Nesnelerin İnterneti Aygıtlarının Görüşmelerinin Blok Zinciri

Araştırma Makalesi/Research Article

Davut ÇULHA

ASELSAN, Ankara, Turkey
culha@aselsan.com.tr

(Geliş/Received:19.08.2020; Kabul/Accepted:02.03.2021)
DOI: 10.17671/gazibtd.782857

Özet— Nesnelerin interneti (Nİ) aygıtlarının dünyası giderek büyümektedir. Bu aygıtların birbirleri arasındaki etkileşimi günden güne artmaktadır. Bu aygıtların etkileşimleri, birçok uygulama için değerli duruma gelmektedir. Bu aygıtların her bir özel ve uzamsal etkileşimi, onlar için bir görüşmedir. Bir Nİ görüşmesi için bu aygıtların birbirlerini kısa-uzaklık iletişim yoluyla doğrudan görmesi gerekmektedir. Bu çalışmada, Nİ görüşmeleri tutulmakta ve başkalarıyla paylaşılmaktadır. Nİ görüşme işlemleri dayanımlı olmalıdır. Bu amaçla, özel bir blok zinciri önerilmekte ve Nİ görüşmelerinin oluşması için gerekli düzenek tasarımı verilmektedir. Önerilen blok zinciri, Nİ görüşme işlemleri için İş Kanıtı uzlaşma düzeneğini kullanmaktadır. Veri bozulmasını engellemek için işlemler, Nİ aygıtları tarafından imzalanmaktadır. Blok zincirinde, sahip oldukları kaynaklara göre 5 tip aktör oluşturulmuştur. Bunlar, görüşme bildirimcisi, görüşme onaycısı, veri istekçisi, veri sağlayıcı ve kazıcıdır. Blok zinciri işlemleri, aktörlerin haklarını ve kişisel gizliliklerini korumak için tasarlanmıştır. Ek olarak, blok zinciri, kendi kriptoparasına sahiptir. Veri paylaşımını arttırmalarını ve görüşme işlemleri oluşturmalarını sağlamak için veri istekçisi dışındaki aktörlere, kriptopara ödülü verilmektedir.

Anahtar Kelimeler— nesnelerin interneti, Nİ aygıtlarının görüşmeleri, Nİ veri paylaşımı, Nİ kriptoparası, Nİ veri pazarı, Nİ blok zinciri

Blockchain of Meetings of IoT Devices

Abstract— The world of IoT devices grows day by day. The interaction of IoT devices increases day by day. Interactions of IoT devices become valuable for many applications. Each special and spatial interaction of IoT devices is a meeting for them. An IoT meeting requires that they should see each other directly via a short-distance communication channel. In this work, meetings of IoT devices are kept and exchanged with others. IoT meeting transactions should be reliable. For this purpose, a special blockchain is proposed, and formation mechanism of IoT meetings is designed accordingly. The proposed blockchain uses Proof-of-Work consensus mechanism to mine meeting transactions. Transactions are signed by IoT devices against data tampering. In the blockchain, 5 types of actors are formed according to their own resources. These are meeting declarer, meeting confirmer, data requester, data provider, and miner. The blockchain transactions are designed to protect privacy and rights of the actors. Moreover, the blockchain has its own cryptocurrency. Actors other than data requester are rewarded with cryptocurrency to increase the willingness of data sharing and to increase participation in forming meeting transactions.

Keywords— internet of things, meetings of IoT devices, IoT data exchange, IoT cryptocurrency, IoT data market, IoT blockchain

1. INTRODUCTION

Internet of Things (IoT) has many connected devices, and the number increases fast day by day. IoT forces science and technology to develop easier communication methods among IoT devices and intelligent mechanisms to better interact with each other. Many IoT devices and their intelligent interactions make systems smarter.

Cities and industries constitute an important part of IoT. Many IoT devices in cities and industries make them smarter. In smart cities, traffic systems become smarter. In other words, vehicles and other elements of traffic systems interact better with each other, and many operations are conducted automatically. Transportation becomes smarter. Security and reliability of transportation become crucial especially for dangerous and critical goods. Likewise, in smart industries, many operations are handled automatically. In industry, power management and their security and reliability are very important. For IoT security and reliability, blockchain technologies can be used.

