

A Decentralized Solution for IoT Data Trusted Exchange Based-on Blockchain

Zhiqing Huang*, Xiongye Su

Faculty of Information Technology, Beijing University
of Technology, Beijing
Beijing Engineering Research Center for IoT Software
and System
Beijing, China
e-mail: zqhuang@bjut.edu.cn

Yanxin Zhang

Advanced Control Systems Laboratory, School of
Electronic and Information Engineering
Beijing Jiaotong University
Beijing, China
e-mail: yxzhang@bjtu.edu.cn

Changxue Shi, Hanchen Zhang

Faculty of Information Technology, Beijing University
of Technology, Beijing
Beijing Engineering Research Center for IoT Software
and System
Beijing, China
e-mail: charlotte@emails.bjut.edu.cn

Luyang Xie

Faculty of Information Technology, Beijing University
of Technology, Beijing
Beijing Engineering Research Center for IoT Software
and System
Beijing, China
e-mail: 570878956@qq.com

Abstract—Internet of Things (IoT) plays an important role in the development of various fields. The increasing scale and scope of applications make a great demand of IoT data exchange in recent years. Meanwhile, a number of IoT data exchange platforms which dedicated to connecting various and distributed data sources are emerging. In such a platform, service providers can search and exchange the data sets that they need. However, the centralized infrastructure cannot provide enough trust as the third-party intermediaries for data exchange. As a result, most platforms unable to satisfy the complex requirements due to few institutions and individuals are willing to share their IoT data sets in such an untrustworthy environment. This paper proposes a decentralized solution based on the blockchain for IoT data trusted exchange. Specifically, In this paper, the basic principles of blockchain and corresponding key technologies are expounded through in-depth analysis of three main reliable requirements in IoT data exchange. Besides, this paper provides an architecture of above solution and detailed design of its main trust component. Finally, it realizes a prototype by using Ethereum blockchain and smart contracts and presents its auditable, transparent, decentralized features visually.

Keywords—IoT data; Trusted Exchange; Blockchain; Smart Contracts

I. INTRODUCTION

Over the past decade, benefiting from the rapid development of wireless communication technology, sensing technology and the improvement of big data analysis capacity [1], the Internet of Things (IoT) is growing with incredible speed in most areas, especially in healthcare [2], smart city [3] and autonomous vehicles [4]. As the essential elements of the IoT world, data collected from various devices can be applied in a wide range of areas after being

analyzed and processed. Combining with advanced technologies such as big data and artificial intelligence [5], IoT service based on data not only reduces the cost of industry and agriculture and makes the devices around people more intelligent, but also repeatedly optimizes the IoT ecosystem (security, equipment management and the standardization [6]) itself. However, due to the limited high maintenance and management cost [7], restricted collecting scope in privacy data, data exchange between individual and organizations become irreversible trend when they realize that connection is more important than possession [8]. Therefore, a lot of data exchange or sharing platform have emerged in the past years. Such as crowdad for archiving wireless data [9], data science central provided industry's online resources for big data practitioners, data.gov as the home of the US government's open data platform, the development of digital coast met the unique needs of the coastal management community [10,11]. Most of them concentrated on data of the same kind or a specific field and led by government or the unions of large institutions. However, the data sets on such centralized platform cannot meet the public's diversified demands, largely due to they cannot provide enough trust to guarantee the transparency, auditable, immutable in data exchange process.

It has been watched by researchers for a long time, as the issue of trust kills the enthusiasm to share data actively and seriously hampers the development of the data industry [12]. Although current platforms integrate a lot of confidentiality mechanisms (access control, authorization privacy) and propose some trust model for data sharing in IoT, they are not break away from the third party [13].

In order to guarantee IoT data exchange in a completely trusted, transparent environment, we propose a decentralized solution based-on blockchain. As the core technology in

Bitcoin, blockchain soon came to be widely attracted attention and application for its trust property[14].

