Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things

18510107 조정훈

▶ Abstract

Blockchain is promising for IoT security, which may influence a variety of areas including manufacture, finance, and trading.

In this paper investigate typical security and privacy issues in IoT and develop a framework to integrate blockchain with IoT

Blockchain can provide great assurance for IoT data and various functionalities and desirable scalability including authentication, decentralized payment, and so on.

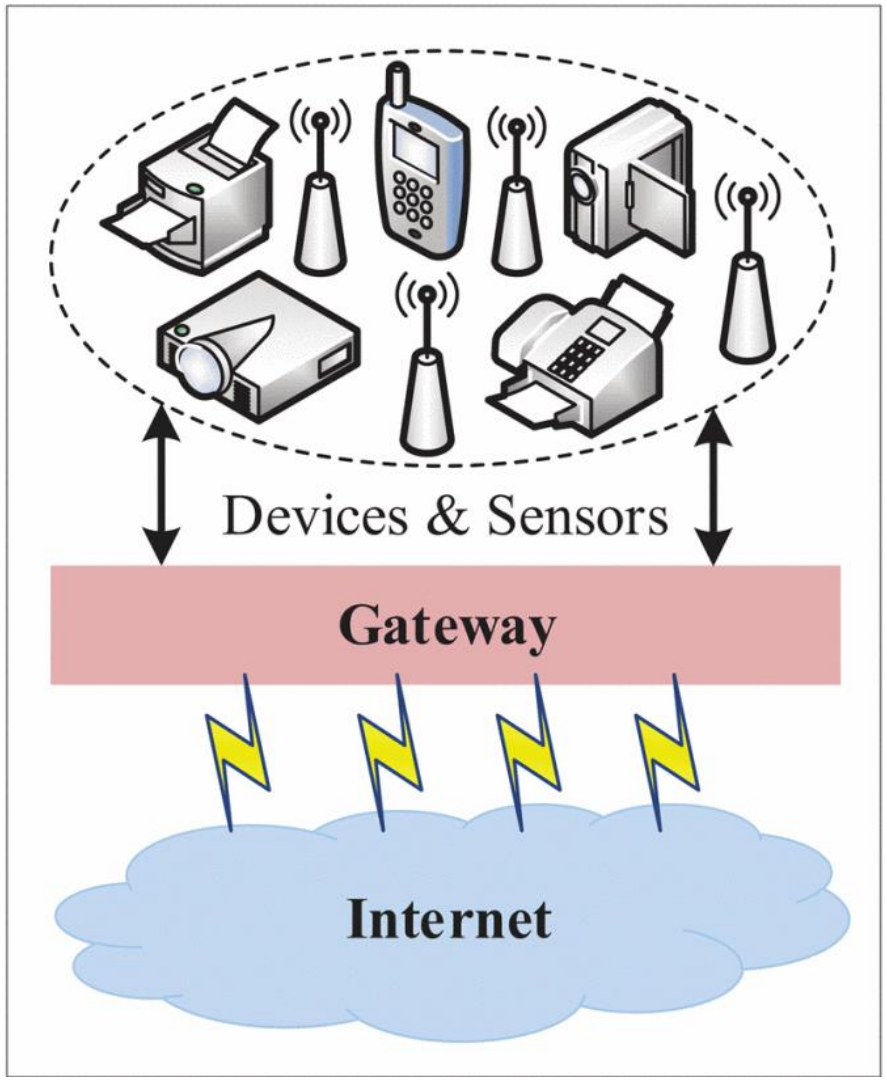
This paper also suggest some possible solutions to these security and privacy issues in IoT based on blockchain and Ethereum to show how blockchain contributes to IoT.

▶ Introduction

Generally speaking, IoT encompasses everything that is connected to the Internet.

The devices are uniquely identified in an IoT system and always regarded as equipped with low power, limited storage, and restrained processing capacity.

The gateways are employed to link IoT devices to the Internet and able to “talk” to each other.



IoT architecture.

IoT in Smart Homes :

Suppose your home is equipped with some IoT devices

Elderly or disabled individuals in a smart home, it is easy to monitor their demands through cameras and help them by remotely controlling the devices at home.

IoT in Smart Cities :

A smart city is an urban area that uses data collection sensors to transmit information, and manage assets and resources efficiently

smart traffic management can monitor traffic streams to control traffic lights and avoid congestion on the roadway in rush hours

IoT brings great convenience to individuals and governments;
However, IoT systems with a large number of devices, tens of millions of data, and sophisticated connections may also be a security nightmare.

To the best of our knowledge, there is no publicly accepted framework to embrace blockchain by IoT.

In this article following three contributions:

- We investigate the traditional architecture of IoT and analyze the security and privacy issues in IoT systems.
- We demonstrate how blockchain can integrate with IoT and describe a framework in which blockchain and IoT work together.
- We show a few possible solutions to address the security and privacy issues in IoT systems based on blockchain and Ethereum.

Blockchain

Blockchain is an append-only decentralized digital ledger based on cryptography.

Blockchain is one of the underlying techniques in decentralized networking with many potential merits

Blockchain is distributed. It allows a variety of peers to join the network without registration, which makes it easier than traditional centralized systems

Blockchain transplants trust into the system via a consensus mechanism, such as proof of work(PoW) and proof of stack (PoS).

Blockchain is immutable. Information on blockchain exists as a shared and intact copy.