Cars, drones, robots, and so on can be part of IoT. These devices are movable devices, and their interactions with other IoT devices generate some interaction data also. Each special and spatial interaction becomes a meeting among those IoT devices. IoT device meetings can be used in many applications. IoT device manufacturers can learn usages of their products. Transportation systems can be improved. Traffic systems can be enhanced. Traffic accidents can be analyzed. Therefore, IoT meeting data needs special attention. For reliability of IoT meeting data, blockchain technologies can be used. In this work, a special blockchain is proposed for IoT meetings.

Blockchain technologies bring trust to systems. However, usually they consume high energy and produce low throughput of transactions. The opposite is the common property of IoT devices. In other words, usually IoT devices consume less energy and produce many transactions. Therefore, the engagement of blockchain technologies and IoT produce additional challenges. In this paper, for keeping IoT meeting data, an additional actor named data provider is proposed.

Interaction of IoT devices, especially meetings among IoT devices are the main requirements for the applications which will use IoT meeting data. However, meetings of IoT devices do not produce enough IoT meeting data because of lack of trust and incentive. Owners of IoT devices do not want to share their data if the system is not trustful. Moreover, they do not want to publish their private information. Even if the trust is realized, they do not want to share information. Therefore, some incentive mechanism is also needed to get IoT meeting data. In this work, IoT device owners are rewarded for sharing data.

IoT devices and their interaction generate data. Especially, sensors as IoT devices generate a lot of data. This data is valuable and can be sold in a market. Similarly, IoT meeting data can be sold. In this paper, a marketplace mechanism is proposed for IoT meeting data, and a special cryptocurrency named CoinM is proposed for the marketplace. Trust in the mechanism, privacy and reliability of IoT meeting data are provided by blockchain technologies.

A meeting between two IoT devices is guaranteed with direct and small-distance communication channel like Wi-Fi. For a reliable IoT meeting, the two IoT devices should see each other directly, and they should be close enough to each other. These requirements can be met with Wi-Fi. There may occur many IoT meetings so the generated IoT meeting data should be managed carefully.

The proposed blockchain keeps mainly IoT meetings. Usually IoT devices are resource-limited devices. Typically, blockchain systems work with agents which have enough memory, storage and processing resources. The proposed blockchain is designed so that IoT devices can integrate to the blockchain with their limited resources. In other words, they are designed as being very thin clients for the blockchain network as much as possible. For this reason, 5 different roles are formed to distribute resource requirements. These are meeting declarer, meeting confirmer, data requester, data provider, and miner. The proposed blockchain creates an economy for IoT meeting data. For reliability and privacy of IoT meetings, transactions are designed using signing and hashing mechanisms. The blockchain has its own cryptocurrency CoinM to buy and sell the IoT meeting data. CoinM is also used as an incentive mechanism to incorporate IoT devices to the network because IoT devices earn some CoinM for sharing data. There can be enormous IoT devices and they can produce enormous IoT meeting data. For this huge data, the role data provider is created, which has enough storage spaces to keep IoT meeting data. Data providers manage IoT meeting data and sell it in return of some CoinM. Validated IoT meeting data is kept in the blockchain by miners, and miners earn some CoinM for their services. Some nodes in the proposed blockchain can carry out some of these roles concurrently.

The rest of this paper is structured as follows. In the next section, related work is given. Then, the proposed blockchain is described. Formation of IoT meetings and experimental results are followed by the future work. Lastly, conclusion comes.

2. RELATED WORK

The physical world is becoming more integrated to internet. In other words, increasing number of intelligent devices are connected to internet, and they describe their environment to other connected devices. Internet becomes huge, and the data transmission among them becomes enormous. This is IoT. IoT creates new opportunities and challenges to humanity because of this huge network and enormous data.

