# Blockchain Based Credibility Verification Method for IoT Entities

Ganjargal Naranjargal

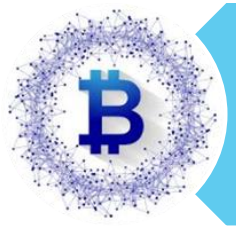
2019-5-7

# outline

- Abstract
- Introduction
- Related works
- Problem statement
- Credibility Verification Method
- Analysis and discussion
- Experiment and evolution
- Conclusion

The worldwide network of interconnection


The internet of things(IoT) is a system of interrelated computing devices mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.



The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.

# Abstract


- In recently, IoT has been used many important and various applications.
- But, it still faces many challenges in security and privacy. Blockchain (BC) technology, which underpins the cryptocurrency Bitcoin, has played an important role in the development of decentralized and data intensive applications running on millions of devices.
- In this paper, to establish the relationship between IoT and BC for device credibility verification, they propose a framework with layers, intersect, and self organizations Blockchain structures (BCS).
- In this new framework, each BCS is organized by Blockchain technology that describe the credibility verification method and show how it provide the verification.
- The efficiency analysis are also given in this paper, including its response time, storage efficiency, and verification.

# Introduction

- What is IoT?
  - The internet of things (IoT) is worldwide network of interconnected objects and humans, which through unique address schemes are able to interact with each other and cooperate with their neighbours to reach common goals.
- Challenges in IoT?
  - IoT devices require less energy, are lightweight and have less memory.

# Introduction

- What is Blockchain?
  - Blockchain (BC) is a distributed, decentralized, public ledger.
  - Blockchain (BC) technology allows all members to keep a ledger containing all transaction data and to update their ledgers to maintain integrity when there is a new transaction.
- Advantages of BC?
- Almost no transaction fee, p2p transactions without authorization by a third party.
- Ownership of the transaction information by many people makes hacking difficult, security expense is saved, transcations are automatically approved and recorded by mass participation, and promptness is assured.
- System can be easily implemented, connected and expanded using an open source and transaction records can be openly accessed to make the transactions public the reduce regulatory costs.
- Very difficult to falsify and alter the registered data.

# Related works

- The Blockchain technology first came to prominence in early 2009, through the cryptocurrency Bitcoin (BTC).
- Blockchain (BC) technology, which underpins the cryptocurrency Bitcoin, has played an important role in the development of decentralized and data intensive applications running on millions of devices.
- Since BTC has fourished, Blockchain, the technology that underpins BTC, could, according to Swan, have far-ranging consequences for all aspects of modern society.

- Such as applying BC to the smart home system to ensure the security and privacy of information, applying smart contract in IoT, using the BC platform to manage IoT devices, and made security transmission for IoT.
- The essence of Blockchain technology is a decentralized database for peer-to-peer networks, providing an effective trust mechanism.
- In the IoT environment, devices form a kind of peer-to-peer network, which is a decentralized application scenario the working conditions required by the Blockchain technology are meted.

# Problem statement

- The credibility verification of an IoT device refers to verifying that the target device has the attributes, such as location and function, that are known in the service-center and that the data the device transmits and receives has not been tampered with by a network attacker.
- The traditional security and to implement in an IoT environment mainly due to the follow reasons:

1. Asymmetric encryption needs a centralized key management system, which cannot meet the needs of a rapidly growing IoT system. Furthermore if the key management system is attacked a large number of IoT devices are likely to be affected.
2. Traditional security methods tend to be expensive for the IoT in terms of energy consumption and processing overhead because sensors are lightweight, of slow processing, and of less memory.

# Problem statement

- Although Blockchain technology can solve these problems, it sill faces the following critical challenges for application in IoT environment.
  1. POW calculation is particularly computationally intensive and time consuming , but the majority of IoT devices are resource restricted and most IoT applications need low latency.
  2. IoT networks are expected to contain a large number of nodes and have a rapidly increasing rate, so that the Blockchain scales poorly as the number of nodes in the network increases.
  3. The underlying Blockchain protocols create significant network traffic flow, which is a disaster for the communication of IoT devices.