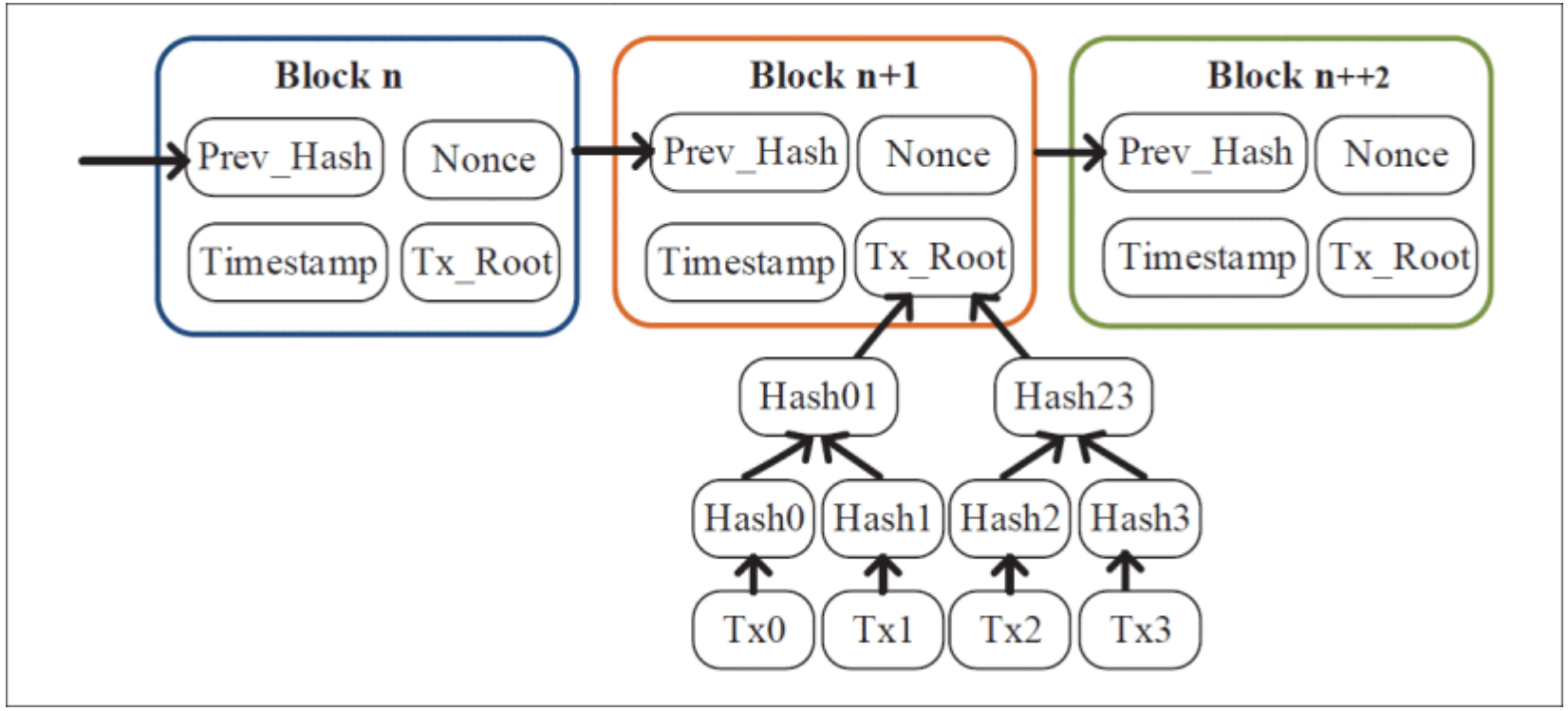


Figure 2 shows a typical structure of blockchain.

Peers join the system with unique private-public key pairs.

block is generated, it is spread to miners, who need to validate all transactions in the block.

블록 #574849

요약	
거래 수	2236
출력 합계	15,959.70267938 BTC
예상된 거래량	3,076.51975171 BTC
거래 수수료	0.95260505 BTC
높이	574849 (주 체인)
타임 스탬프	2019-05-06 13:06:24
수신 시간	2019-05-06 13:06:24
릴레이된 곳	SlushPool
난이도	6,702,169,884,349.17
Bits	388628280
크기	1080.0 kB
무게	3993.042 kWU
번역	0x20000000
해시 난수	715471215
블록 보상	12.5 BTC

해시	
해시	00000000000000000018edac64b16e4937ad91e0783548d17a974f5d9a06d96f
이전 차단	00000000000000000000411d764db0be06bd717724136dc6ac66df4e80b3f6b4d
다음 블록	00000000000000000016817d08baa5a6f43599e0546c59317cceecf6639d614d
Merkle Root	be47d1b677b80b893983372fc3dac6c67b50cec00f85a04af6aa52de8ad2f9c1