The core advantage of blockchain is decentralization. It consists of data encryption, timestamp, distributed consensus algorithm, economic incentive mechanism and other technology. It is applicable to the point-to-point transaction based on decentralized credit in distributed systems without mutual trust. Sequentially, this technology solves the prevailing high cost, low efficiency and uneasiness of data storage in current central institutions. This paper utilizes the feature of data is not tampered and completely transparent, combines with the time stamp and the transaction details in the process of storage and trading, so that it can be trusted by many parties. Its mixed encryption technology based on asymmetric encryption makes the user's privacy information secure with the public and private key as the only identifier of transaction subject. The second generation blockchain introduces intelligent contract, which makes the blockchain easier to use distributed application programming and speed up transaction speed. The Ethereum intelligent contract combined with capability-based access control method makes the data provider can completely control their own data sharing permissions quickly and efficiently and completely solve the credible issues of original system in the data.

The rest of this paper is organized as following: Section II analysis three main kinds of trust requirements in IoT data exchange. The solution architecture is presented in Section III. Section IV describes the design of key trust components in our solution. It discusses the practicality of our proposed solution and conclusion in Section V and VI.

II. TRUSTED REQUIREMENTS

IoT data as a special commodity, is collected by government, corporations, even individual, which are of great value to different application fields. Such owner needs a trusted platform to exchange their IoT data in order to improve data utilization and benefit from the trade. We divided data exchange needs for trust into three categories.

A. Trusted Trading

Trusted Trading requirement means the whole transaction process is recorded and can not be modified by either party if once confirmed. Besides, the detail transaction history should be traceable by public.

In brief, the requirement of such trusted trading requirement mainly includes accurate transaction description, traceable and immutable transaction process. Some existing solutions can record the trading history and provide convenient searching function, even use distributed cloud storage system to protect the system from single point failure problem [15]. However, such systems were developed and maintained by third-party organization which can not guarantee the transaction record from maliciously modified [16].

Unlike the common system, blockchain based system stored the exchange data in completely distributed peer to peer network [17]. It ensures the data on blockchain can not be arbitrarily changed and can audit according to time order.

In addition, the blockchain node can be downloaded by anyone, so the exchange data is transparent [18]. At the same time, the chain of blockchain information is completely transparent, so the data transaction information can be completely symmetric compared with traditional trading platform.

B. Trusted Data Access

Trusted Data Access requirement means data owner can hold their ownership, even can be realized personalized empower the access right after exchange IoT data [19].

Current platforms need the data providers upload their data set to website or special cloud. So that the user cannot hold the access permission of their data set after send to third-party organization and don't know who access their data.

In our solution, we separate the data exchange into two parts: origin data exchange and data access right exchange. Origin data exchange way is customized by data provider, and can be verified by the data access right store on blockchain which protected by consensus mechanism. Adopting various safety related technologies of block chain to jointly safeguard the security of data access and the rights of the data owner during transaction. Meanwhile, the full distribution characteristics of the blockchain can also make the access verification of permissions more convenient.

C. Trusted Privacy Preserve

Trusted Privacy Preserve requirement mean data owner can protect their personal information while data exchange. Because some IoT data regarding privacy matters are not the data requesters' concerns.

In third-party data exchange platform, users should provide some personal information even binding the credit card at registration time. Such privacy is vulnerable to hijacking by others and some IoT data also can reflect living habits of individuals. So privacy also preserves a pressing need in IoT data exchange [20].

Blockchain as an anonymous network, use 64-bit address to identify users which generated by RSA and protected by SHA-256. Participants send transactions only with public address without any personal information, so that the privacy preserve can be trusted [21].

III. ARCHITECTURE

A. Overall Architecture

The IoT data exchange framework based on blockchain is a decentralized application platform in which user can trade data in trusted environment. The framework can be divided into Data Layer, Network Layer, Protocol Layer and Interaction Layer. Fig. 1 shows the overall architecture.

B. Data Layer

Data layer consists of two parts: the IoT data and the exchange data. The former can be stored in various places as data source, such as storage clouds, database clouds, even wireless sensor network nodes which was managed by the owner. Exchange data stored in blockchain network which use to record the whole data exchange process. Exchange

parties are able to choose the data access methods and personal customization storage medium which make them feel appropriate, such as peer-to-peer transmission, access online database with limited permissions, and even hard disk. Exchange data includes the description of provide data or data requirement, conditions of data exchange and the data access authority.

