Received 4 August 2017
Revised 6 September 2017
Accepted 7 September 2017

Using blockchain to build trusted LoRaWAN sharing server

Jun Lin
The Joint NTU-UBC Research Centre of Excellence in Active Living for the Elderly (LILY), Nanyang Technological University, Singapore, Singapore

Zhiqi Shen
School of Computer Science and Engineering, Nanyang Technological University, Singapore, Singapore

Chunyan Miao
The Joint NTU-UBC Research Centre of Excellence in Active Living for the Elderly (LILY), Nanyang Technological University, Singapore, Singapore and School of Computer Science and Engineering, Nanyang Technological University, Singapore, Singapore, and

Siyuan Liu
The Joint NTU-UBC Research Centre of Excellence in Active Living for the Elderly (LILY), Nanyang Technological University, Singapore, Singapore

Abstract

Purpose – With the rapid growth of the Internet of Things (IoT) market and requirement, low power wide area (LPWA) technologies have become popular. In various LPWA technologies, Narrow Band IoT (NB-IoT) and long range (LoRa) are two main leading competitive technologies. Compared with NB-IoT networks, which are mainly built and managed by mobile network operators, LoRa wide area networks (LoRaWAN) are mainly operated by private companies or organizations, which suggests two issues: trust of the private network operators and lack of network coverage. This study aims to propose a conceptual architecture design of a blockchain built-in solution for LoRaWAN network servers to solve these two issues for LoRaWAN IoT solution.

Design/methodology/approach – The study proposed modeling, model analysis and architecture design.

Findings – The proposed solution uses the blockchain technology to build an open, trusted, decentralized and tamper-proof system, which provides the indisputable mechanism to verify that the data of a transaction has existed at a specific time in the network.

Originality/value – To the best of our knowledge, this is the first work that integrates blockchain technology and LoRaWAN IoT technology.

Keywords Internet of things, Blockchain, LoRa, LoRaWAN

Paper type Conceptual paper

This research is supported by the National Research Foundation, Prime Minister's Office, Singapore under its IDM Futures Funding Initiative.

International Journal of Crowd Science
Vol. 1 No. 3, 2017
pp. 270-280
Emerald Publishing Limited
2398-7294
DOI 10.1108/IJCS-08-2017-0010

1. Introduction

As a major research area of crowd science and engineering, the Internet of Things (IoT) is a fast-growing industry targeted to transform cities, farms, factories, homes and practically everything else to be more intelligent and efficient. According to Gartner, the total spending on IoT devices and services will reach almost $2tn in 2017, and there will be more than 20 billion connected things all over the world by 2020 (Gartner, 2017).

Different IoT technologies can be applied to different application areas and realistic scenarios. As different application areas have specific requirements and considerations, different technologies are needed. For example, widely installed short-range radio connectivity (e.g. WIFI, Bluetooth and ZigBee) is not suitable for the scenarios, which require long-range performance with low bandwidth. Although machine to machine (M2M) or the 5th generation (5G) solution based on the cellular technology can provide large coverage, they consume a lot of power. Therefore, Low-Power Wide Area Network (LPWAN) technologies are proposed, targeting these emerging applications and markets.

"LPWAN" was not proposed until the early of 2013 (LoRa Alliance, 2017a). As the IoT market rapidly grows, LPWAN rapidly became one of the faster growing areas in IoT. Many of the LPWAN technologies depicted in Table I have arisen in both licensed and unlicensed markets, such as SigFox, LoRa, LTE-M and Narrow Band IoT (NB-IoT). Among them, LoRa and NB-IoT are the two leading emergent technologies, which involve many technical differences.

LoRa is an emerging technology in the current market, which is an LPWAN solution intended for the systems, which require the ability to send and receive low amounts of data over a range of 2-20 km with low power costs. The name LoRa comes from its advantage of long-range capability, which benefits from the long great link budget provided by the spread spectrum modulation scheme that is a derivative of chirp spread spectrum modulation (CSS) and which trades data rate for sensitivity within a fixed channel bandwidth. LoRa uses the unlicensed ISM bands below 1 GHz and is able to transmit over several kilometers depending on the environment. It is a spread spectrum solution which uses wide bandwidth to help protect against deliberate interferences or environmental noises. According to LoRa's documentation (LoRa Alliance, 2015b), LoRaWAN, the network used by the LoRa technology, is capable of providing data rates from 0.3 kbps to 50 kbps, which vary based on the required range and interference. Some experimental research