Bitcoin Transaction

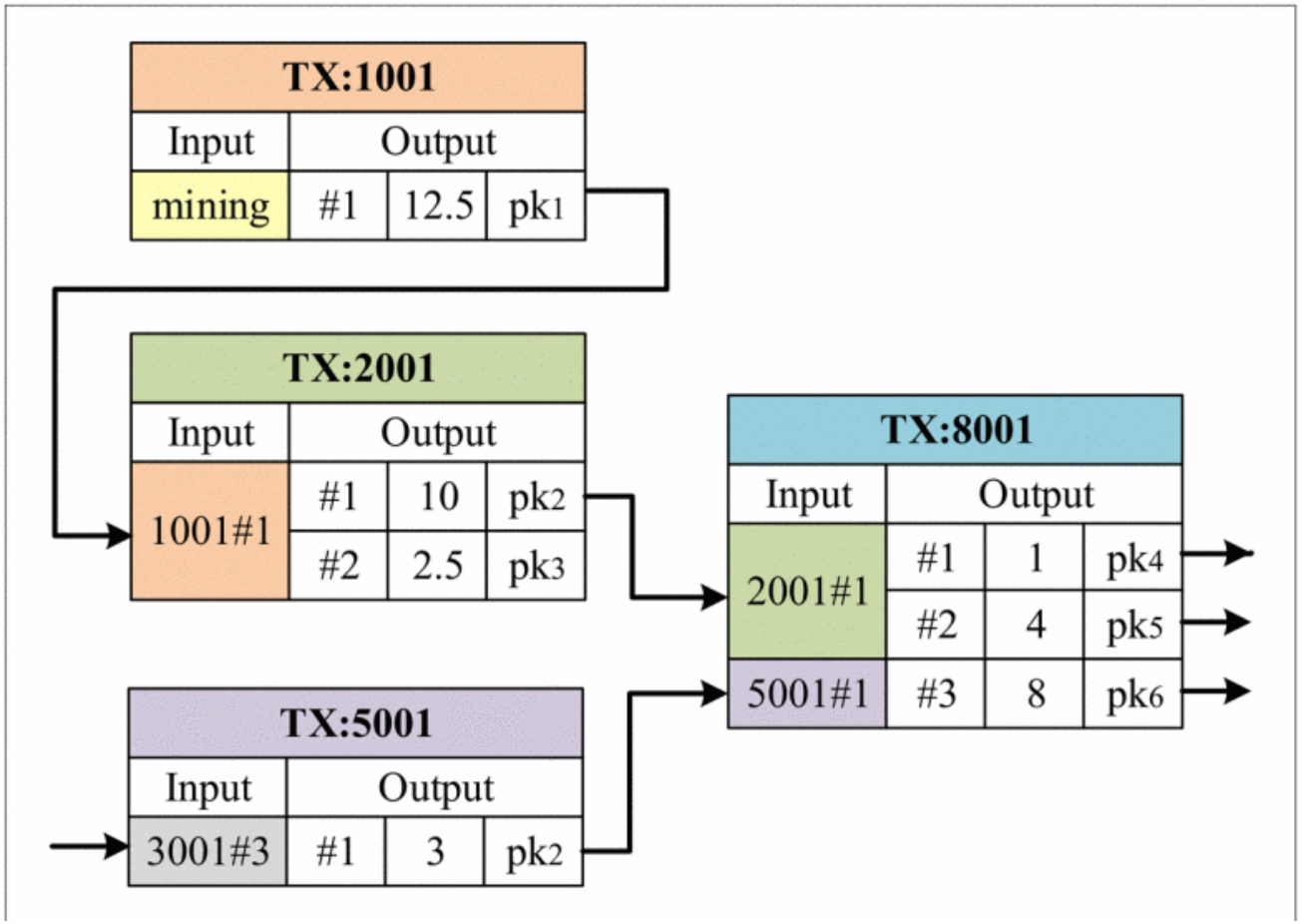
The UTXOs spent in a transaction are the inputs and outputs of a transaction, which are the UTXOs that the transaction creates in the system.

The user with pk1 contains 12.5 bitcoins in account.

TX2001, it takes as input TX1001 and generates two UTXOs, pk2 and pk3

Bitcoin supports multiple UTXOs as inputs, as shown in transaction TX8001

Digital assets are transferred via transactions, and each transaction in the system leads to the generation of new UTXOs and revocation of used UTXOs.



e0637f9e0870a6663c6c4b18e076247cfa3d69cdb9d0bb19bd785c8a5499d49a

3M6YkdSBQhrEchpWy4WpTetZv1m4Xoqoof
3MWgiBZg5bSW9CYfdDrQxeboYSTXisKLgv
32yd1PPqk2ptCV6ymC2D87rzpb6eCfjnh7
3LyvWUAY9N5smxhpPNkQkWiwNEEQdHBXp7
3CHPi4GcfN5bTnKyGyF3iUQP4SFjNHzrax
39EPMQcxuxVpwhVrS6SNsCXaKLwXppudu3
3LMvRtWFzyqnjfAYvh7bnjuc3BNmFXX5V6
13hpscLD3p6CNGUjr2wSwhnvSCUBpqPXZz
1BqHkK1bTsyYkRipTAwAPrpkJJhX1zXCY4
3KJXdvhMFzb46RWHyL3qY9kYfRuYzTk4JZ
3LcyJPV5w513N2pV2jktpF3nNorNGGajWk
3GazmwC331qku9u8XuaKMjfFwEnrHvScQD
3CxXnYYaWo3njX6uUMN42HzuF2a4JsDRwB
3HMBgCnMZdYVwAJZE7R1WNtUctxyVCAz2p
3JDAKxKTRGtAFxzWRzphdc9HqqcpP4yVg6
33zZaEZfWQnVBHHkUWeAK7mT5BgtP6RC6R
33qLWPvaYx7jZgqHMeQLi4YD3JLdKdvZUZ
19bvfWaEzG2dP5fofRGRzXCPGQ6G2QcLvb
19XdnWYxyR8zN2crdceEjKyYVysF6YnqGu
3Qkr7Shak1x7NHx2bmCdkiB2f2rgxJWqps
3CW1Pgfu7NMcVmPEF5dLvmY3fr8QtBEQgW
36jEN5jZDHVxGAMHuFAyEihz2AGnzC6eJK