# Credibility Verification Method

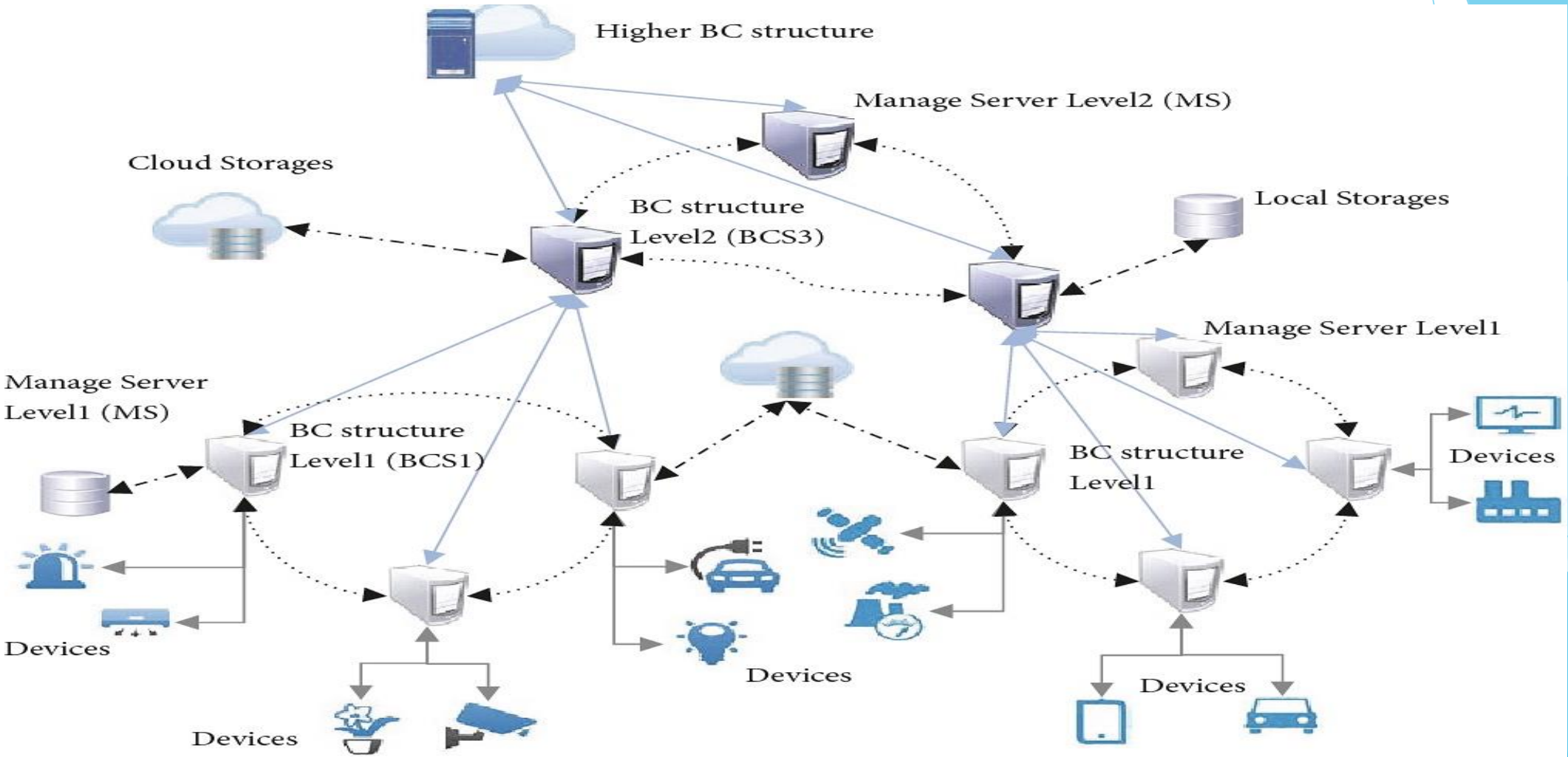



Figure1 : Overview of the credibility verification framework

# The Credibility verification network framework

- In the IoT scenarios, every application, such as a smart home, smart healthcare, and shared cycling, requires a server that manages the underlying devices, such as a smart home gateway, medical portal server, or shared platform.
- These servers have better computational ability than bottom IoT devices with limited resources and bandwidth.
- In addition these devices often work on cloud computing and cloud storage platforms and this have good storage capabilities and network communication capabilities.

# Manage server (MS)

Devices for managing and providing calculation and storage.

- MS is invoked in different BC structures depending on what position they are in. The bottom MS is directly connected with the device.
- Their responsibilities were to provide a Private Key and generate the Public Key for the device, store the device information, and published it to the Blockchain network responsible for the devices credibility verification.
- MSs in other positions were responsible for managing a number of lower-level and providing key pairs to accessed lower-level MSs storing their infromation.

- Other side the MSs managed by the same MS also formed a Blockchain network and each MS served as a Blockchain network node and acted as a miner.
- MSs published the “add” or “delete” information of entities as records to the Blockchain network where they formed.
- The information constructed Blockchain-blocks.

# BC structure (BCS)

- Different from the fact that all the nodes in the BTC network existed in the same blockchain network and all had peer-to-peer chracteristics, the credibility verification network had a plurality of blockchain networks composed of MSs.
- Each Blockchain networks was managed by one MS.
- Storage: The information BC-blocks can be stored in local storage or cloud storage.

# Credibility verification Data model

- In order to archive verification a corresponding data model needed to be established based on the orginal IoT data communication.
- For devices, the added data includes an ID and a Private key, where the ID was used as a unique identifier of devices to distinguish each other.
- The Private key is generated and issued by the MS which was responsible for managing the device.
- The additional data in the MS included the ID, Private key, and BC-blocks. Among them, the ID was the unique identifier of the MS.