Technology	LoRaWAN	SigFox	NB-IoT	LTE Cat M1
Frequency band	433/868/780/915 MHz (Unlicensed ISM)	868 MHz/902 MHz (Unlicensed ISM)	Cellular (Licensed Band)	Cellular (Licensed Band)
Bandwidth	500 Hz-125 kHz	100 kHz	180 kHz	1.08 MHz
Data rate	0.3-50 kbps	10-100 kbps	<250 kbps	1 Mbps
Range (km)	2-5 (urban) 15 (suburban) 45 (rural)	3-10 (urban) 30-50 (rural)	2.5-5	2.5-5
Coverage	157 dB	149 dB	164 dB	160 dB
Capacity	40k/cell	50k/cell	200 k/cell	1M/cell
Battery life	>10 years	>10 years	>10 years	>10 years
Mobility support	Yes	No	Idle mode	Connected + Idle mode
Location support	Yes	No	Needs GPS	Needs GPS
Device cost	1-5$	5$	<5$ per module	<5$per module
Governing body	LoRa Alliance	Sigfox	3GPP	3GPP

Table I. Comparison of LPWAN technologies

shows that unlicensed LoRa has advantages in terms of battery lifetime, capacity and cost. Meanwhile, licensed NB-IoT offers benefits in terms of quality of service, latency, reliability and range (Sinha *et al.*, 2017). NB-IoT is a narrowband radio technology designed for the IoT, and is one of a range of Mobile IoT (MIoT) technologies standardized by the 3rd Generation Partnership Project (3GPP), which uses licensed cellular telecommunications spectrum bands (3GPP TR 36.802, 2016). As spectrum resources are very limited and expensive, network operators need to bid the spectrum licenses from each country's government, and the high cost finally will post burdens to customers and end users.

A typical LoRaWAN includes end nodes, gateways, network servers (including network controller, join server), application servers and customer servers (optionally), as shown in Figure 1.

End nodes are used to collect and transmit sensor data and sometimes to remotely control external systems. They are typically low powered and communicate wirelessly with one or many gateways. A node is normally formed by a LoRa transceiver, which is managed by a microcontroller unit (MCU). The MCU can send LoRa MAC (media access control) commands to the transceiver to configure LoRa network settings or to send and receive application data which the transceiver is responsible for delivering to network servers via gateways. Although end nodes are able to listen at all times, it is standard for the end node to work in a "call then listen" configuration, whereby the end node will send data to the network server via gateways and then have short windows afterwards where it listens for data coming back from the network server via one gateway, which is called Class A end node in LoRaWAN specification (LoRa Alliance, 2015a).

Gateways are fewer in number, and transfer data from the end nodes back to the network server using standard TCP/IP connections. Therefore, LoRaWAN network architecture is

