet of Things
    b. Discussion of current IoT implementations
    c. Introduction to blockchain
2. **Blockchain IoT example 1**
3. Blockchain IoT example 2
4. Blockchain Implementation Difficulties
5. Conclusion

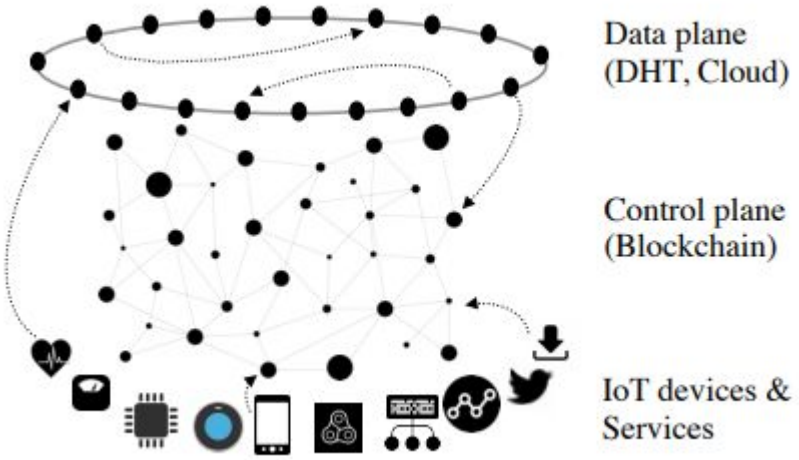
IoT Implementation Security Concerns

Again, specific security concerns with current system designs:

- Complete separation from your data
- Devices communicating with system not monitored
- Third parties often trusted with data

Shafagh et al. System Design

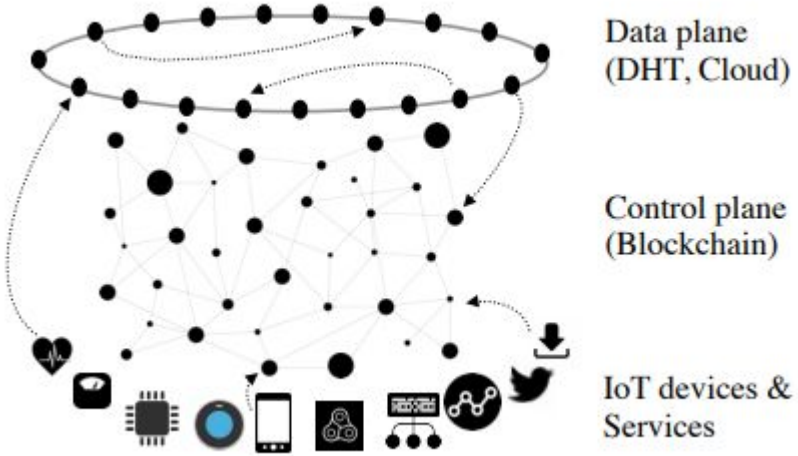
- System designed to provide access control
- Built on top of Bitcoin's blockchain system



Source: Shafagh (2017)

Control Plane and IoT Devices

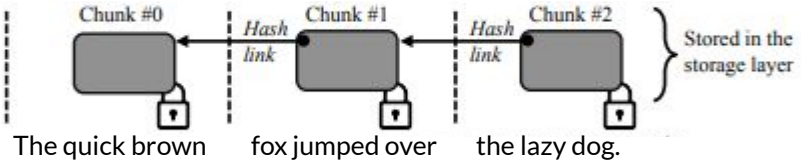
- IoT Device layer
  - Each device contains the private key for the IoT network
  - Private key is essentially system's password
- Control Plane: blockchain containing authenticated device ID's and the private key
- Data Plane: data chunked and stored on a third party server



Source: Shafagh (2017)

Example 1 Chunking Visual

- Data is chunked, then sent to data plane
- Each chunk encrypted



Source: Shafagh (2017)

Ex 1 Example of attack this system prevents

- Peloton Example
  - Leaky API
  - Data chunking
- DDoS Attack
  - Low power devices typically used as part of “swarm”
  - Access control