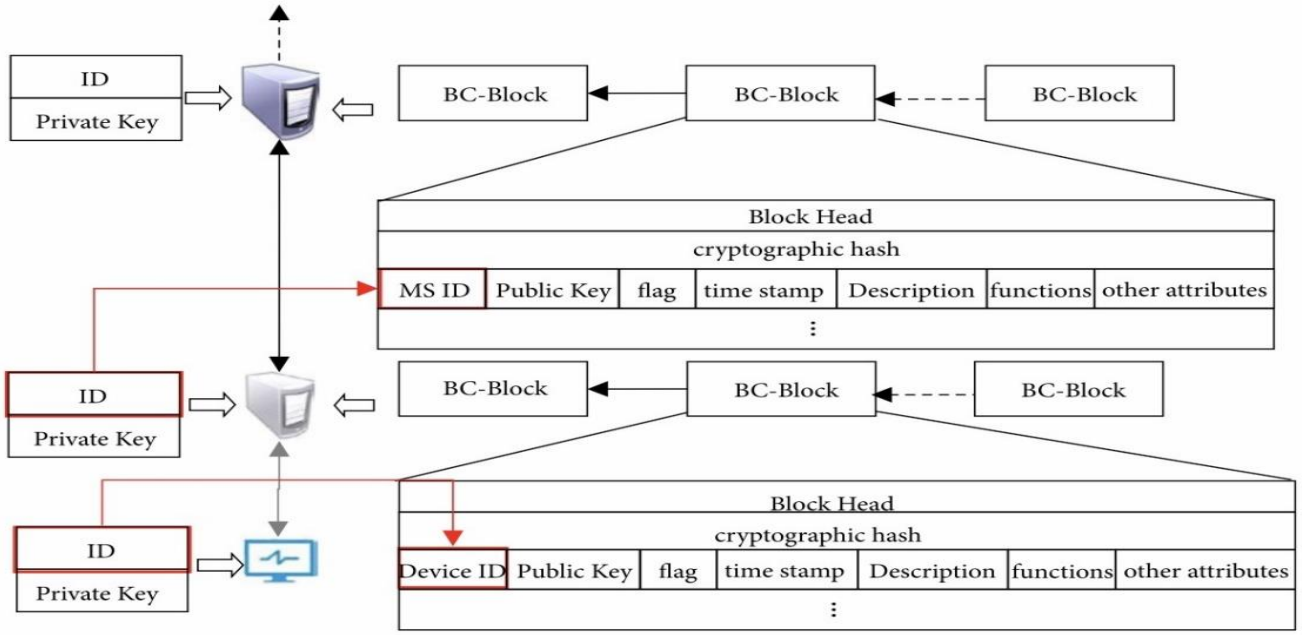



**Figure 2:** Data model for verification.

For devices, the added data includes an ID and a Private Key, where the ID was used as a unique identifier of device to distinguish each other.

The Private Key used for asymmetric encryption was used as the verification flag of device credibility.

The Private Key is generated and issued by the MS which was responsible for managing the device.

# Credibility Verification Process

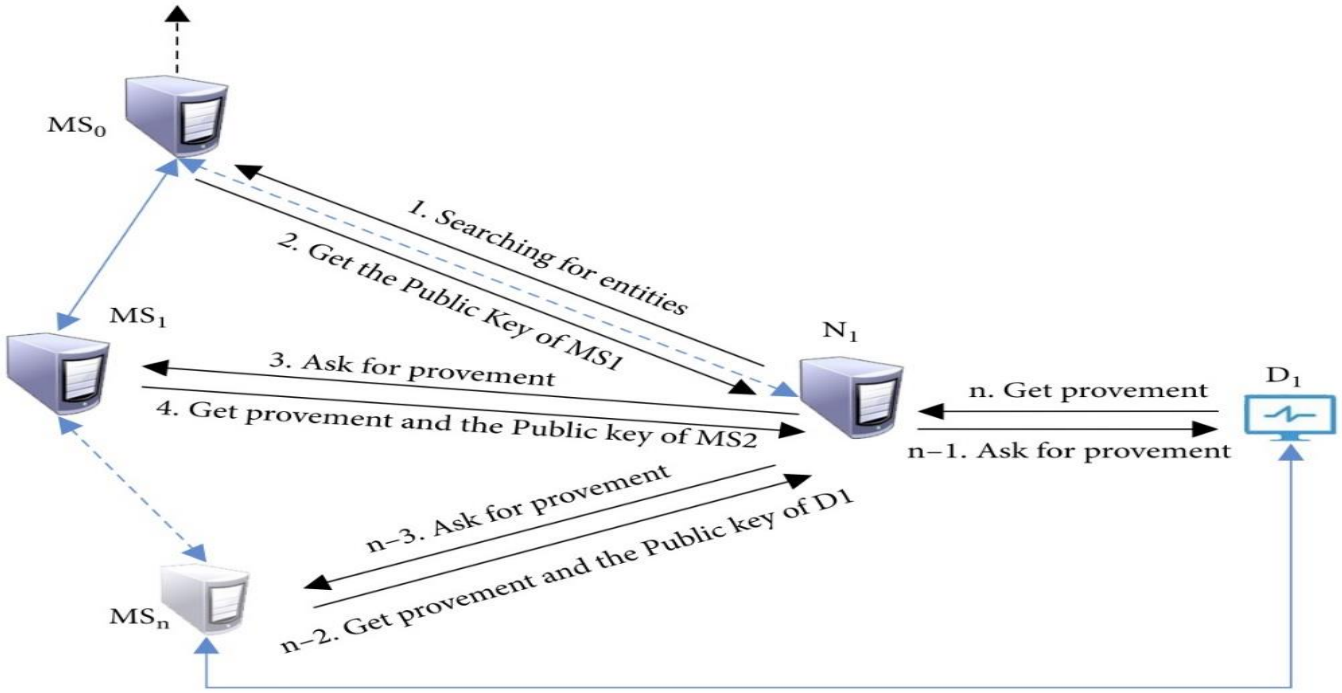



**Figure 3:** The process of verifying the device credible.

The MS1's ID and its Public Key are Obtained from MS0's BC-block-record.

A request is sent to MS1 to ask for the encrypted data by using the Private Key, and the identity is verified with the Public Key of MS1.
When MS1 is identified, we can get MS2's ID and the Public Key from its BC-block-record, using the same method to verify the credibility of MS2.

Steps 2-3 are repeated until the Public Key of D1 is obtained. Then a request is sent to D1 to ask for encrypted data and the resulting Public Key is used for verification

# Analysis and discussion

- The method presented in this paper is based on several intersecting Blockchain networks, and credibility is transmitted through Blockchain networks.
- Therefore, this method is reliable only if each Blockchain network can be proven trustworthy.
- When security of Blockchain technology lies in the sharing mechanism of its distributed data.
- The mining mechanism is defined so that when a node wants to tamper with certain records, it must recalculate the encryption hash of the entire BC thereafter.