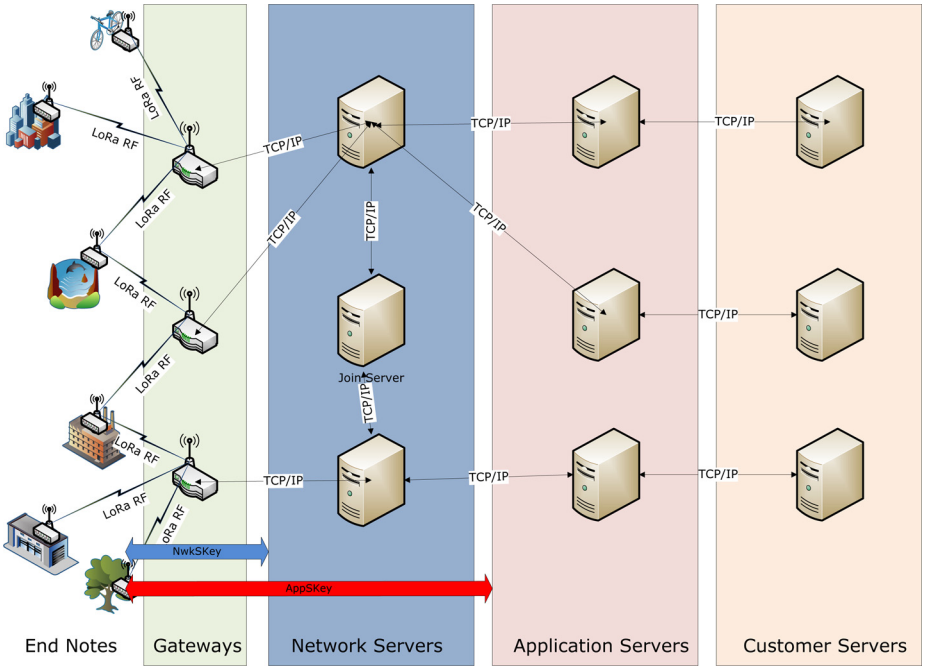

Figure 1.
LoRaWAN architecture

typically laid out in a star-of-stars topology in which gateways are a transparent bridge relaying messages between end nodes and a single network server in the backend. Gateways perform no security functionality themselves, but merely act as a conduit to relay data between end nodes and the network server.

The network server is not so well defined in LoRaWAN specifications but represents the edge of the systems that would store and parse the data sent from end nodes. To maximize both battery life of the end nodes and overall network capacity, the LoRaWAN network server is able to manage the data rate and radio frequency output for each end node individually by means of an adaptive data rate scheme (LoRa Alliance, 2015a). In some LoRaWAN implementations, the network controller is used for adapting the algorithms to end node-specific radio parameters and the application type (LoRa Alliance, 2015a), and the join server is used for security key provisioning during the network join procedure (LoRa Alliance, 2017b). In several systems deployed in the industry already, e.g. https://loriot.io/ and www.thethingsnetwork.org/, the network servers are designed as internet-facing Web services to which the gateways can connect via cellular networks.

Compared with other IoT solutions, the LoRaWAN protocol is equipped with very good built-in security mechanisms based on proven advanced encryption standard (AES) cryptography, including the considerations of mutual authentication, integrity protection and confidentiality. It provides both signing and encryption for parts of network packages. These are performed using symmetric keys known both to the end node and to the network server, as well as the application server located behind the network server. Those keys are distributed in one of two ways depending on how an end node joins the network. The first way by which an end node is allowed to join a LoRaWAN is through ABP. The end node is shipped with the DevAddr and both communication session keys: the network session key (NwkSKey) and the app session key (AppSKey) in advance, which should be unique to the end node. The NwkSKey is used for network layer security, and the AppSKey is used for application layer end-to-end security. As the end node already has the information and keys they need, they can begin communicating with the network server without the need for the network to join the procedure. Another way is OTAA. In this way, each end node is deployed with a unique 128-bit AppKey, which is used when the end node sends a join request message. The join request message is not encrypted, but is signed using this AppKey, which includes the end node's unique AppEUI and DevEUI values plus a DevNonce which should be a randomly generated two-byte value. The AppEUI should be unique to the owner of the device. The DevEUI should be a globally unique identifier for the device. These three values are signed with a four-byte message integrity code. The server should check the values and then re-calculate the message integrity code with the AppKey. If valid, the server will respond with a join accept message within the receive windows of the end node. The network server generates its own nonce value (AppNonce), and calculates the end node's two new 128-bit keys: the AppSKey and the NwkSKey. Once an end node has joined a LoRaWAN network, through either OTAA or ABP, all future messages will be encrypted and signed using a combination of NwkSKey and AppSKey. As the NwkSKey key is only known by the network server and the specific end node, and the AppSKey key is only known by the application server and the end node, there should be no way for another end node or a person in the middle attack to recover the cleartext data. Even the network server cannot decrypt the application data when it has no the AppSKey in some LoRaWAN deployments (LoRa Alliance, 2017b).

However, public LoRaWAN networks operated by one single organization are facing not only a security issue but also a trust issue. People trust mobile operators, as they have spent a lot on the spectrum resources and telecommunication infrastructure that makes customers believe that operators will not be evil under the strict supervision by the government. But,

how to let people trust that a public LoRaWAN can help them transport data from gateways to application servers without stealing, tampering or cheating? That is our vision in this paper. The blockchain technology proposed by Nakamoto (2008) that underpins Bitcoin, the first cypto-currency system, has the potential to overcome aforementioned challenges as a result of its distributed, secure and private nature. By introducing the blockchain technology into LoRaWAN, we propose an open, trusted and decentralized LoRaWAN server architecture design. Besides this, the architecture should allow any existing servers to join into this peer-to-peer network when it follows the design, which will quickly expand the data processing capacity of the whole network and make it a sharing LoRaWAN system.