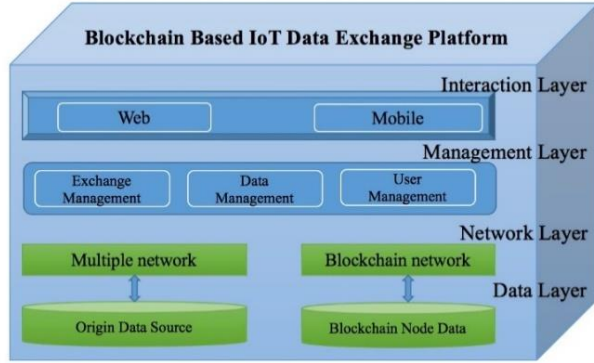


Figure 1. Architecture of blockchain based IoT data exchange platform

C. Network Layer

Network layer includes multiple network and blockchain network [22]. Multiple network is responsible for origin data access and transmission which form customized by the needs of the individual. Typical access methods include peer-to-peer network, personal website, and storage cloud. Blockchain network composed of one or more blockchain nodes that storage completely identical transactions happened in such network [23]. As the core of the architecture, the encryption and decentralized consensus mechanisms of blockchain guarantee IoT data exchange in a reliable, transparent and tamper-resistant environment.

D. Management Layer

Management layer is mainly responsible for common management function of IoT data exchange. User management controls the user's security and permissions for the platform. Data management is in charge of data collecting and quick search by data attribute. Exchange management as the core function of data exchange process, will manage the data access right, exchange relationship even records the transaction history.

E. Interaction Layer

Interaction layer provides the interface for data exchange parties to communicate with each other. According to the current mode of interaction, we separate them into two pieces: web based interactions and mobile based interactions. Web-based usually provides visual interfaces on website while mobile based provides more common to packaging into a app running on mobile phone, tablet even other embedded device.

IV. MAJOR COMPONENT DESIGN

To increasing the degree of automation and system configurable, we design a set of smart contracts for the major

management functions. Fig.2 shows the architecture of smart contract based management component.

A. Exchange Management Contracts

Exchange management contracts include three types protocols: access contracts, communication contracts and auto exchange contracts. Access contracts use capability based access control method to provide a trusted data permission management. Communication contracts record the whole communicated process in IoT data exchange for traceability. Auto exchange contracts will automatically send the data access right to demander while they satisfy the condition.

Access contracts implement capability-based data access control method, including two functions of the data access identifier generation and the data access rights exchange. The data identification contract assigns a Data Access Ticket to the data after the data owner has registered the data, Referred to as "DAT". Through this identifier, the user can obtain access way and access permissions of the data. The data access rights exchange contract is responsible for setting data provision conditions and implementing automated transaction. We assume that the data provider sets the conditions set as Condition1, Condition2, for short C1, C2. The contract will automatically provide DAT to the demander when the data demanders send data to the contract for a request for a transaction and the transaction satisfies C1, C2, and put the demanders in the list of authorized access to that data. When users get access, they can download the source data by means of URL or FTP or P2P seeds.

Communication contracts are determined by data, data demanders, and data providers, and record all transaction records between the three. When a data demander sends a request or a negotiation to the contract, two parameters of the data name and data provider are required. And vice versa, the contract will be notified to both parties.

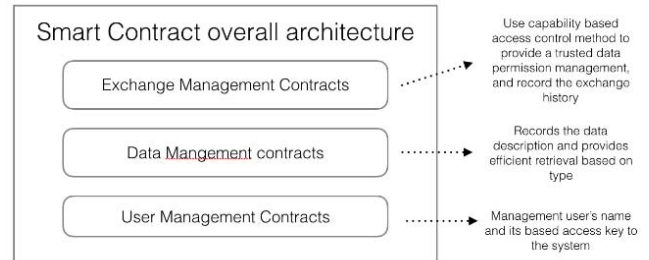


Figure 2. Architecture of smart contract based management component

B. Data Management Contracts

Data management contracts include data contracts and classified search contracts. When the data provider registers data, the data contract will generate a separate corresponding data object contract, which records the basic description of the data (Such as name, attribute, data provider), and call the data access contract method to generate data access identifier at the same time. In order to improve the search efficiency, we use the basic principle of hash table to perform secondary classification for data, and design an extensible and

customizable classifications. Data classification contracts include data type management and data type corresponding to the data set about management. Data type management is responsible for generating and modifying Type Contract, and the Data Type Contract is responsible for recording all data object Contract address as pointer of this type. The user invokes the contract and passes in the type parameter, which can quickly get the data set of the corresponding type.