- The computational workload is so great that cheating codes none of chance unless their processing power overtakes 51% of the whole network processing power, which is almost impossible.
- But Transactions (addition or deletion of entities) are generated too slowly to meet the security requirements at all.
- Resulting in excessive idle time and allowing the cheating node to have enough time to recalculate the entire BC.

# In this regard 3 solutions

1. Select the right size of each BCS and let the transaction record generation speed meet ”mining” requirements so that the counterfeit records costs are unacceptable.
2. Devices should send empty transaction records with a random probadibility, making the transaction records generation speed (real or empty) meet the “mining” requirement in each BCS.
3. When verifying the credibility of particular MS, several nodes are randomly selected from the BCSs are compared to the records in the MS(cryptographic hash can be used as well) to determine the credibility of the MS.

# Efficiency analysis

- In the current IoT environment credibility verification depends on the management center. Device information is obtained by querying the center.
- If the entire IoT environment is using Blockchain technology to archieve the credibility verification, the processing of synchronizing requires a large network overhead and response time.
- Because it needs to synchronize all the nodes in the network, the time complexity means 0(n).

# Efficiency analysis

- The proposed method is relatively complex with respect to the management center model(current IoT structure).
- Whole network model whole IoT environment organized by a big blockchain
  - The number of nodes in each BCS is (k)
  - An Iot environment with (n) nodes
  - The depth of the complete K-tree