3M6YkdSBQhrEchpWy4WpTetZv1m4Xoqoof → 36HAYcC6uVoutPnpReqyEaAsB3HyuD4fPD 3.80008373 BTC
3MWgiBZg5bSW9CYfdDrQxeboYSTXisKLgv → 3NnHqtKDqzKib25SGXK1mTHcsbbz6yFYQp 0.029365 BTC

요약	
주소	3M6YkdSBQhrEchpWy4WpTetZv1m4Xoqoof
Hash 160	d4ddb11aa39b067ab9e3081df2315292dd132ee8
거래	
거래 수	35
총 수신량	1.47171184 BTC
최종 잔액	0 BTC

요약	
주소	36HAYcC6uVoutPnpReqyEaAsB3HyuD4fPD
Hash 160	3255d7cb28028aaa4ec567ec2ce92df231e5e71e
거래	
거래 수	2935
총 수신량	5,423.70220396 BTC
최종 잔액	44.36463043 BTC

Smart Contract

The smart contract concept was proposed by Nick Szabo in 1994 when he realized that the decentralized ledger could achieve a smart contract.

Traditional trusted lawyer or notary.

Smart contract can act as a trusted third party without any assumption

Contracts can be stored as programming codes and run automatically on the blockchain once the conditions are satisfied.

- Autonomy. Smart contracts can be executed independently and automatically in a prescribed manner.
- Trust. The documents on the ledger are encrypted using symmetric encryption algorithms.
- Accuracy. Smart contracts are faster, cheaper, and more accurate than traditional contracts.

Ethereum

Ethereum and Bitcoin are two main applications of blockchain.

The main difference is that the Bitcoin blockchain is for tracking the transfer of ownership of cryptocurrencies, while the Ethereum blockchain focuses more on running programming codes on the platform, which achieves more powerful functionality such as voting and ballots.

Contains two types of accounts, Externally Owned Accounts controlled by private keys and Contract Accounts controlled by codes in contracts.

Data Integrity

The data generated by IoT systems of a company are critically important, and may involve trade secrets that are closely related to the future development of the company and are often kept confidential from outsiders.

Traditional centralized storage, such as cloud storage, can be integrated into IoT architecture

The centralized server is vulnerable and may easily have a single point of failure, cause many-to-one traffic jams, delayed response, system scalability problems

Data Sharing

A primary object of an IoT system is sharing information between objects, which is helpful to manufacturing, transportation, and business to provide better service in people's daily lives.

these data are usually not free; thus, a convenient and fair data trading mechanism is needed.

Authentication and Access Control

Another security issue is unauthorized access to the resources and sensitive information in IoT systems.

However, the IoT system makes centralized approaches a bottleneck when the number of devices explosively grows.