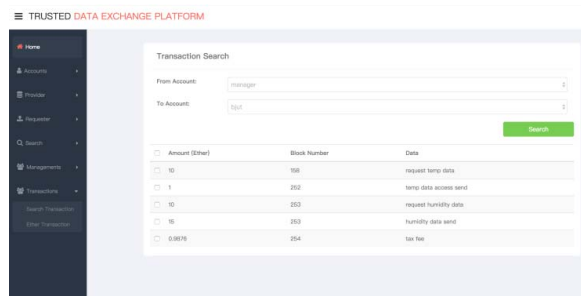
C. User Management Contracts

User management contracts as the basic contracts control the user's security and permissions of the platform by maintaining the user-nickname relationship and user-role relationship. User can use their nickname to communicate with others facilitate the identification rather than 64-bit address. The platform contains three main user roles: user provider, user demander and auditor. Role contracts maintain the user-role list used to defined responsibilities. The user's interaction in the system uses the user alias and password, so it can avoid privacy leak and better protect users' privacy.

V. IMPLEMENT

The deployment of this prototype platform includes blockchain network, smart contract and web-side. Blockchain network was composed of 10 Ethereum nodes. Two of them are deployed in Aliyun servers which responsible for mining. The system environment of the node is the Ubuntu system. The web is deployed on the Nginx server and can run on the universal browser on windows. Remaining nodes are deployed in PC for IoT data exchange. Smart contract is developed with Solidity language, and then compiled on one of two miner nodes. Web-side is based on Laravel framework which is one of the most popular PHP web framework. We store the relevant data collected by wireless sensor networks in the forest inspection project on the remote database such as Ali Cloud and so on, and use this system to achieve multi-party simulation data transaction experiment. Achieving data permission exchange and verify access on the chain successfully, in addition, we can visualize all point-to-point transaction records stored on-chain. Fig.3 shows that the exchange history protected by blockchain network.

TRUSTED DATA EXCHANGE PLATFORM



Amount (Ether)	Block Number	Data
10	100	request temp data
1	202	temp data access send
10	203	request humidity data
10	203	humidity data send
0.0075	204	fee fee

Figure 3. IoT data Exchange history

VI. CONCLUSION

This paper deeply analyses current trusted requirement in IoT data exchange and divides them into three categories: trusted trading, trusted data access and trusted privacy

preserve. After that, it proposes a blockchain based solution to meet such requirement and designs the major trusted components. Based on the design, we develop a prototype system for IoT data exchange with Ethereum blockchain and related web technology. The prototype shows that blockchain network can record the transaction in an auditable, transparent and immutable way.

During the future work, we will continue to refine the IOT data transaction process on the basis of this system to make it more standardized. At the same time, combining with the block chain itself, the research is applicable to the high-efficiency consensus mechanism, incentive mechanism of data transaction of IoT and establishes an impeccable evaluation mechanism for data credibility of Internet of things. what's more, we will make use of the node network topology based on the blockchain to carry out raw data transmission and so on..

ACKNOWLEDGMENT

This work was supported by National Development and Reform Commission (NDRC) (No.Q5025001201502).