Cities become smarter as various IoT devices are deployed to public facilities of cities. In smart cities, the most important part is the traffic system. For intelligent traffic systems, each vehicle should be an IoT device and may include many IoT devices as well as other elements of city traffic system. Each vehicle can communicate with other vehicles via peer-to-peer networking. The interaction of each vehicle with other elements of the traffic system constructs a big network of vehicles. This is the Internet of Vehicles (IoV), which is a sub-internet of IoT [1]. IoV also creates a big amount of data. This data can be used to manage transportation. Secure, efficient and smart transportation can be constructed, which is called intelligent transportation. Intelligent transportation also provides road efficiency and safety especially for dangerous and critical goods. IoT devices can be used also for industrial applications like in factories. At that time, IoT devices are named as Industrial IoT (IIoT) devices, and factories are named smart factories where many operations are handled automatically [2]. For industry, power management is also very crucial. IIoT devices can be deployed also to plants to achieve secure transmission and management for power data.

IoV introduces important data which can be used in many applications related to manufacturers, maintenance service providers, insurance companies, and drivers. IoV data can be used to enhance vehicular services. The natural communication among vehicles is via peer-to-peer networking. Moreover, security of IoV data is very important. These two features can be supplied by blockchain technology which is the technology behind Bitcoin [3]. When blockchain technology is applied to IoV, IoV gains its required trust. The trust brings traffic safety and efficiency to IoV.

IoT is combined with blockchain for resilience and reliable data. In [2], blockchain-based data transmission technique is used among IIoT devices for the security of power data. Blockchain takes role to share transmission secrets of power data dynamically. Achieved security and reliability also realizes decentralization of trading centers, and results in management of power data efficiently. Likewise, power data, transportation of dangerous goods also needs security and reliability. In [4], blockchain is used to share sensitive data of transport activities of dangerous goods. Blockchain technology provides reliability and security to IIoT. However, blockchain technologies usually consume high energy and process low throughput of transactions. In contrast, IoT devices do not consume high energy and produces many transactions. In [5], to solve these issues a blockchain is proposed. The blockchain uses an efficient credit-based proof-of-work (PoW) mechanism. Moreover, a Directed Acyclic Graph (DAG) structure is employed to build the blockchain infrastructure to increase the throughput of the system. In [1], delegated proof-of-stake (DPoS) consensus algorithm is used in the blockchain for IoV. In order to empower the security of the blockchain, the consensus algorithm is improved according to the reputation of vehicles. IoV data is also important in case of traffic accidents. In order to unveil traffic accidents, the IoV data should be reliable. In [6], blockchain is used for IoV data, and its security is improved by introducing a special consensus algorithm named Proof-of-Physics (PoP). In [7], blockchain is used to increase road safety and efficiency of intelligent transportation. Identity of vehicles is verified using a signature scheme based on signatures of ring-based structure.

Number of IoT devices increases, data exchange among IoT devices increases, and number of applications using IoT data increases. However, amount of IoT data exchange is not satisfactory. IoT data exchange needs trust in the system. Otherwise, owners of IoT devices are not willing to share their data. In [8], an attribute-based access control scheme is proposed for IoT systems to simplify access management. Attributes are recorded in blockchain against single point of failure and data tampering. The blockchain decentralizes the access control mechanism, which increases the credibility of the system. In [9], a private blockchain is introduced to manage and monitor IoT devices securely. Configuration files of IoT devices are stored in blockchain that secures configuration changes. In [10], a permissioned blockchain is designed for self-driving cars, which is intended to be used for forensic analysis of traffic accidents. Privacy and membership of cars are realized using a special cryptography infrastructure named as Vehicular Public Key Infrastructure (VPKI). In [11], a blockchain based secure system is proposed to encourage vehicles for data sharing. In the blockchain, vehicles are rewarded with some cryptocurrency according to participation in data sharing. In [12], a reward system based on blockchain technology is proposed to provide secure and reliable information in IoV communication. In [13], a secure and auditable architecture is introduced for IoT data exchange. A prototype on Ethereum blockchain [14] is implemented using smart contracts. In [15, 16], methods are presented to store and share data among IoT devices. IOTA [17] is used as an underlying blockchain technology. In [18], integration of IoT and blockchain technologies is evaluated. Cybersecurity, data privacy, energy consumption, and scalability are some important challenges in IoT, which can be solved by applying blockchain technologies. However, some disadvantages of blockchain technologies like computational load and bandwidth should be considered carefully not to introduce new problems.

