Securing IOT devices using Blockchain

Rafsal Rahim
TVE16MCA41

October 21, 2018

Dept. MCA, College of Engineering Trivandrum

Table of contents

Introduction

What do IOT mean?

Definition

The internet of things is a system of interrelated computing devices that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

IoT architecture can be represented by four building blocks:

- Things
- Gateways
- Network infrastructure
- Cloud infrastructure

Figures 1

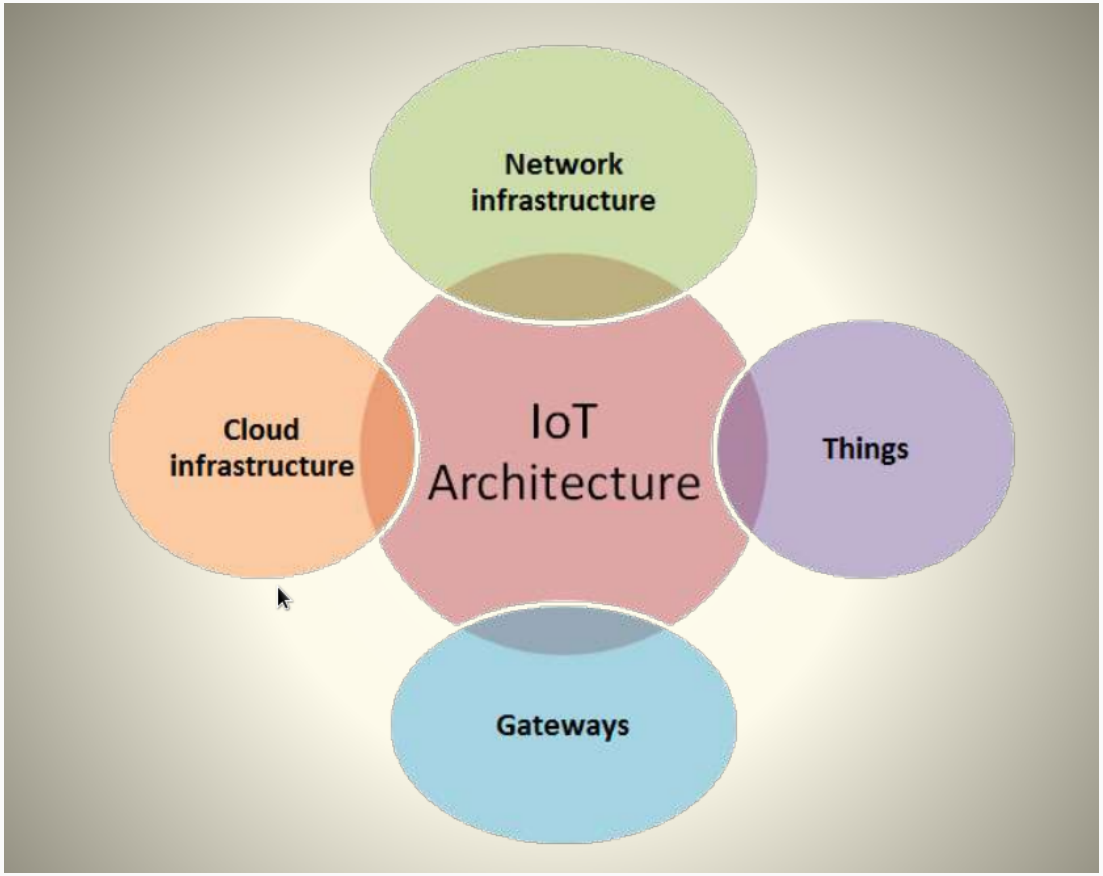

Figure 1: building blocks of IoT

Challenges

Challenges to secure IoT deployments

- IoT Systems are poorly designed
- complex and sometimes conflicting configurations
- Limited guidance for life cycle maintenance and management of IoT devices
- There is a lack of standards for authentication and authorization of IoT edge devices.
- denial-of-sleep attacks
- denial-of-service attacks (DoS) attacks

Problem with current centralized model

- Current IoT ecosystems rely on centralized, brokered communication models.
- Existing IoT solutions are expensive.
- Lack of security has made users loose trust on the data sharing system.
- No relaible way to ensure security of collected data.
- Cloud servers will remain a bottleneck and point of failure that can disrupt the entire network.

Solution using decentralization

Decentralizing IoT networks

A decentralized approach to IoT networking would solve many of the issues above.