REFERENCES

- [1] Chaudhary, Muhammad Hafeez, and B. Scheers. "Software-defined wireless communications and positioning device for IoT development." *International Conference on Military Communications and Information Systems* IEEE, 2016:1-8.
- [2] RJ Krawiec, Dan Housman, Mark White, Mariya Filipova, Florian Quarre, Dan Barr, Allen Nesbitt, Kate Fedosova, Jason Killmeyer, Adam Israel, Lindsay Tsai. Blockchain: Opportunities for Health Care
- [3] Theodoridis, Evangelos, G. Mylonas, and I. Chatzigianakis. "Developing an IoT Smart City framework." *Fourth International Conference on Information, Intelligence, Systems and Applications* IEEE, 2013:1-6.
- [4] Hashemi, Sayed Hadi, et al. "World of Empowered IoT Users." *IEEE First International Conference on Internet-Of-Things Design and Implementation* IEEE, 2016:13-24.
- [5] Leiding, Benjamin, P. Memamoshrefi, and D. Hogrefe. "Self-managed and blockchain-based vehicular ad-hoc networks." *ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct* ACM, 2016:137-140.
- [6] He, Hongmei, et al. "The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence." *Evolutionary Computation* IEEE, 2016:1015-1021.
- [7] Marjani, Mohsen, et al. "Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges." *IEEE Access* 5.99(2017):5247-5261.
- [8] Sliwa, Jan. "A Generalized Framework for Multi-party Data Exchange for IoT Systems." *International Conference on Advanced Information NETWORKING and Applications Workshops* IEEE, 2016:193-198.
- [9] Kotz, D., and T. Henderson. "CRAWDAD: A Community Resource for Archiving Wireless Data at Dartmouth." *IEEE Pervasive Computing* 4.4(2005):12-14.
- [10] Ding, Li, et al. "TWC data-gov corpus: incrementally generating linked government data from data.gov." *International Conference on World Wide Web* ACM, 2010:1383-1386.
- [11] Krishnamurthy, Rashmi, and Y. Awazu. "Liberating data for public value: The case of Data.gov." *International Journal of Information Management* 36.4(2016):668-672.

- [12] Zyskind, Guy, O. Nathan, and A. ' . Pentland. "Decentralizing Privacy: Using Blockchain to Protect Personal Data." *IEEE Security and Privacy Workshops* IEEE Computer Society, 2015:180-184.
- [13] Yin, Keting, C. Shou, and Z. Cai. "A data exchange optimized approach for cloud migration." *International Conference on Computer Science and Network Technology* IEEE, 2016:169-172.
- [14] Beck, Roman, et al. "BLOCKCHAIN – THE GATEWAY TO TRUST-FREE CRYPTOGRAPHIC TRANSACTIONS." *Twenty-Fourth European Conference on Information Systems* 2016.
- [15] Chatzigiannakis, Ioannis, A. Vitaletti, and A. Pyrgelis. "A privacy-preserving smart parking system using an IoT elliptic curve based security platform." *Computer Communications* s 89–90.C(2016):165-177.
- [16] Li, Tingli, et al. A Storage Solution for Massive IoT Data Based on NoSQL. 2012.
- [17] Wilson, Duane, and G. Ateniese. "From Pretty Good to Great: Enhancing PGP Using Bitcoin and the Blockchain." *International Conference on Network and System Security* Springer International Publishing, 2015:368-375.
- [18] Singh, Sachchidanand, and N. Singh. "Blockchain: Future of financial and cyber security." *International Conference on Contemporary Computing and Informatics* IEEE, 2017:463-467.
- [19] Maesa, Damiano Di Francesco, P. Mori, and L. Ricci. "Blockchain Based Access Control." (2017).
- [20] Appavoo, Paramasiven, et al. "Efficient and privacy-preserving access to sensor data for Internet of Things (IoT) based services." *International Conference on Communication Systems and Networks* IEEE, 2016:1-8.
- [21] Mukhopadhyay, Ujan, et al. "A brief survey of Cryptocurrency systems." *Privacy, Security and Trust* IEEE, 2017:745-752.
- [22] YUAN Yong, WANG Feiyue. " Blockchain : The State of the Art and Future Trends." *Acta Automatica Sinica* 42.4(2016):481-494.
- [23] ZHAO He, LI Xiaofeng,ZHAN likui, et al. "Data integrity protection method for microorganism sampling robots based on blockchain technology." *Journal of Huazhong University of Science and Technology (Nature Science Edition)* 43.s1(2015):216-219.