# Experiments and Evolution

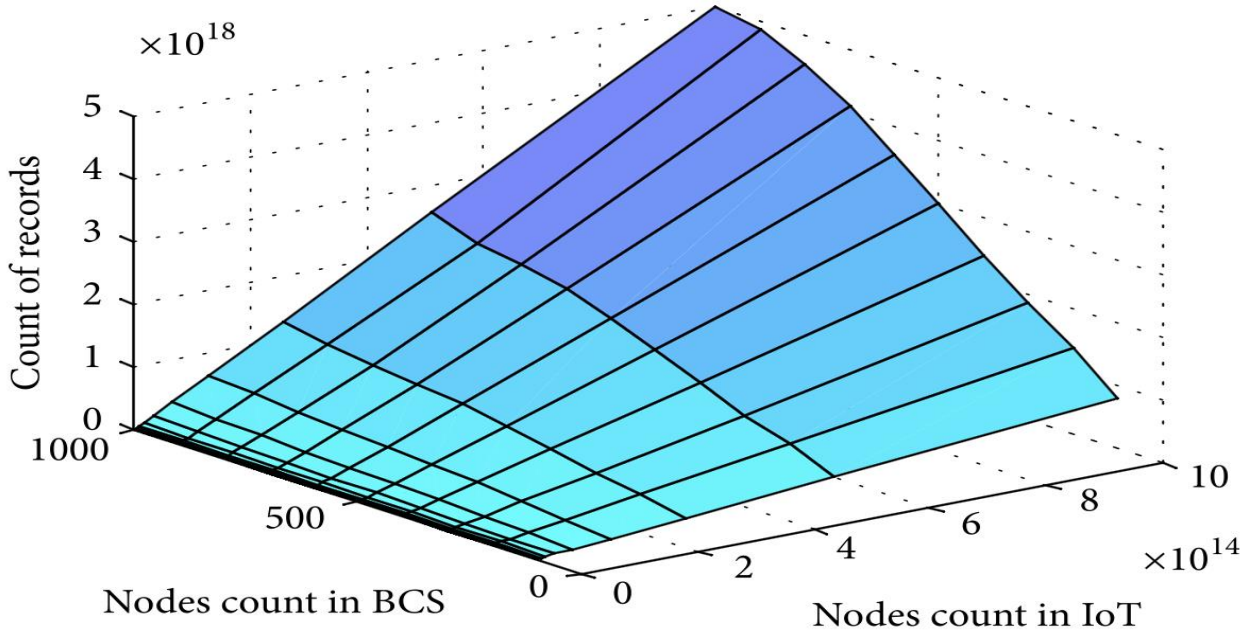



**Figure 4:** Storage capacity measurement with different K (node count in BCS) and n (node count in IoT).

# Experiment Records count

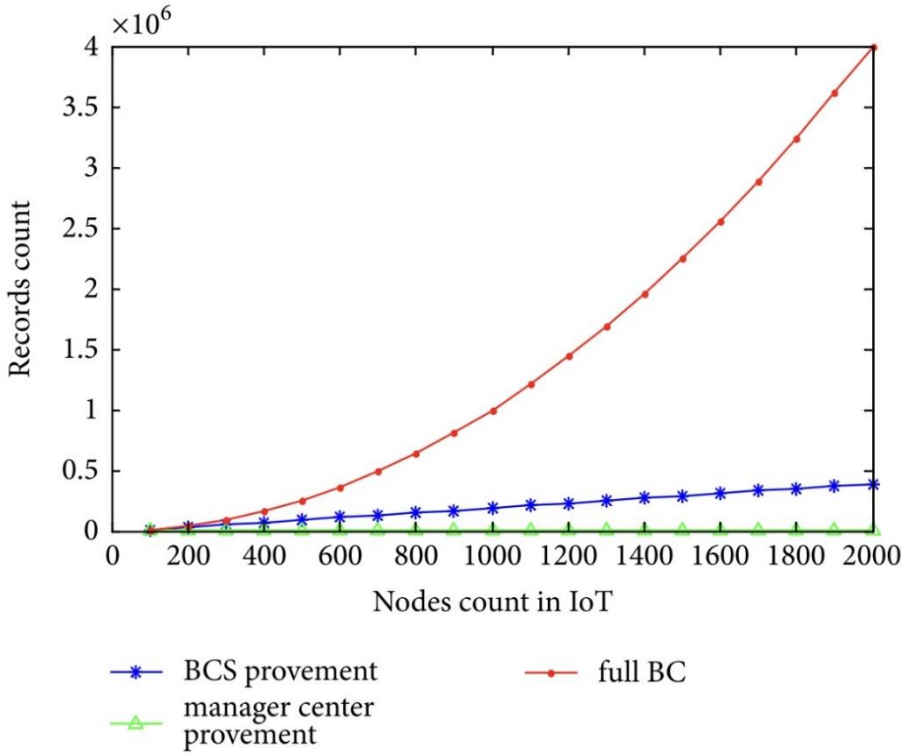