- prevent failure in any single node in a network from bringing the entire network to a halting collapse.
- reduce the costs associated with installing and maintaining large centralized data centers.
- IoT security is much more than just about protecting sensitive data.
- Any decentralized approach must support three foundational functions:
  1. Peer-to-peer messaging.
  2. Distributed file sharing.
  3. Autonomous device coordination.

The Blockchain Approach

Blockchain distributed ledger technology.

The data recorded are transparent, secure, auditable, and efficient.

What do blockchain means?

- distributed ledger
- maintaining a permanent and tamper-proof record of transactional data.
- Each of the computers in the distributed network maintains a copy of the ledger

Some advantages of blockchain?

- The big advantage of blockchain is that it's public.
- A blockchain is decentralized, so there is no single authority
- Most importantly, it's secure. The database can only be extended and previous records cannot be changed

How does it work?

Figure 2

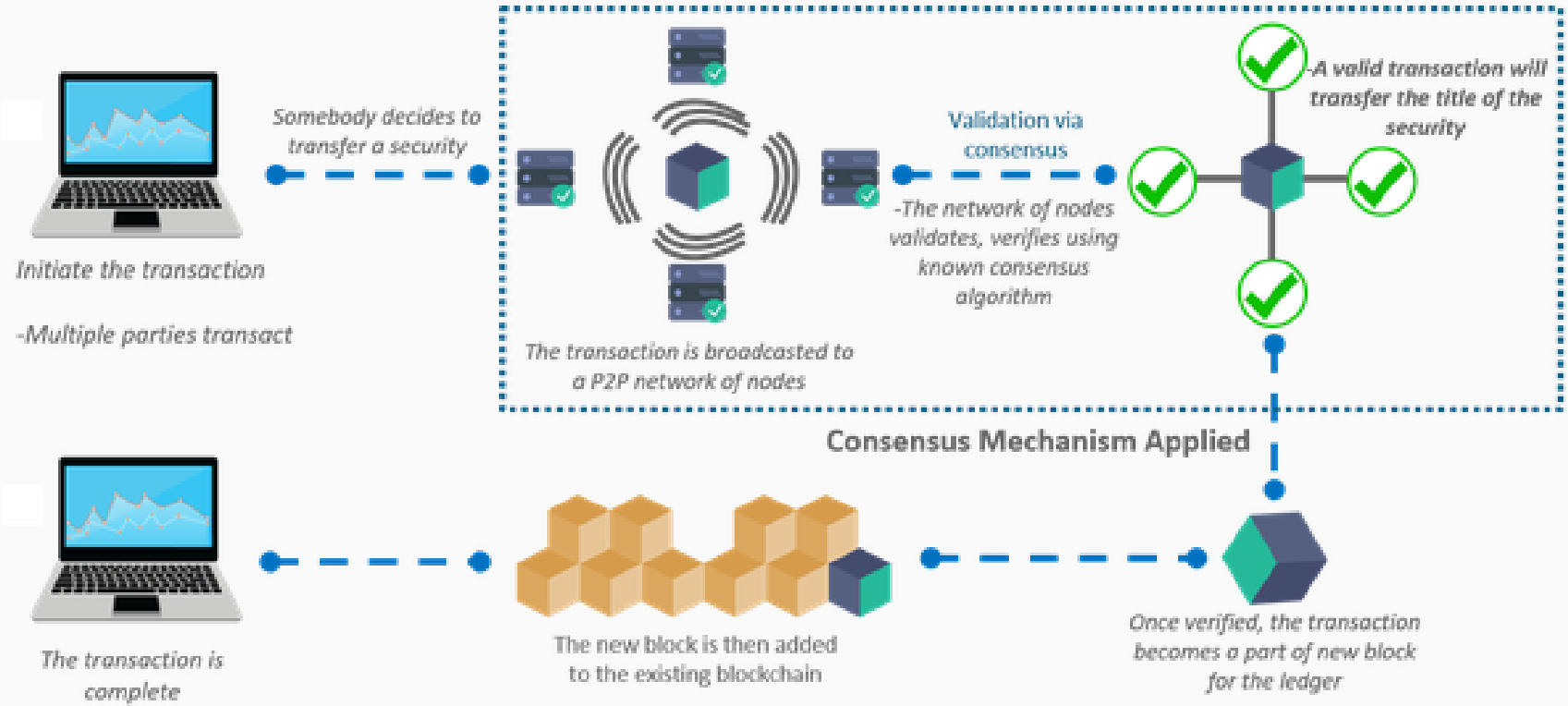

Figure 2: Blockchain basic image

Block structure

- Block ID
- Timestamp
- Nonce
- Data
- Previous block hash

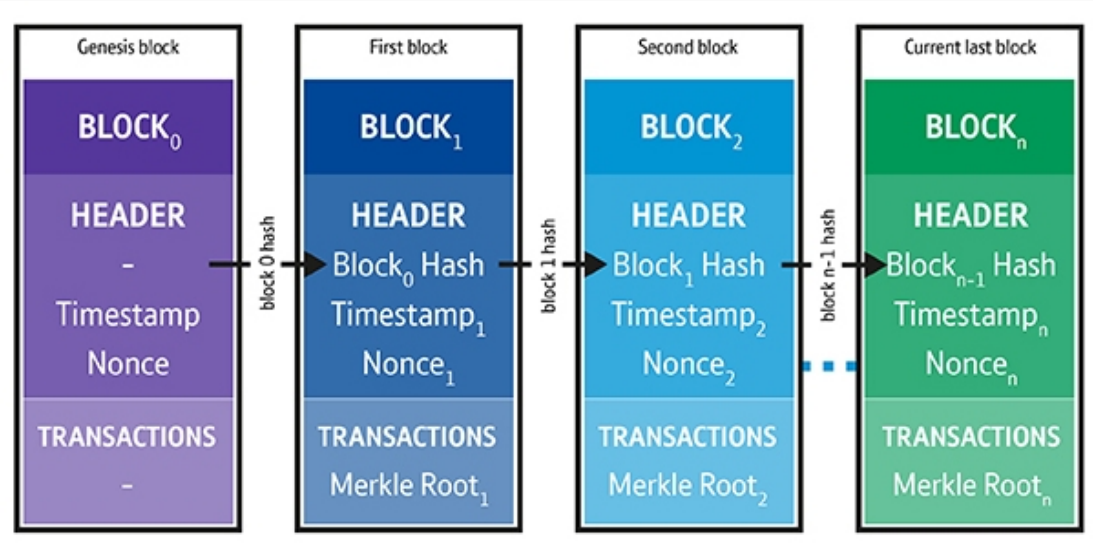

Figure 3: Block structure

Modification of Data

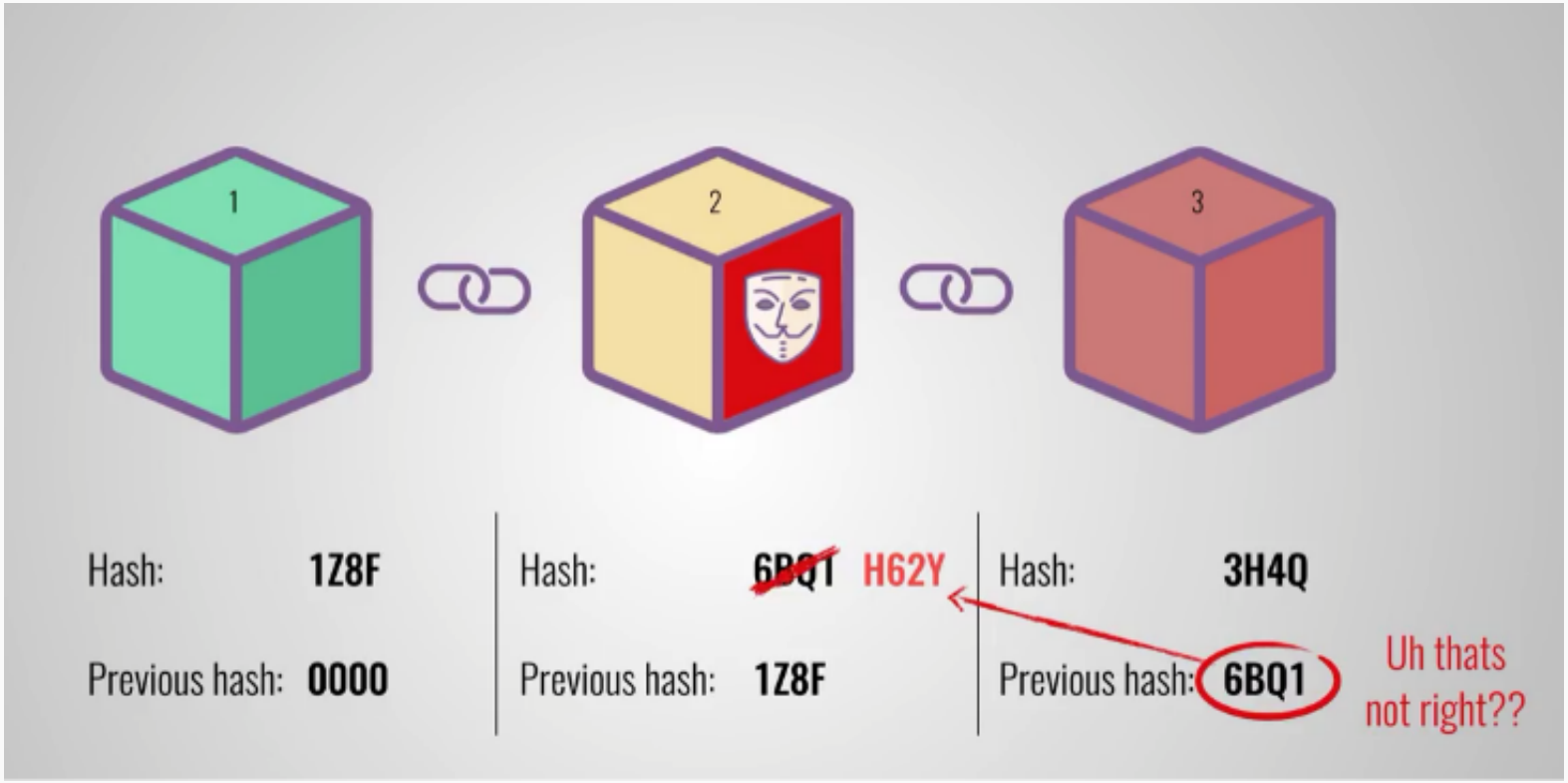

Figure 4: When Mutation of data happens.

How blockchain can be used to secure IoT data.

Trusted Requirements

IoT data as a spacial commodity, collected by government, corporates, even individuals, which are of greate value to different application fields. Such owner need a trusted platform to exchange there IoT data.