The rest of this paper is structured as follows. In Section 1, we review the state of art for the integration of blockchain and IoT technologies and highlight existing IoT-on-the-blockchain applications. In Section 3, we propose our blockchain-based LoRaWAN server architecture design, including the network server inner architecture, message process flow and blockchain data structure. In Section 4, we present our conclusions.

2. Related work

2.1 Blockchain technology

Blockchain is a peer-to-peer (P2P) distributed and decentralized ledger technology which can be used to record transactions, agreements, contracts and events (Christidis and Devetsikiotis, 2016). A blockchain is essentially a distributed database of records or public ledger of all transactions or digital events that have been executed and shared among participating parties. Unlike other ledger approaches, blockchain guarantees tamper-proof storage of approved transactions without an intermediary. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. And, once entered, information can never be erased. A blockchain contains a certain and verifiable record of every single transaction ever made.

Blockchain is originally developed to support crypto-currency, Bitcoin (Nakamoto, 2008), a decentralized peer-to-peer digital currency, which is the most popular example that uses blockchain technology. With the success of Bitcoin, the underlying blockchain technology has worked flawlessly and found a wide range of applications in both the financial and non-financial world. The main hypothesis of the blockchain technology is that it establishes a system of creating a distributed consensus in the P2P network. This allows participating entities to know for certain that a digital event is happening by creating an irrefutable record in a public ledger.

A blockchain is a mechanism using a P2P that has functions of:

- enabling the transactions whose authenticity is guaranteed (prevent double spend);
- ensuring traceability of data and enabling transparent transactions (tamper-proof); and
- stably maintaining the ecosystem against any attacks by malicious users without a central authority.

Attacking a blockchain system has to compromise 51 per cent of the systems to surpass the hashing power of the target network. Thus, it is computationally impractical to launch an attack against the blockchain network. Expansively, it can be defined as a protocol to mutually approve value information on the IoT.

The main technologies underlying blockchain include:

- hash;
- public key cryptography and digital signature;

- P2P; and
- proof of work (Nakamoto, 2008).

The blockchain technology provides an indisputable mechanism to verify that the data of a transaction have existed at a specific time in the block. Moreover, because each block in the chain contains information about the previous block, the history, position and ownership of each block are automatically authenticated and cannot be altered. Blockchain resilience stems from its structure, as it is designed as a distributed network of nodes in which each one of these nodes store a copy of the entire ledger. Hence, when a transaction is verified and approved by the participating nodes, it is highly impossible to change or alter the transaction's data (Morabito, 2017).

The integration of network resources and service abilities across organizations is typically beneficial for all involved parties, especially for the LoRaWAN network providers. However, the lack of trust is often a roadblock. Blockchain is an emerging technology for decentralized and transactional data sharing across a network of untrusted participants. It can be used to find agreement about the shared state of collaborating parties without trusting a central authority or any particular participant.

2.2 Integration of blockchain and IoT

There are some researchers who have studied the integration of blockchain and IoT technology.

Christidis and Devetsikiotis discussed how a blockchain–IoT combination can:

- facilitate the sharing of services and resources leading to the creation of a marketplace of services between devices; and
- allow a user to automate in a cryptographically verifiable manner several existing, time-consuming workflows.

They pointed out certain issues that should be considered before the deployment of a blockchain network in an IoT setting: from transactional privacy to the expected value of the digitized assets traded on the network. The conclusion of their paper is that the blockchain–IoT combination is powerful and can cause significant transformations across several industries, paving the way for new business models and novel, distributed applications (Christidis and Devetsikiotis, 2016).

Biswas and Muthukkumarasamy proposed a blockchain-based security framework to enable secure data communication in a smart city. They discussed the main advantages of using blockchain in smart cities, which are:

- the resilience against many threats;
- improved reliability;
- better fault-tolerance capability;
- faster and efficient operation; and
- scalability.

Their conclusion is the integration of the blockchain technology with devices in a smart city will create a common platform where all devices would be able to communicate securely in a distributed environment (Biswas and Muthukkumarasamy, 2016).