Data sharing among IoT devices is valuable for many applications. Producers, owners and service providers of IoT devices can benefit from IoT data in many kinds of applications. Likewise, the data in IoV can be used to improve traffic safety and efficiency. However, IoT devices may not be involved in sharing data even if a satisfactory environment for data security is provided. In [11], a secure blockchain infrastructure is proposed where vehicles in IoV are encouraged with some cryptocurrency to incentivize participation in data sharing. In [19], an effective announcement network named CreditCoin is proposed for smart vehicles in IoV. The blockchain guarantees the privacy of vehicles using an anonymous aggregation protocol. In addition, CreditCoin motivates vehicles to share traffic information and to forward traffic announcements.

Sensors can be IoT devices. In this case, the collected data of sensors can be sold in the network. This results in a market for sensor data, which is called sensor data market. Sensor data market can be generalized to include all IoT devices, which becomes IoT economy. For the IoT economy there should be a payment platform. In [20], the requirements of IoT payment systems are examined, and how those requirements can be fulfilled with blockchain technology in an effective manner is analyzed. In [21], a marketplace is implemented for IoT data on Ethereum blockchain. In [22, 23], usage of Bitcoin platform and its payment system are discussed to exchange IoT data. Cars and their many sensors also become part of IoT. Their collected data is valuable for many use cases. In [24], a survey is conducted to determine the willingness of people about sharing their own data. The results show that a critical amount of data can be collected from people using monetary rewards.

Each IoT device can generate some data. In addition, interaction of IoT devices can also generate data. Basically, each interaction is a meeting for IoT devices. Data about meetings are valuable and can be shared with others in return for some money [11]. An IoT meeting occurs among IoT devices when at least one IoT device is movable and the IoT devices are close enough to each other. Each meeting transaction should be non-repudiable for reliability.

Interaction among IoT devices can be realized using Wi-Fi communication, or similar small distance communication method. When two IoT devices can see each other directly, a meeting occurs. The two IoT devices should declare the meeting and it should be non-repudiable. Data among meetings should require additional data space so that there should some mechanism to keep the meeting data. For this purpose, there can be special meeting data providers. Data about meetings should be strong against data tampering so that meetings should be signed by IoT devices using their private keys. In [8], an attribute-based access control scheme is proposed for IoT systems. The scheme uses blockchain technology to avoid data tampering and single point of failure.

Access to meeting data can be authenticated. In [10], a permissioned blockchain is proposed to keep and manage vehicle related data. Vehicle related data can be used in many applications related to drivers, maintenance service providers, insurance companies, and manufacturers. A special public key infrastructure for vehicles is used to access to the permissioned blockchain. This framework is designed for forensic analysis. Traffic accidents can be analyzed using this framework. In [6], a permissionless blockchain is proposed, which uses PoP consensus mechanism to increase security of IoV data. If enough vehicles feed information to the blockchain, the blockchain can be used reliably for the analysis of past accidents.

3. THE PROPOSED BLOCKCHAIN

An IoT meeting occurs when two IoT devices see each other directly. IoT meetings can be used in many applications. Therefore, IoT meetings can be saved and exchanged by applications. In this work, a novel blockchain is proposed to store and trade IoT meeting data.

The proposed blockchain has 5 different actors. These are the followings:

- Meeting declarer: an IoT device
- Meeting confirmer: another IoT device
- Data provider
- Data requester
- Miner

An IoT meeting is realized by two different IoT devices which are meeting declarer and meeting confirmer. Meeting declarer initiates the IoT meeting data. The two IoT devices see each other via a short distance communication channel like Wi-Fi communication. One of them is declares the meeting and becomes the meeting declarer. The other IoT device confirms the meeting and becomes the meeting confirmer. When there is a confirmed meeting, the data providers store these meetings to sell. Data providers want to earn money and they have enough resources but IoT devices may have limited resources. Data providers have storage capacity whereas miners have processing capacity mostly. The proposed blockchain has its own cryptocurrency named CoinM. Data requesters can request IoT meeting data with a query in return for some CoinM. If data providers satisfy the data request, then data providers create an IoT meeting transaction. The meeting transactions are recorded in the blockchain by miners. For each IoT meeting transaction, a data requester pays some CoinM to the IoT devices, to the data provider, and to the miner. This fee system provides IoT devices to sell their meeting data, data providers to keep IoT meeting data, and miners to store validated meeting data immutably. If a request to IoT meeting data is resulted with a transaction in the blockchain, then it is called an IoT meeting blockchain transaction.