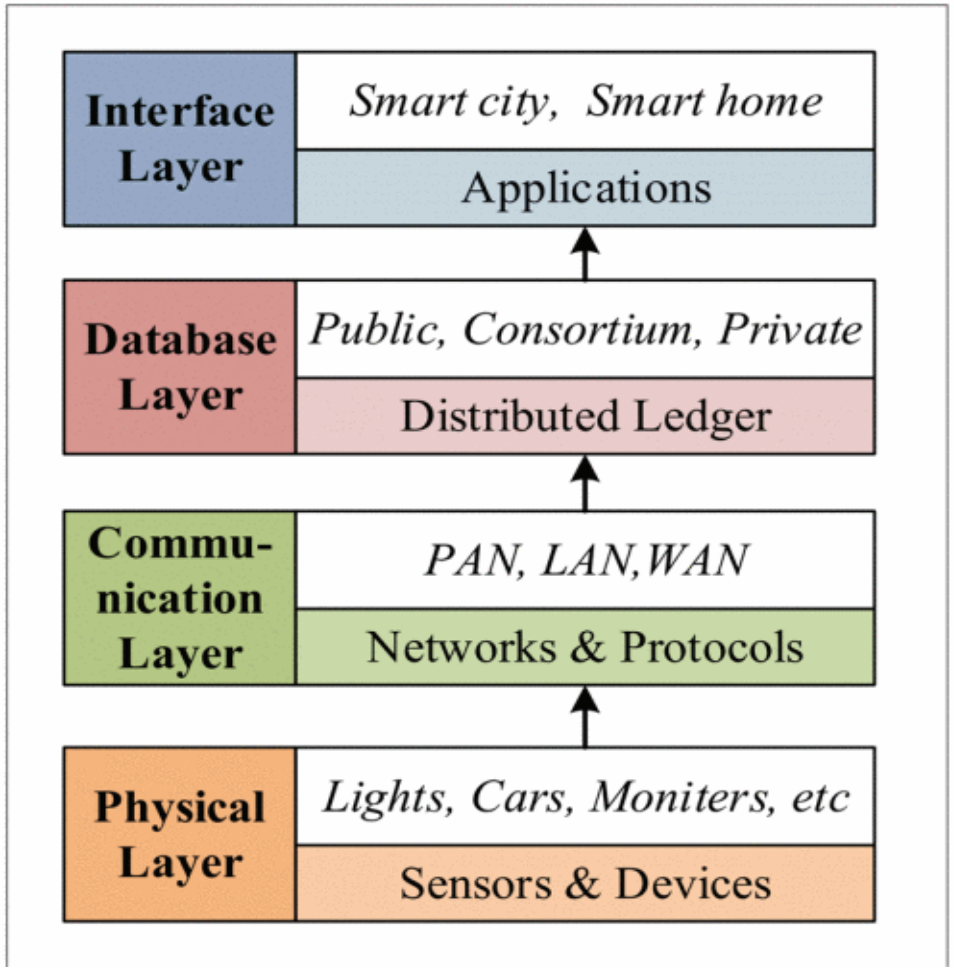
Privacy

An IoT system collects data using a variety of smart devices and sensors to make a comprehensive decision according to customized requirements.

privacy is easily violated in various ways, such as data acquisition, raw data processing, and data exchange

Thus, privacy preservation in IoT systems, including data privacy and entity privacy, is of great importance and also a challenge.

IoT Framework with Blockchain



Security IoT framework with blockchain.

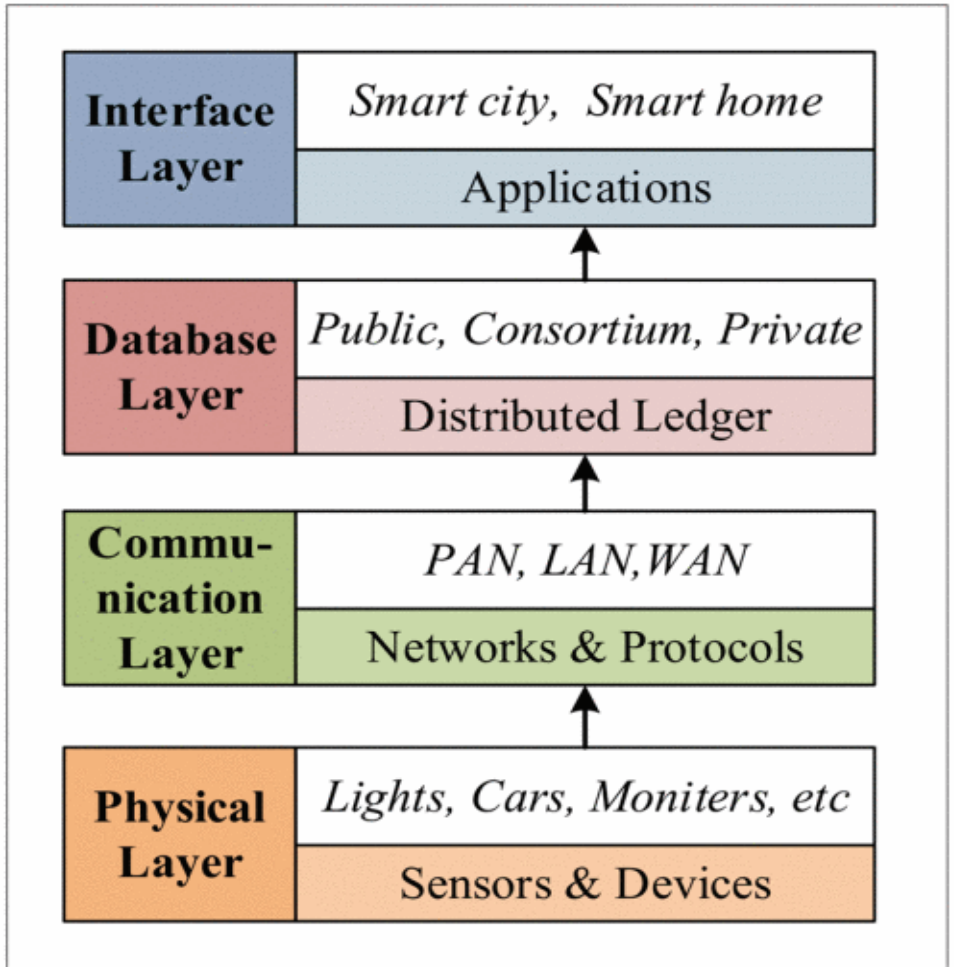
Physical layer: The physical layer includes all the smart devices, equipped with sensors and actuators, that collect and forward data to upper layers.

Usually, there is no single standard for smart devices to share and integrate with each other to provide cross-functionality.

Communication layer: Smart devices in IoT use different communication mechanisms to get access to the system and exchange information.

Security and privacy of the transmitted data within the system are quite important. Blockchain can be integrated with the system and contribute a lot to this circumstance.