**Figure 5:** Comparison of storage efficiency.

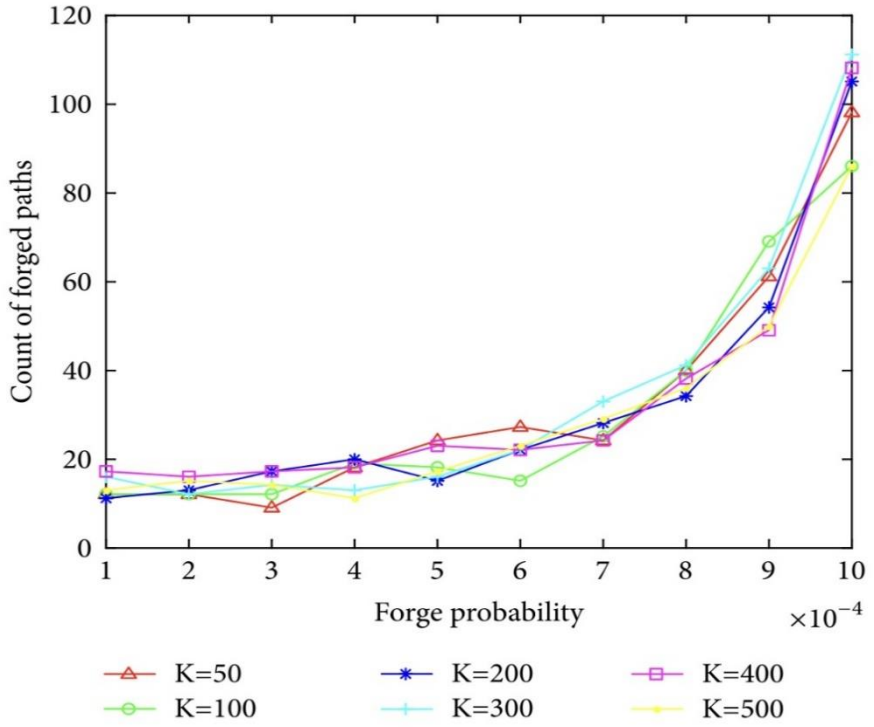



**Figure 6:** Paths with forged node.

# Experiment paths with forged node

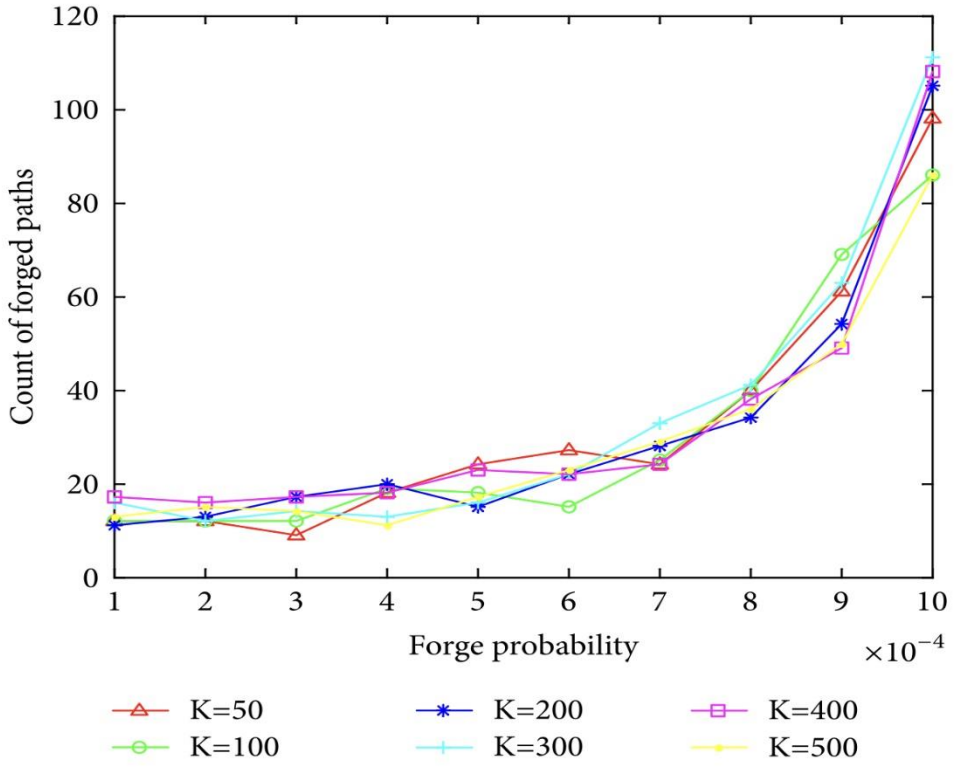
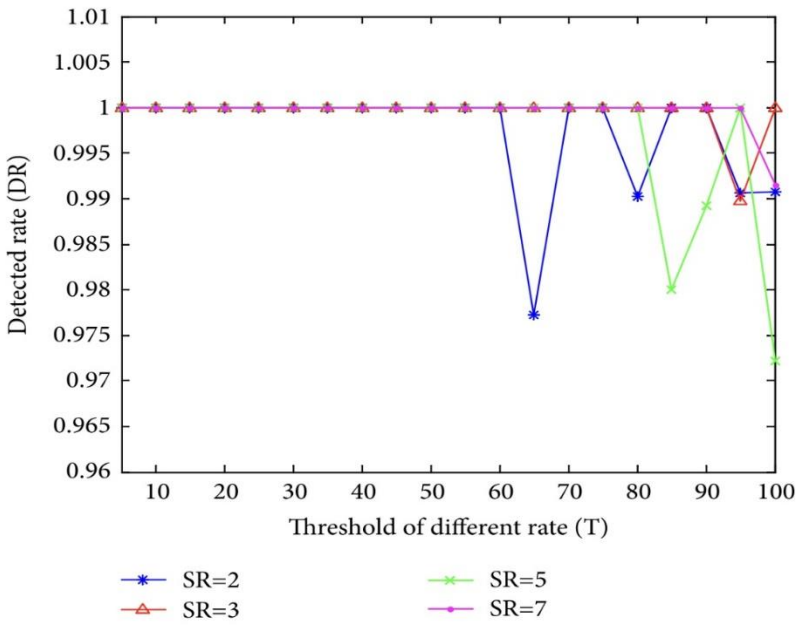
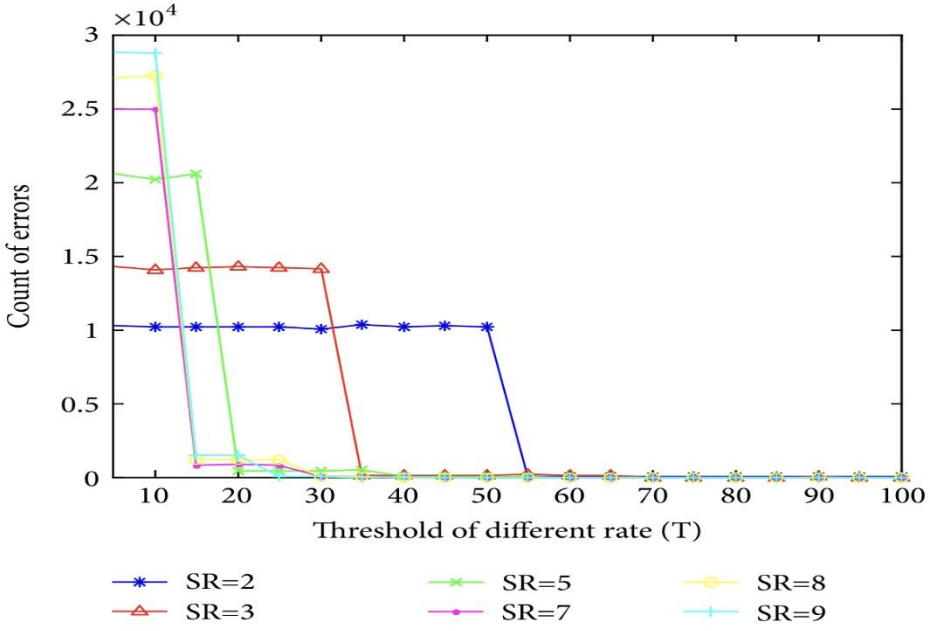