The steps of creation of an IoT meeting blockchain transaction are the followings:

1. An IoT device sees another IoT device directly. Then, it creates an IoT meeting declaration because of being rewarded with some CoinM and becomes the meeting declarer.
2. The other IoT device sees the IoT meeting declaration while seeing the meeting declarer directly. Then, the IoT device confirms the IoT meeting declaration by creating an IoT meeting confirmation because of being rewarded with some CoinM and becomes the meeting confirmer. The meeting confirmer sends the confirmation to the meeting declarer.

3. The meeting declarer takes the confirmation and signs it so that the IoT meeting data is fixed and cannot be changed later. The meeting declarer broadcast the fixed IoT meeting declaration to the blockchain network.
4. When a data provider sees a fixed IoT meeting declaration, it stores it to sell to data requesters because of being rewarded with some CoinM.
5. When a data requester requests a special IoT meeting data, it creates an IoT meeting data request by offering some CoinM to the related actors.
6. When a data provider satisfies an IoT data meeting request, it creates an IoT meeting transaction for the blockchain because of being rewarded with some CoinM.
7. When a miner sees an IoT meeting transaction, it checks for validity, signs it, and adds the transaction to the blockchain because of being rewarded with some CoinM.

Every step of an IoT meeting blockchain transaction is checked by the related actor to validate the IoT meeting. After validation, they progress the formation of the IoT meeting blockchain transaction.

4. FORMATION OF IoT MEETINGS

In the proposed blockchain, IoT meetings are added to the blockchain using PoW consensus mechanism.

Meeting data is simplified to manage easily. The basic meeting data includes the following:

- The time of the meeting (T)
- The GPS position of the meeting (P)
- The meeting declarer (D)
- The meeting confirmer (C)

The first two elements of meeting data are simplified to manage easily. The first element is based on Unix epoch time. The Unix epoch time is converted to times slices of 10 minutes. In other words, it is divided by 600, and its integer part is taken. If two IoT devices meet, they should be in the same time slice. Time slice information can be kept in 4 bytes.

The second element is the position of an IoT meeting. To simplify the position information, the world is assumed to consist of 10-meter square slices. To approximate position slices, Virtual Earth's Tiling System [25] is used. 14 levels in the tiling system indicate nearly 10-meter squares. Therefore, the GPS position of an IoT meeting is converted to 14 level latitude and longitude values. Each level is kept with 1 bit. Therefore, these two values can be kept also in 4 bytes. If two IoT devices meet, they should be in the same GPS position slice.

When there is an IoT meeting, one of the IoT devices will declare the meeting as the following:

Formula (1): Meeting declarer: $D\ C\ T\ P\ D_0\ D_a$

where

D is the public key of meeting declarer,

C is the public key of meeting confirmer,

$D_0 = H(D\ C\ T\ P)$,

$H(x)$ is SHA256 hash of x,

$D_a = D_g(D_0)$, and

$Y_g(x)$ is the signature of signing of x by Y.

In Formula (1), hash function is used to obtain a unique key for the basic meeting data. The key will help to hide private data of IoT devices. Meeting declarer is confirmed by a meeting confirmer if there is an IoT meeting. The meeting confirmer sends the following message to the meeting declarer:

Formula (2): Meeting confirmer: $D\ C\ T\ P\ D_a\ C_a$

where

$C_a = C_g(D_0)$.

After the IoT meeting is confirmed, the meeting declarer fixes it by signing, and broadcasts the following IoT meeting confirmation to the blockchain network:

Formula (3): Meeting declarer: $D\ C\ T\ P\ D_0\ D_a\ C_a\ D_f$

where

Df = Dg(Ca).