IoT Framework with Blockchain

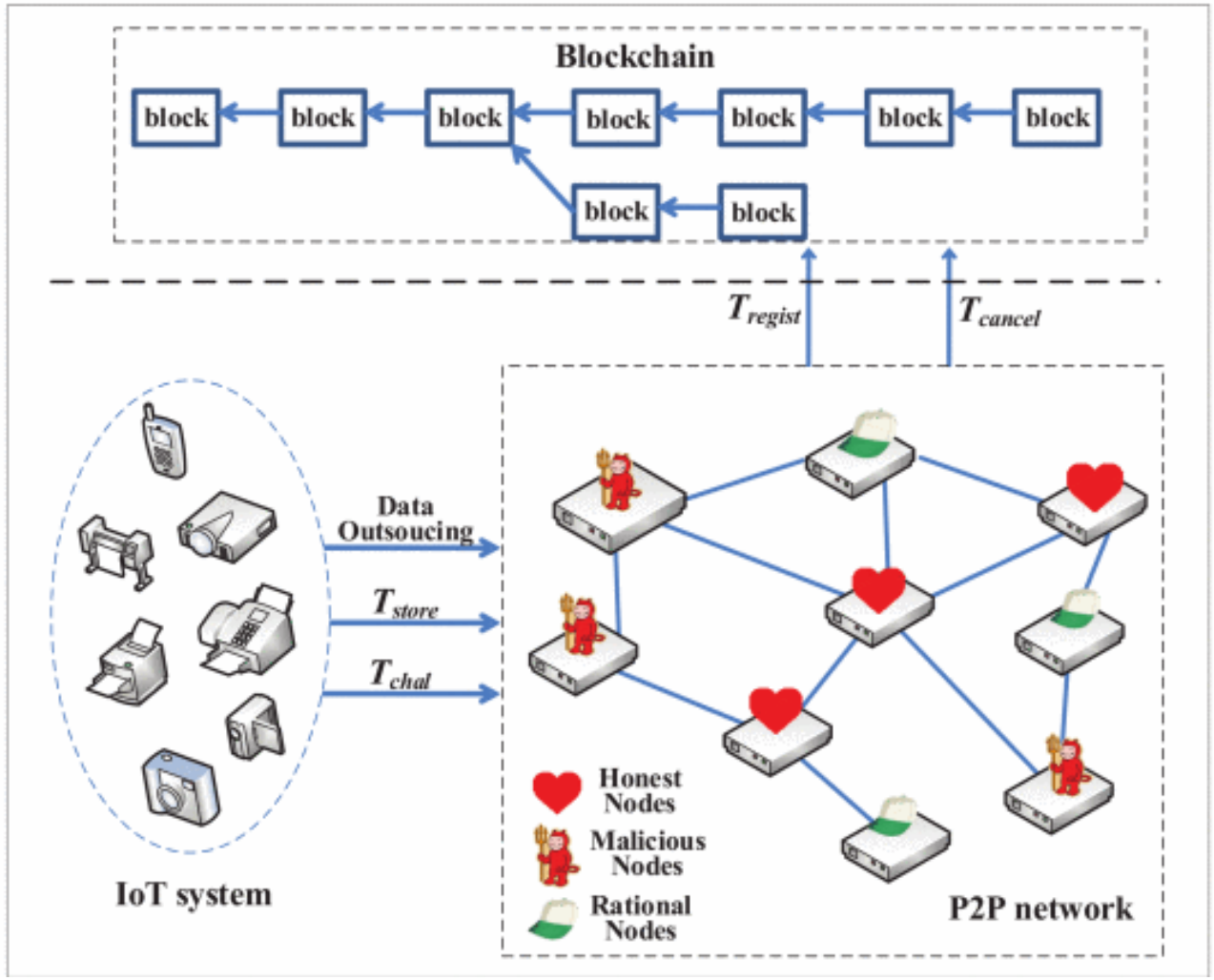


Security IoT framework with blockchain.

Database Layer: Blockchain itself is a distributed database that records immutable and continuously growing transactions.

Interface Layer: The interface layer contains applications that communicate with each other to make a beneficial decision collaboratively.