Dorri *et al.* (2017) discussed that IoT security and privacy remain a major challenge, mainly due to the massive scale and distributed nature of IoT networks. Although the blockchain technology provides decentralized security and privacy, it requires significant energy and causes delay and computational overhead that is not suitable for most resource-constrained IoT

devices. Therefore, a lightweight instantiation of a blockchain is proposed, particularly geared for use in IoT by eliminating the proof of work (POW) and the concept of coins. This approach was exemplified in a smart home setting and consists of three main tiers, namely, cloud storage, overlay and smart home. In this solution, each smart home is equipped with an always online, high resource device, known as "miner" that is responsible for handling all communication within and external to the home. The miner also preserves a private and secure blockchain used for controlling and auditing communications. The used simulation results highlight that the overheads (in terms of traffic, processing time and energy consumption) introduced by our approach are insignificant relative to its security and privacy gains (Dorri *et al.*, 2017).

Huh *et al.* (2017) proposed a way to manage IoT devices using Ethereum, an open-source, public, blockchain-based distributed computing platform featuring smart contract (scripting) functionality. They use the smart contract script to save data coming from meter and smart phones. Their experiment shows that using an Ethereum account, a meter constantly sends electricity use and a smart phone sends policies for air conditioner and light bulb. And air conditioner and light bulb constantly check the values on Ethereum to update their devices. When necessary, they switch their modes from normal to energy-saving. This is a good application example for the integration of blockchain and IoT.

Samaniego and Deters proposed the idea and evaluation of using virtual resources in combination with a permission-based blockchain for provisioning IoT services on edge hosts. They thought that moving IoT components from the cloud to edge hosts helps in reducing overall network traffic, and thus minimizes latency. However, provisioning IoT services on the IoT edge devices presents new challenges regarding system design and maintenance. One possible approach is the use of software-defined IoT components in the form of virtual IoT resources. This, in turn, allows exposing the thing/device layer and the core IoT service layer as collections of micro services that can be distributed to a broad range of hosts (Samaniego and Deters, 2016a). In another paper, they discussed the idea of using the blockchain as a service for IoT and evaluated the performance of a cloud and edge-hosted blockchain implementation (Samaniego and Deters, 2016b).

Although the aforementioned researchers have explored the integration and implementation of the blockchain and IoT technologies, they seldom target the LoRaWAN. LoRaWAN and especially the LPWA are new emerging technologies in recent years, and also as we discussed before, LoRaWAN already has built-in strong security mechanisms for building a private network. However, the current main challenge for LoRa technology is not the security concerns, but the network coverage concerns. Big mobile operators tend to choose cellular technology-based NB-IoT, as they already have the licensed spectrum resources and they can recover the expensive cost of building the network from end consumers finally.

3. Proposed method

The market left to LoRaWAN is small-medium enterprises or organizations' private network. But for some typical field IoT applications, such as animal tracking, fleet tracking, asset tracking and smart parking, the network coverage is very important for the quality of service. It requires a big union network for LoRaWAN to provide consistent services, such as the roaming service for end user and accounting and settlement service for each party.

Based on concepts of crowdsourcing and sharing economy, we propose the following blockchain architecture for LoRaWAN servers, which can utilize both advantages of blockchain technology and LoRaWAN technology to provide an open, trusted, decentralized and tamper-proof network system.

In Figure 2, the blockchain system is built in the network server layer of LoRaWAN. The reasons are listed below:

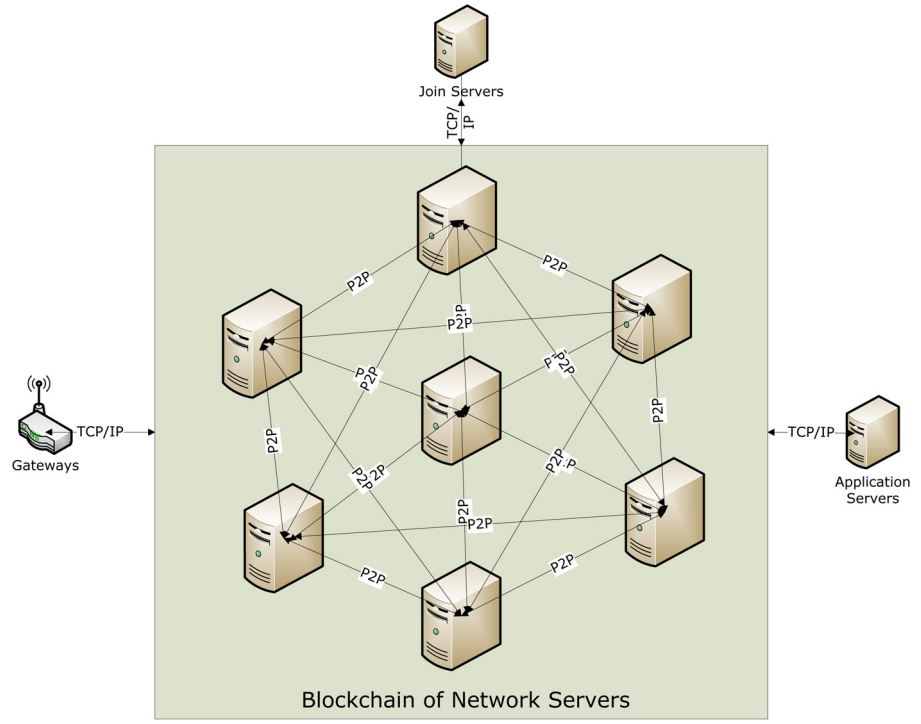

Figure 2.
Blockchain architecture for LoRaWAN server

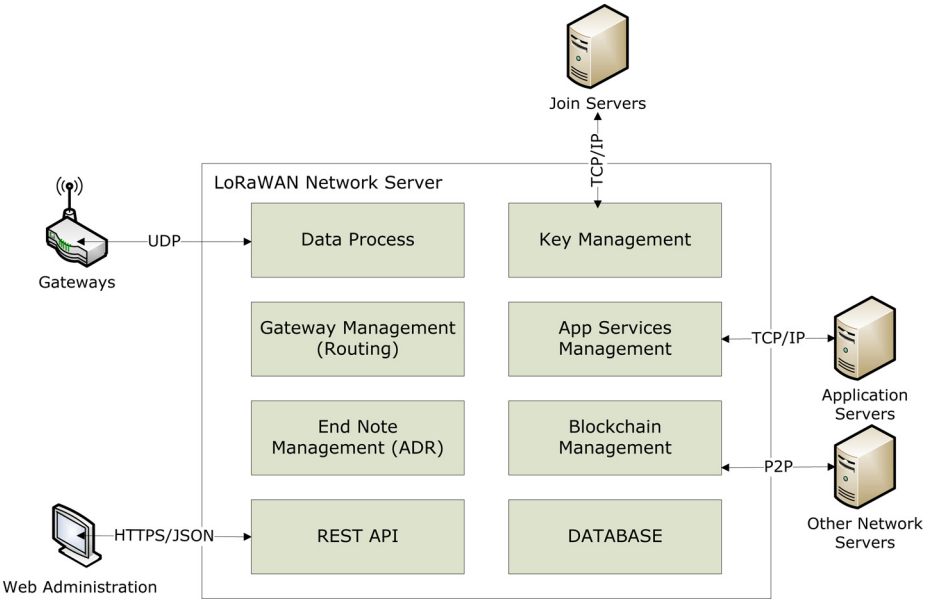

Figure 3.
LoRaWAN network server inner architecture

- *for Gateways*: LoRaWAN's gateways normally are resource-constrained and outdoor-deployed IoT devices, which are not suitable to bear too many blockchain computing functions of security, verification and storage;
- *for Join Servers*: LoRaWAN's join servers normally are provided by end node's manufactories to produce session keys, which are also not suitable to undertake the blockchain functions; and
- *for Application Servers*: LoRaWAN's application servers normally are provided by customers to process core business data, which are also not suitable to undertake any blockchain function.

In each network server (NS), except the normal functions of LoRaWAN NS, we added the blockchain management component, which can be communicated with other NS to fulfill blockchain's functions. Figure 3 is the inner architecture of the LoRaWAN network server.