In Formula (3), basic meeting data is fixed by the meeting declarer. After this point, no one cannot change the meeting data because it is signed by IoT devices. This mechanism prevents data tampering. Data providers listens the blockchain network. When they see a fixed IoT meeting confirmation, they store the meeting data to their internal databases.

A data requester requests an IoT meeting data by sending a message like the following:

Formula (4): Data requester: $D\ C\ T\ P\ N\ R_0\ R_a$

where

N is the amount of reward CoinM for each actor,

R is the public key of data requester,

$R_0 = H(D_0\ N)$, and

$R_a = R_g(R_0)$.

Data providers listen the blockchain network. When they see a satisfiable request, they broadcast the following blockchain transaction to the blockchain network:

Formula (5): Data provider: $D\ C\ D_0\ D_a\ C_a\ D_f\ N\ R_0\ R_a\ P_a$

where

P is the public key of data provider, and

$P_a = P_g(R_0)$.

In Formula (5), the data provider does not publish the time and position elements of basic meeting data. Therefore, privacy of IoT devices are assured. Miners listen the blockchain network. When they see a blockchain transaction request, they control it for validity. If the transaction request is valid, they create the following blockchain transaction, adds it to the blockchain, and broadcast the transaction to the network.

Formula (6): Miner: $D\ C\ D_0\ D_a\ C_a\ D_f\ N\ R_0\ R_a\ P_a\ N_w(R,D)\ N_w(R,C)\ N_w(R,P)\ N_w(R,M)\ M_0\ M_a$

where

$N_w(x,y)$ is transfer of N CoinM from x to y,

M is the public key of miner,

$M_0 = H(R_0\ N_w(R,D)\ N_w(R,C)\ N_w(R,P)\ N_w(R,M))$, and

$M_a = M_g(M_0)$.

In Formula (6), miners try to add the transaction to the blockchain. However, they do not know the details of IoT meeting. In other words, they cannot learn the time and position data of IoT meetings. Therefore, privacy of IoT devices is provided using this mechanism. Miners listen blockchain transactions. When they see a blockchain transaction, they check it for validity. They apply the following validity rules to the transaction:

- D_a should be a valid signature of D for D_0.
- C_a should be a valid signature of C for D_0.
- D and C should be different.
- D_f should be a valid signature of D for C_a.
- R_0 should be the hash of D_0 N.
- R_a should be a valid signature of R for R_0.
- P_a should be a valid signature of P for R_0.
- M_0 should be the hash of $D_0\ R_0\ N_w(R,D)\ N_w(R,C)\ N_w(R,P)\ N_w(R,M)$.
- M_a should be a valid signature of M for M_0.
- R should have more than 4*N CoinM in its account.

If all these rules are valid and D_0 is not used in the previous transactions of the blockchain, then they add the transaction to their own copy of the blockchain and broadcast it to the whole blockchain network. Therefore, the same meeting data cannot be sold more than once.

The data requester searches the blockchain for its request using the key D_0. When it finds the key, it will understand that D and C IoT devices met at the time slice T and in the location slice P. Others will not understand the meeting time and position from the blockchain because they cannot see T and P data. In brief, the privacy of IoT meeting is guaranteed in the blockchain.

5. EXPERIMENTAL RESULTS

The proposed blockchain is implemented with a program in python. The blockchain structure is designed like bitcoin blockchain. There are blocks, and they are connected. Each block has a header with the following fields:

- Index: keeps the height of the block in the blockchain
- Timestamp: keeps the creation time in Unix epoch time
- Nonce: a random value for PoW
- Previous: keeps the hash value of the previous block header
- Transactions: keeps the IoT meeting transactions

The blockchain is initialized with 1000 IoT devices. Each IoT device has a private key for signing transactions. The IoT meeting transactions are constructed randomly from these IoT devices. 50 data requesters and 10 data providers are defined. Each of them also has private keys for signing transactions. Threads are used in the implementation of 100 miners.

Data requesters create random requests about two IoT devices. Some of the requests are fulfilled by data requesters. In this way, IoT meeting transactions are formed, and each of them is signed by the two IoT devices, the data requester and the data provider. In the blockchain, each block is limited up to 25 transactions. From the pool of IoT meeting transactions, 20-25 transactions are selected randomly to create candidate blocks. Miners work on the candidate blocks to find the required hash value pattern for PoW. If a miner finds the solution, the candidate block is added to the blockchain.