**Figure 6:** Paths with forged node.

# Experiment detected rate and error



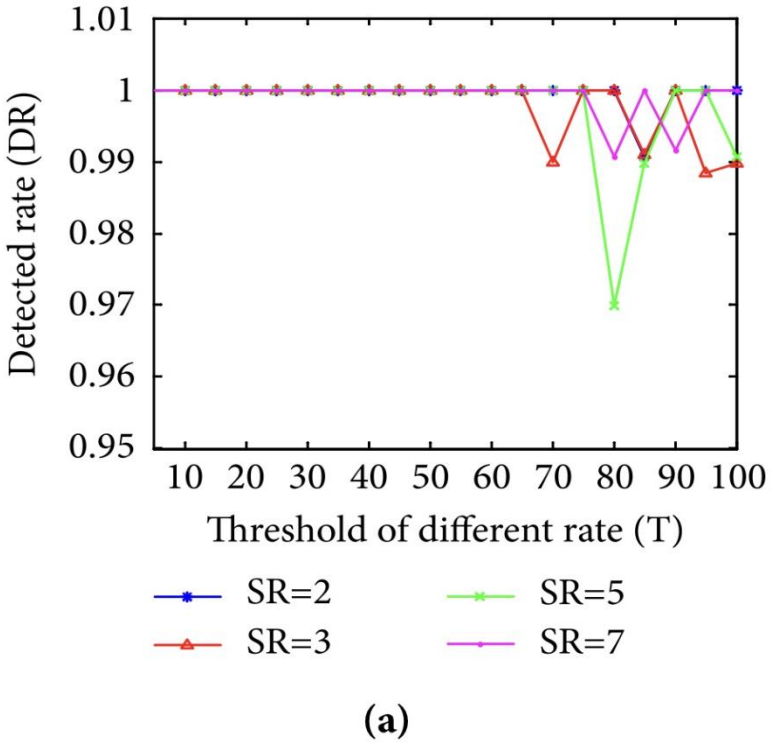

(a) Detected rate



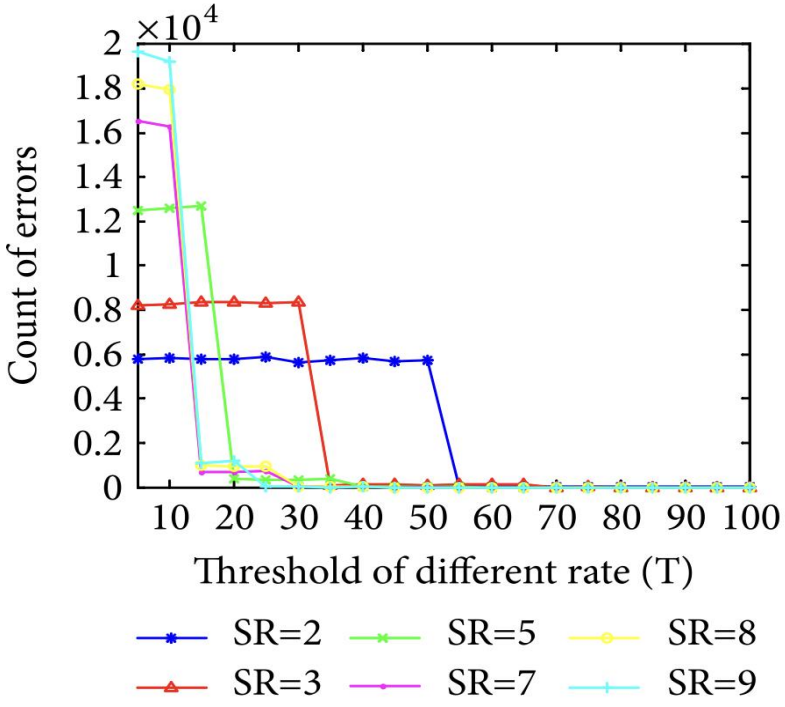

(b) Count of Errors

**Figure 7:** The experimental results of detected rete and error rate.

# Experiment detected rate count of errors

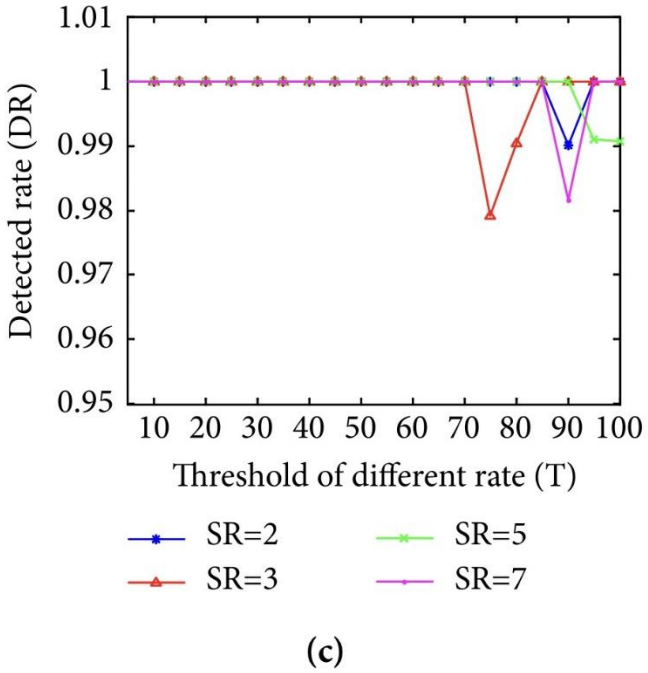



(a)

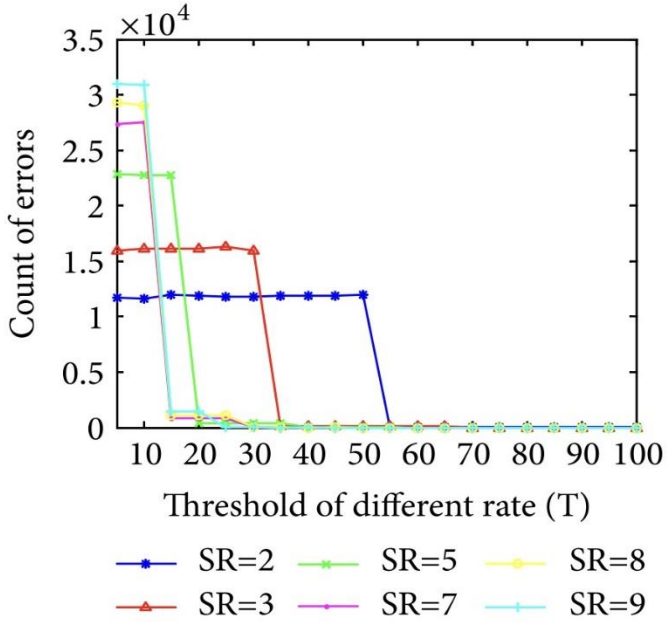



(b)

# Experiment detected rate count of errors

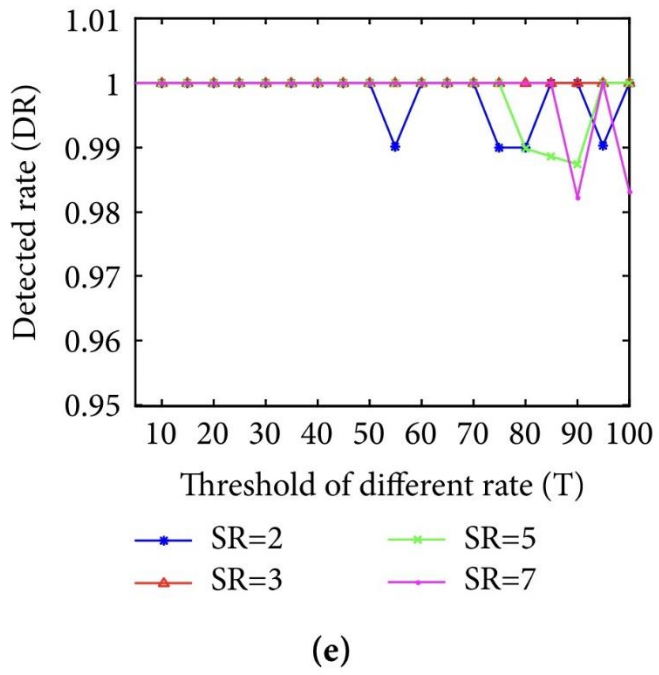



(c)