Data Integrity



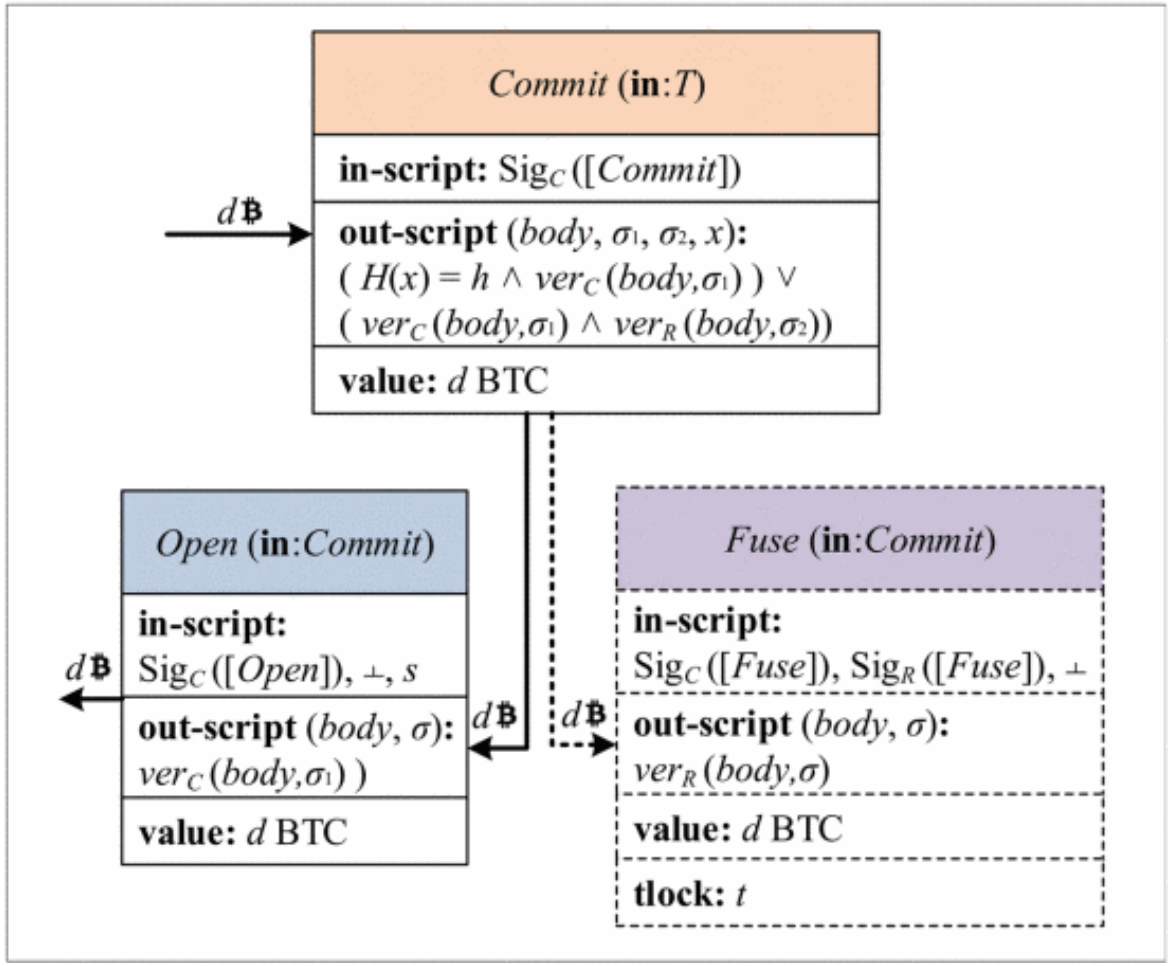
Specifically, it works as follows, in which Ethereum and smart contract are employed.

IoT devices should be encrypted before outsourced.

Peers in a peer-to-peer (P2P) system need to commit the space they possess by generating a proof of space to prove their claims and make deposits.

Miners validate the transactions by checking verification equations in proof of space and link valid trans-actions in blockchain.

Data Sharing



Suppose a data owner collects data generated in an IoT system and shares the data at a price of d BTC with a receipt.

If you read the contract, the script works with "Open", and if you do not read the contract within the time limit t, the script will work with "Fuse".

트랜잭션 비트코인 거래에 대한 세부정보 보기

b16561de0ba39162bedaf4a9c2a123f86c27d4ddf94174aa60b7fc23f5b0912a

187P1HZqXdeGd4Vieak1S4TcmK6WwmaZq5 (0.038254 BTC - 산출)

1JbnuBYhuvt2BMhT5wLgEeLeg1ZQekMjKs - (지출) 0.0003 BTC

1PSitQH9CAgkacXuENy4ktfKMdZMYVTSLb - 0.0289515 BTC (지출)

5 승인 | 0.0292515 BTC

요약	
크기	226 (bytes)
무게	904
수신 시간	2019-05-06 12:53:53
잠금 시간	블록: 574848
블록에 포함됨	574849 (2019-05-06 13:06:24 + 13 의사록)
승인	5
시각화	트리 차트 보기

입력 및 출력	
총 거래량	0.038254 BTC
총 출력	0.0292515 BTC
거래 수수료	0.0090025 BTC
1 바이트 당 수수료	3,983.407 sat/B
무게 단위당 요금	995.852 sat/WU
예상 BTC거래량	0.0003 BTC
스크립트	스크립트 숨기기 & coinbase

입력 스크립트

ScriptSig: PUSHDATA(72)
[3045022100f8df57ec6851d286cf15dc78294c1c7529b574805167b7f9ded1b81dc2c5331302200147a4de720b4ccad7
PUSHDATA(33)[020bc44c197104b6107e63e572674ddef3412851f4dfcb41545b0b10445fd5cf3e]

출력 스크립트

DUP HASH160 PUSHDATA(20)[c10e989d8e747267cdeb6d7335e7a0861a0b2a31] EQUALVERIFY CHECKSIG

DUP HASH160 PUSHDATA(20)[f63021932ce73d1981c690f9dec0d57910033abc] EQUALVERIFY CHECKSIG

Authentication and Access Control

Ethereum can provide authentication and access control to smart devices

removes the dependent central parties and gets better efficiency compared to traditional access control models

Users can pre-define access policies in smart contracts and generate several

T_{policy} Includes the pre-denned access policies
T_{access} is for access management
T_{query} is for access query.

When a new entity enrolls in an IoT system for the first time, a newly generated public key together with the corresponding access permission is determined

Privacy

To protect privacy in an IoT system, consortium and private blockchain are usually involved.

blockchain uses pseudonyms, say public keys, to achieve anonymity.

However, this is not strong enough in some real-world applications.

1. Linkable ring signatures are well suited to sign a transaction that can hide the sender's identity in a spontaneous ring.