Each request has a fee value field for rewarding. The fee is fixed to 1, which means that each of the two IoT devices, the data provider and the miner earns 1 CoinM from the IoT meeting transactions. In other words, data requesters pay 4 times the value in the fee field.

The program was executed up to 1000 blocks. Totally 22454 IoT meeting blockchain transactions were formed. Data requesters paid 89816 CoinM to the IoT devices, the data providers, and the miners. 44908 CoinM was earned by the IoT devices. 22454 CoinM was earned by the data providers, and another 22454 CoinM was earned by the miners.

6. FUTURE WORK

The proposed blockchain is designed to search meetings of IoT devices using public keys for a specified time slice and a specified location slice. First of all, IoT devices can be extended with other properties like producer identification key, IoT type, production year, factory place, and so on. Moreover, for time slices and for location slices, searches can be conducted within ranges. Additionally, an expressive search language like SQL can be designed for querying IoT meeting data. Above all, exact values of time and position data can be used instead of slice data.

In this work, access to the IoT meeting data is not limited. IoT meeting data is accessed by others in return for some cryptocurrency. The access to the IoT meeting data can be limited with additional criteria to increase the privacy.

In this paper, a direct communication of IoT devices are accepted as meetings. In the future, when the GPS positions of IoT devices are guaranteed as correct by additional mechanisms, indirect communication of IoT devices like internet communication can generate IoT meetings.

In the blockchain, PoW consensus algorithm is used. IoT transactions can be enormous so that faster algorithms like DPoS can be used.

In this work, meetings are considered as two-party meetings. As a future work, a blockchain can be designed for meetings of more than two IoT devices. In this paper, simple rewarding system is used. As a future work, the rewarding system can be extended to increase the willingness of actors for sharing data. In this work, as a position data, two dimensions are used. As a future work, the third-dimension altitude can be added.

7. CONCLUSION

Interactions of IoT devices are valuable for many applications. Each special and spatial interaction of IoT devices is a meeting for the IoT devices. In this work, a special blockchain is proposed to exchange and trade IoT meeting data. Basically, an IoT meeting is declared by two IoT devices. They should see each other directly via a short-distance communication channel like Wi-Fi. They declare their meeting including time and position information. They sign the meeting against data tampering.

IoT devices usually do not have big storage spaces. Therefore, for keeping IoT meeting data, a special actor named data provider is proposed in the blockchain. Data provider collects IoT meeting data and share it with other in return for CoinM.

In the blockchain, there are 5 types of actors as meeting declarer, meeting confirmer, data requester, data provider, and miner. Moreover, the blockchain has its own cryptocurrency named CoinM. CoinM is used to contribute generation and exchange of IoT meeting data. IoT devices are rewarded with CoinM to share their meetings. Data providers are rewarded with CoinM for keeping IoT meeting data. Miners are rewarded to generate reliable data.

Formation of IoT meeting data is formulized using hashing and signing mechanisms to enable reliability and privacy of IoT meetings.

Miners listen blockchain transactions. When they see a blockchain transaction, they check it for validity. If it is valid, they try to add the transaction to the blockchain. However, they do not know the details of IoT meeting because the transaction only keeps a unique key of the IoT meeting. In other words, they cannot learn the time and position data of IoT meetings. Therefore, privacy of IoT devices is provided using this mechanism. Moreover, the proposed blockchain guarantees that the data requester will only see the requested correct data after paying the fee.

REFERENCES

[1] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, J. Zhao, “Towards Secure Blockchain-enabled Internet of Vehicles: Optimizing Consensus Management Using Reputation and Contract Theory”, *IEEE Transactions on Vehicular Technology*, 2019.

[2] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, K. C. Li, “A Secure Fabric Blockchain-based Data Transmission Technique for Industrial Internet-of-Things”, *IEEE Transactions on Industrial Informatics*, 2019.

[3] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”, *Bitcoin*, 2008.