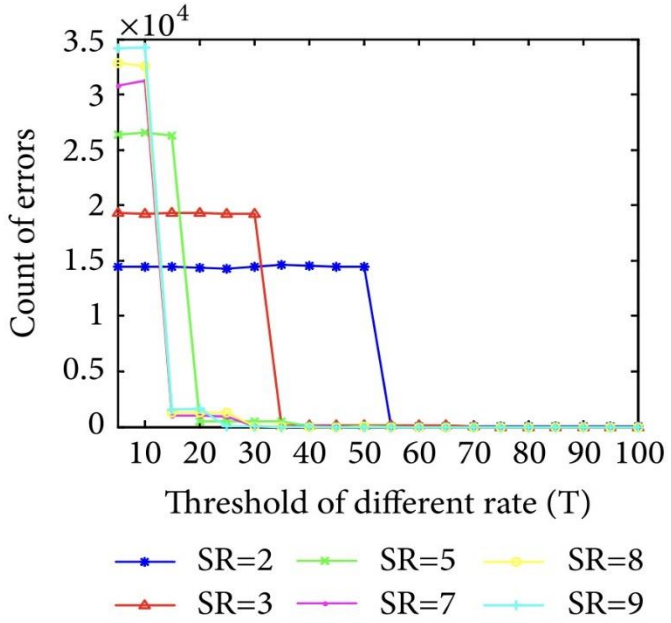



(d)

# Experiment detected rate count of errors

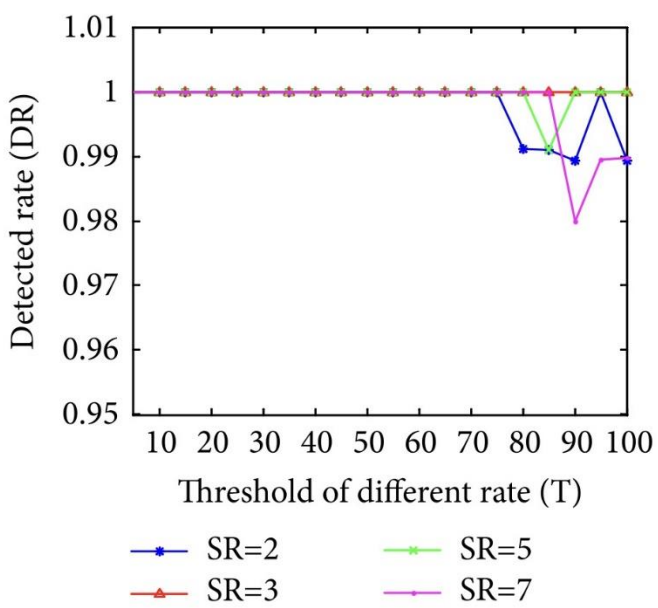



(e)

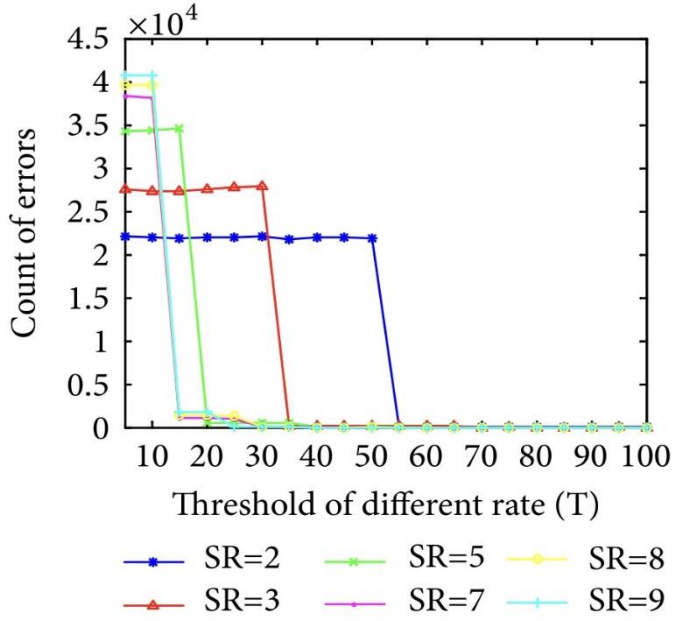



(f)

# Experiment detected rate count of errors




(g)




(h)

**Figure 8:** Detected rate and count of errors with different K: (a) and (b) $K = 200$; (c) and (d) $K = 400$; (e) and (f) $K = 500$; (g) and (h) $K = 1000$.

# Conclusion

In this paper was presented an IoT device credibility and discussed it in detail.

- With the continuous development of IoT technology  increasing attention the problems of security and credibility.
- The validity of the proposed model and method can reach the credible requirement by Blockchain technology and also has certain advantages in regard to storage space and response time.
- The 51% of the computation problem is still not effectively addressed and still threatens the entire network under such an attack.

# Opinion

In this