Performance Evaluation

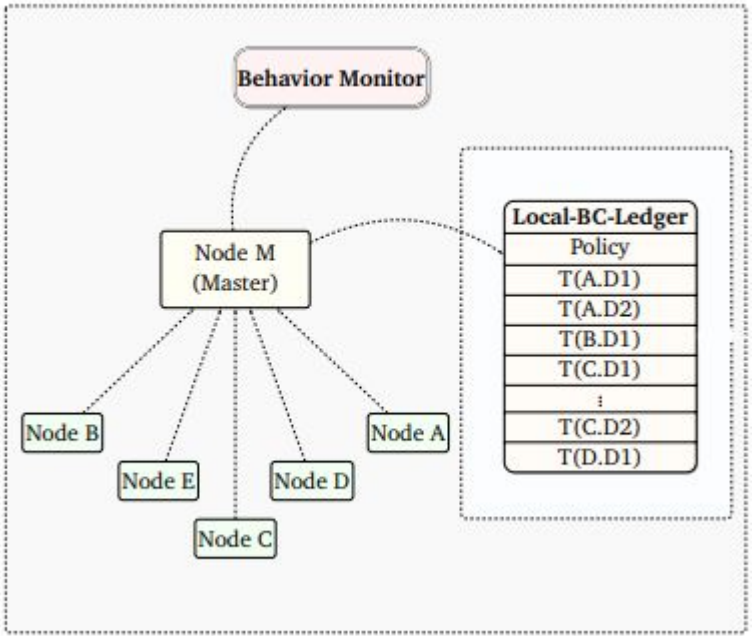
- 10% slowdown in request throughput
- “Moderate overhead” due to the system hardware requirements
- Future work will include optimizing that overhead, and building more expansive IoT system for more testing

Talk Outline

1. Background Information
    a. Introduction to Internet of Things
    b. Discussion of current IoT implementations
    c. Introduction to blockchain
2. Blockchain IoT example 1
3. **Blockchain IoT example 2**
4. Blockchain Implementation Difficulties
5. Conclusion

Ali et al. System

- Designed for IoT network
- Most powerful device designated as master node
- Transaction data stored in local blockchain on master node
- Behavior Monitor on top of master node



Source: Ali (2019)

Behavior Monitor

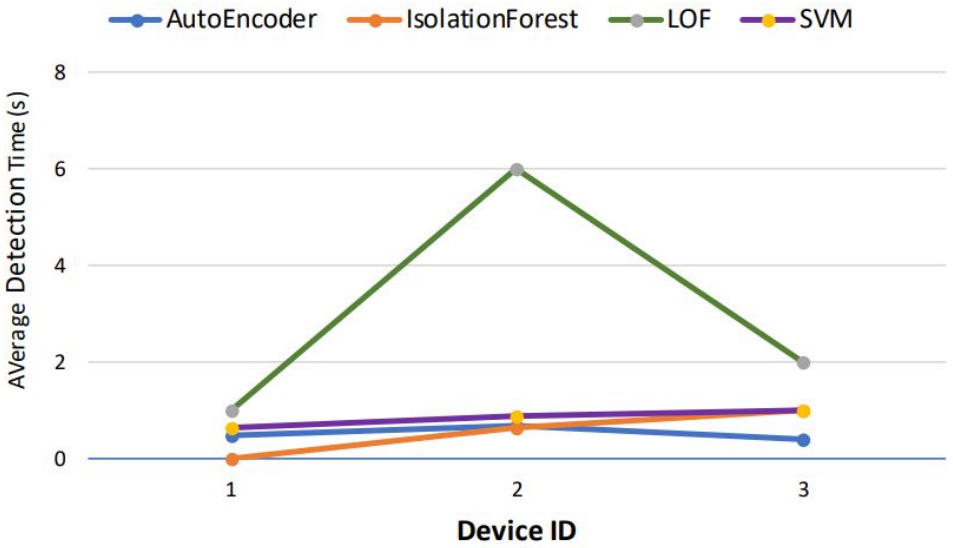
- Behavior monitor uses machine learning to identify bad actors
  - Machine learning is the process of training an algorithm on data in order to “teach” the machine patterns to look for.
- This system uses an algorithm which is trained on benign data to detect malicious behavior

What this system solves

- System does monitoring of IoT network
- Flags administrator of system when malicious behavior detected
- Takes care of IoT devices which provide advertised functionality, but in the background misuse your data

Performance Evaluation

- Performed tests comparing detection time to other popular anomaly detection algorithms
  - Isolation Forest
  - Local Outlier Factor
  - Support Vector Matrix
- AutoEncoder model produced similar detection times



Source: Ali (2019)

Blockchain Implementation Difficulty/Concerns

- Climate concerns
- Hardware limitations
- More involved on the user's side
- Scalability

Conclusion

- Current IoT has problems
- Blockchain can solve problems, but comes with some of its own
- More work is being done to address these

Sources

Jawad Ali, Toqeer Ali, Yazed Alsaawy, Ahmad Shahrafidz Khalid, Shahrulniza Musa. Blockchain-based Smart-IoT Trust Zone Measurement Architecture. (May 2019)

Hossein Shafagh, Lukas Burkhalter, Anwar Hithnawi, Simon Duquennoy. Towards Blockchain-based Auditable Storage and Sharing of IoT Data. (November 2017)

Questions?