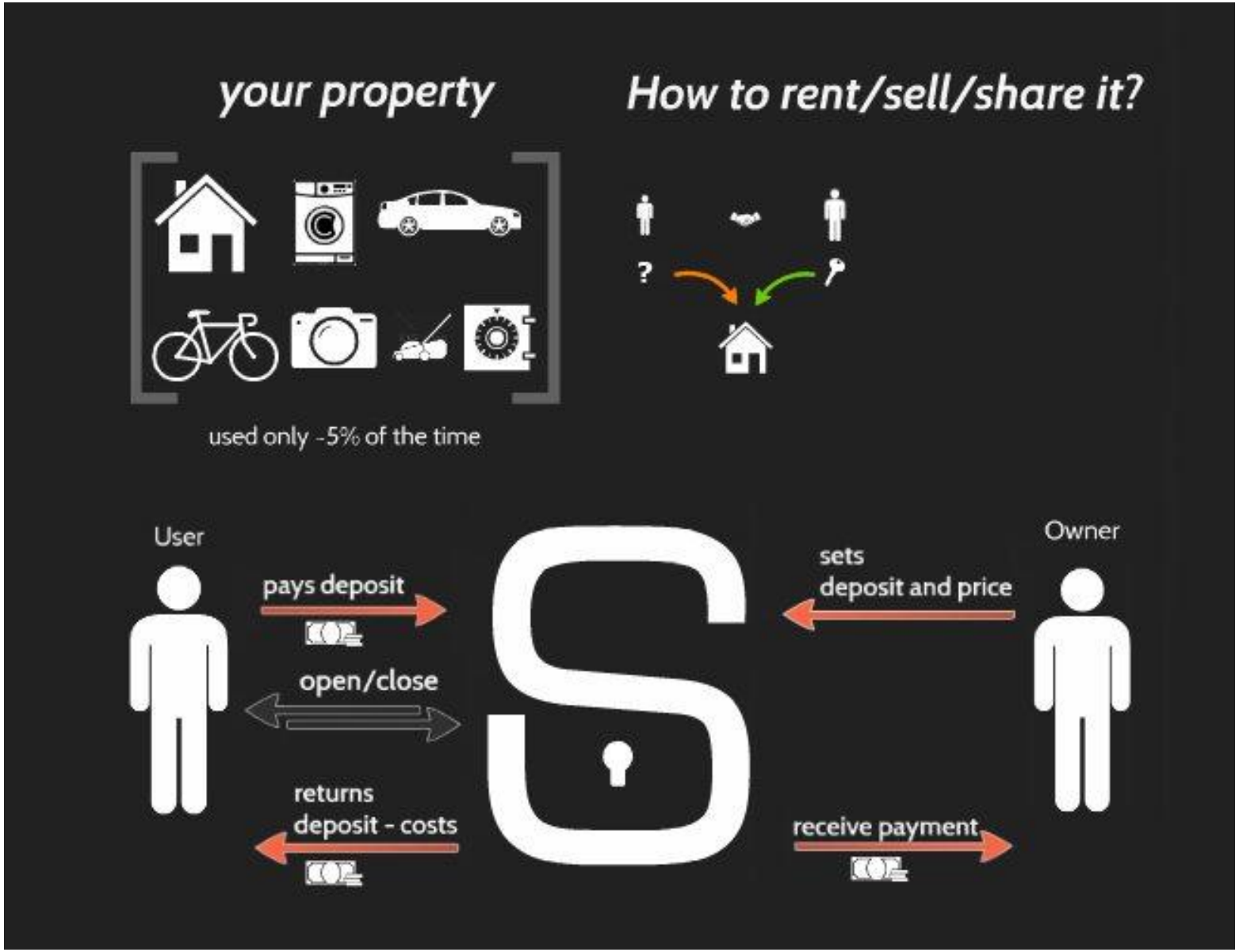
2. Homomorphic commitments can hide the amount of currency in billing transactions.

3. Zero knowledge proof are perfect tools to convert any information in a transaction into random ones to restrain any third party from obtaining even one bit of the information.

Sharing Service and Properties

Sharing services is one of the fundamental components in smart cities.

The sharing business model can not only improve the utilization of the properties but also save costs and resources.



Device Management

When the number of devices keeps proliferating, it is hard for the traditional client-server model to handle the issues.

Blockchain, which is based on elliptic curve cryptography, has a 160-bit identification address

Smart devices in IoT are identified by public keys, which are pseudonyms. Devices communicate with each other by transactions and can be verified by the signatures and public keys.

In block-chain model, a manufacturer puts the location of the firmware in a transaction on the blockchain.
Then the devices can automatically download the update and install as preset.

Supply Chain

Blockchain also provides supply chains for devices to be tracked at every point of the life cycle from manufacturers, shippers, and retailers to owners, and so on.

When the owner of the device changes (e.g., the device is resold), the key pairs for the device can be re-issued, which also needs a record on blockchain.

▶ Conclusion

IoT offers great convenience to people's daily lives by exchanging data and making comprehensive decisions.

It brings security and privacy concerns simultaneously.

Blockchain has potential in dealing with these security and privacy issues in IoT.

▶ Opinion

This paper analyzes the problems that can occur in the Internet of objects in the block chain. The framework presented in the paper is unclear.

I think it would have been nice to write a paper describing the time of medical data or streaming service in detail using the data sharing of the blockchain.

However, many of the above solutions will need to be written based on personal privacy and information security.