Trusted Requirements

IoT data as a spacial commodity, collected by government, corporates, even individuals, which are of greate value to different application fields. Such owner need a trusted platform to exchange there IoT data.

Trusted Trading

Trusted Requirements

IoT data as a spacial commodity, collected by government, corporates, even individuals, which are of greate value to different application fields. Such owner need a trusted platform to exchange there IoT data.

Trusted Trading

- Transaction once conformed can not be modified.

Trusted Requirements

IoT data as a spacial commodity, collected by government, corporates, even individuals, which are of greate value to different application fields. Such owner need a trusted platform to exchange there IoT data.

Trusted Trading

- Transaction once conformed can not be modified.
- Should not be maintained by a third-party.

Trusted Requirements

IoT data as a spacial commodity, collected by government, corporates, even individuals, which are of greate value to different application fields. Such owner need a trusted platform to exchange there IoT data.

Trusted Trading

- Transaction once conformed can not be modified.
- Should not be maintained by a third-party.
- Exchange data should be transparent.

Trusted Requirements

IoT data as a spacial commodity, collected by government, corporates, even individuals, which are of greate value to different application fields. Such owner need a trusted platform to exchange there IoT data.

Trusted Trading

- Transaction once conformed can not be modified.
- Should not be maintained by a third-party.
- Exchange data should be transparent.

Trusted Requirements

IoT data as a spacial commodity, collected by government, corporates, even individuals, which are of greate value to different application fields. Such owner need a trusted platform to exchange there IoT data.

Trusted Trading

- Transaction once conformed can not be modified.
- Should not be maintained by a third-party.
- Exchange data should be transparent.

Trusted Data Access

Data owner can hold their ownership.

Trusted Requirements

IoT data as a spacial commodity, collected by government, corporates, even individuals, which are of greate value to different application fields. Such owner need a trusted platform to exchange there IoT data.

Trusted Trading

- Transaction once conformed can not be modified.
- Should not be maintained by a third-party.
- Exchange data should be transparent.

Trusted Data Access

Data owner can hold their ownership.

Trusted Requirements

IoT data as a spacial commodity, collected by government, corporates, even individuals, which are of greate value to different application fields. Such owner need a trusted platform to exchange there IoT data.

Trusted Trading

- Transaction once conformed can not be modified.
- Should not be maintained by a third-party.
- Exchange data should be transparent.

Trusted Data Access

Data owner can hold their ownership.

Trusted Privacy Preserve.

Data owner can protect their personal information while data exchange.

Architecture

The framework can be divided into Data Layer, Network Layer, Protocol Layer and Interaction Layer.