[4] A. Imeri, N. Agoulmine, D. Khadraoui, “A secure and smart environment for the transportation of dangerous goods by using Blockchain and IoT devices”, 2019.

[5] J. Huang, L. Kong, G. Chen, M. Y. Wu, X. Liu, P. Zeng, “Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism”, *IEEE Transactions on Industrial Informatics*, 2019.

[6] J. Joy, “Vehicular blocktrees”, **2017 IEEE Vehicular Networking Conference (VNC)** (147-150). IEEE, 2017 November.

[7] J. A. L. Calvo, R. Mathar, “Secure Blockchain-Based Communication Scheme for Connected Vehicles”, **2018 European Conference on Networks and Communications (EuCNC)** (347-351), IEEE, 2018.

[8] S. Ding, J. Cao, C. Li, K. Fan, H. Li, “A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT”, *IEEE Access*, 7, 38431-38441, 2019.

[9] K. Košťál, P. Helebrandt, M. Belluš, M. Ries, I. Kotuliak, “Management and Monitoring of IoT Devices Using Blockchain”, *Sensors*, 19(4), 856, 2019.

[10] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, S. Uluagac, “Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles”, *IEEE Communications Magazine*, 56(10), 50-57, 2018.

[11] L. Zhang, M. Luo, J. Li, M. H. Au, K. K. R. Choo, T. Chen, S. Tian, “Blockchain based secure data sharing system for Internet of vehicles: A position paper”, *Vehicular Communications*, 2019.

[12] M. Singh, S. Kim, “Trust Bit: Reward-based intelligent vehicle commination using blockchain paper”, **2018 IEEE 4th World Forum on Internet of Things (WF-IoT)** (62-67), IEEE, 2018.

[13] Z. Huang, X. Su, Y. Zhang, C. Shi, H. Zhang, L. Xie, “A decentralized solution for IoT data trusted exchange based-on blockchain”, **2017 3rd IEEE International Conference on Computer and Communications (ICCC)** (1180-1184). IEEE, 2017.

[14] G. Wood, Ethereum: “A secure decentralised generalised transaction ledger”, *Ethereum project yellow paper*, 151, 1-32, 2014.

[15] B. C. Florea, “Blockchain and Internet of Things data provider for smart applications”, **2018 7th Mediterranean Conference on Embedded Computing (MECO)** (1-4), IEEE, 2018.

[16] O. Lamtzidis, J. Gialelis, “An IOTA Based Distributed Sensor Node System”, **2018 IEEE Globecom Workshops (GC Wkshps)** (1-6), IEEE, 2018.

[17] S. Popov, “The tangle”, *White Paper*, 2017.

[18] M. Maroufi, R. Abdolee, B. M. Tazekand, “On the Convergence of Blockchain and Internet of Things (IoT) Technologies”, *arXiv preprint arXiv:1904.01936*, 2019.

[19] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, Z. Zhang, “CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles”, *IEEE Transactions on Intelligent Transportation Systems*, 19(7), 2204-2220, (2018).

[20] I. C. Lin, T. C. Liao, “A Survey of Blockchain Security Issues and Challenges”, *IJ Network Security*, 19(5), 653-659, 2017.

[21] K. R. Özyilmaz, M. Doğan, A. “Yurdakul, IDMoB: IoT Data Marketplace on Blockchain”, **2018 Crypto Valley Conference on Blockchain Technology (CVCBT)** (11-19), IEEE, 2018.

[22] K. Noyen, D. Volland, , D. Wörner, E. Fleisch, “When money learns to fly: Towards sensing as a service applications using bitcoin”, *arXiv preprint arXiv:1409.5841*, 2014.

[23] D. Wörner, T. von Bomhard, “When your sensor earns money: exchanging data for cash with Bitcoin”, **Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication** (295-298), ACM, 2014.

[24] A. Dahlinger, B. Ryder, F. Wortmann, “Car as a Sensor. Paying people for providing their car data”, **Proceedings of the 5th International Conference on Internet of Things, Seoul, South Korea. 5th International Conference on Internet of Things**, 2015.

[25] Internet: Bing Maps Tile System, http://msdn.microsoft.com/en-us/library/bb259689.aspx, 29.08.2019.