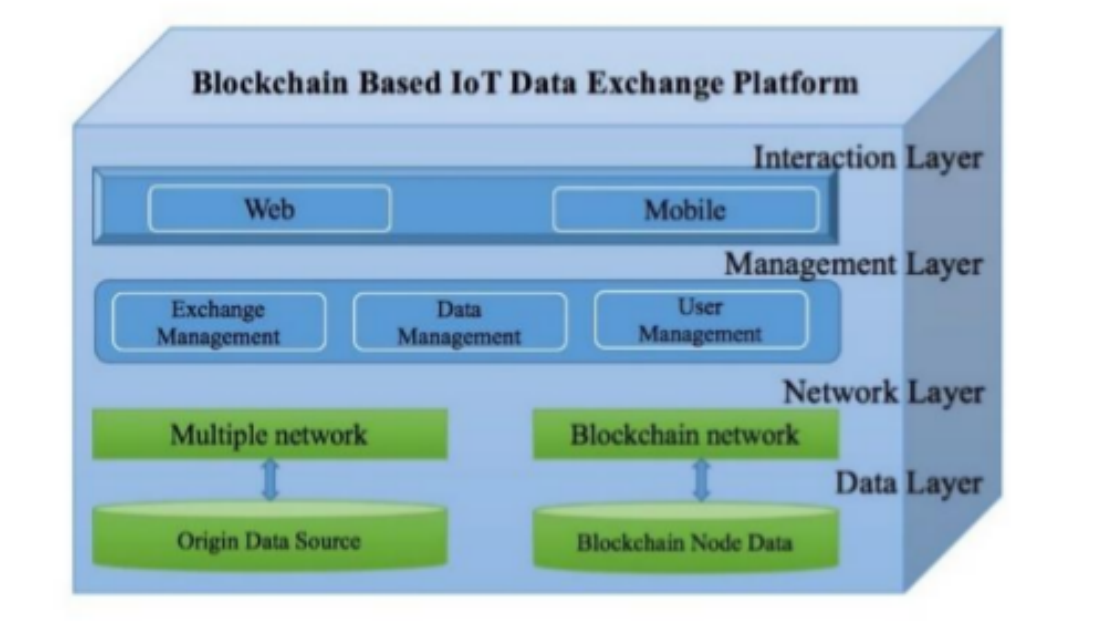

Figure 5: Architecture of blockchain based IoT data exchange platform

Layers

Data Layer

Consists of multiple network and blockchain network:

- Multiple network is responsible for origin data access and transmission.
- Blockchain network composed of one or more blockchain node.

Network Layer

Consists of two parts:

- IoT data : Stored in any place the user wants.
- Exchange data : Stored in blockchain.

Layers

Management Layer

- Data Management
- User Management
- Exchange Management

Interaction Layer

Provides the interface for data exchange parties to communicate with each other.

Component Design

Exchange Management Contracts

Exchange management contracts include three type protocols:

- Access Contract: Uses capability based access control method to provide a trusted data permission management.
- Communication Contract: Record the whole communicated process in IoT data exchange for traceability.
- Auto Exchange Contract: Send the data access right to demander while they satisfy the condition.

Data & User Management Contracts

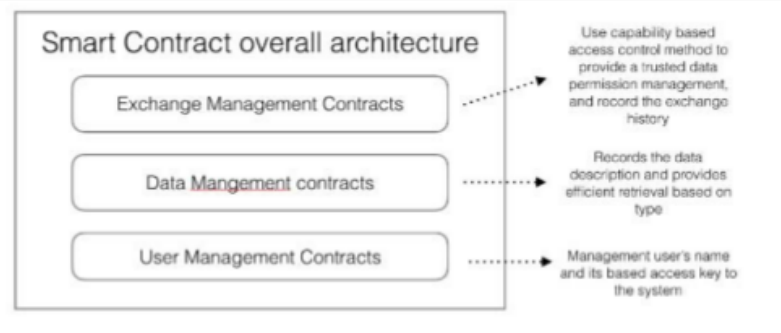

Figure 6: Architecture of smart contract based management component

Data Management Contracts

- Data Contract: Generate a *data object contract* and *call data access contract*.
- Classified search Contract: Record the whole communicated process in IoT data exchange for traceability.

User Management Contracts

Controls the users's security and permissions of the platform.

Conclusion

Summary

IoT data exchange was divided into three categories:

- trusted trading
- trusted data access
- trusted privacy preserve.

It proposes a blockchain based solution to meet such requirement and designs the major trusted components.

Blockchain network can record the transaction in an auditable,transparent and immutable way.

Questions?

References I

1. A Decentralized Solution for IoT Data Trusted Exchange Based-on Blockchain by Zhiqing Huang , Xiongye Su at 2017 3rd IEEE International Conference on Computer and Communications.
2. How Does the Blockchain Work?
3. What is Blockchain Technology? A Step-by-Step Guide For Beginners
4. Securing the Internet of Things (IoT) with Blockchain