The blockchain manager component implements the blockchain functions of packaging transaction, hashing transaction, verifying transaction, making block, storing blockchain,

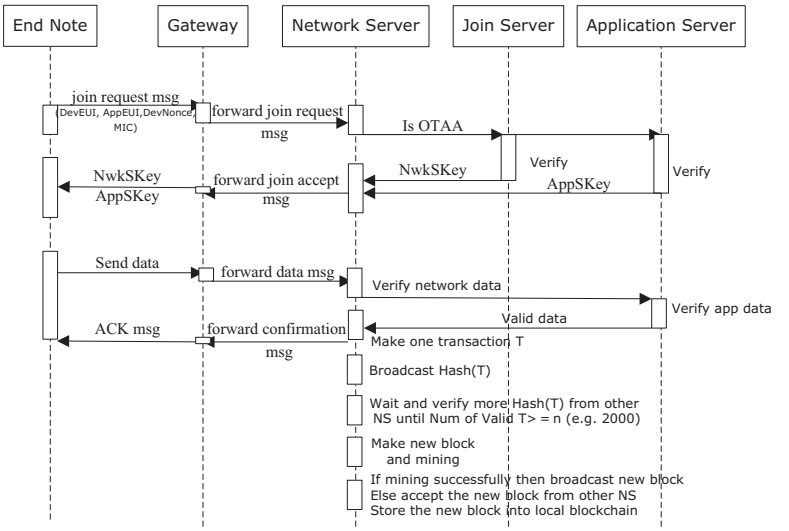

Figure 4.
Message process flow

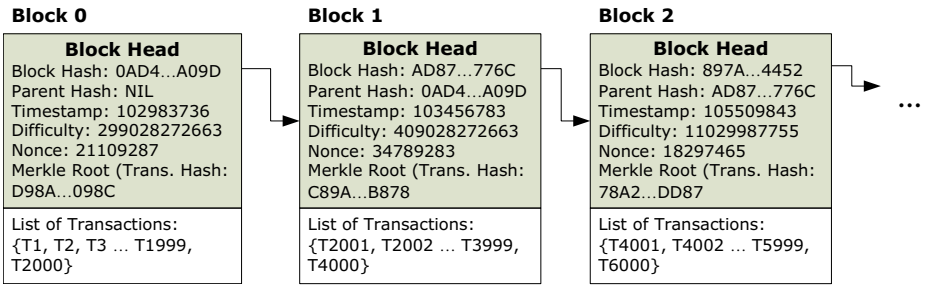

Figure 5.
Example of blockchain data structure

etc. A message process flow is shown in Figure 4. If the message is sent from the ABP mode, then the steps of joining network can be ignored.

Figure 5 below shows how the blockchain data structure is stored in each NS node. The hash values on the blockhead will be different in implementation. In Figure 5, the number of transactions in one block is 2000, which can also be changed when necessary. For some lightweight client of the network server, it allows only storing the blockheads without the full blockchain, but still can use the simplified payment validation (SPV) method to verify that confirmed transactions are part of a block, without providing the full ledger to download (Gervais *et al.*, 2014).

4. Conclusion

It should be clear to all developers of LoRaWAN solutions that LoRa and the LoRaWAN protocols allow secure solutions to be developed that protect companies and the end users from cyber-attacks. However, using LoRa and LoRaWAN does not guarantee the trust of network operators. In this paper, we proposed a blockchain built-in solution for LoRaWAN network servers. Our solution uses the blockchain technology to build an open, trusted, decentralized and tamper-proof system, which provides the indisputable mechanism to verify that the data of a transaction has existed at a specific time in the network. To the best of our knowledge, this is the first work that integrates blockchain technology and LoRaWAN IoT technology. This integration utilizes advantages of both technologies. In the future, we also can use smart contract script technology to define automated trading model in the IoT network. But even without it, some basic functions like billing and roaming could be used in an automatic way in the LoRaWAN. In further studies, we would like to build fully scaled LoRaWAN blockchain networks to link customers' gateways and application servers.

References

3GPP TR 36.802 (2016), "Narrowband internet of things (NB-IoT)", Technical Report TR 36.802 V1.0.0, Technical Specification Group Radio Access Networks, June, 2016.

Biswas, K. and Muthukkumarasamy, V. (2016), "Securing smart cities using blockchain technology", *Proceedings of the 2016 IEEE International Conference on High Performance Computing and Communications, The IEEE 14th International Conference on Smart City and the IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*.

Christidis, K. and Devetsikiotis, M. (2016), "Blockchains and smart contracts for the internet of things", *IEEE Access, Special Section on the Plethora of Research in IoT*, Vol. 4, pp. 2292-2303.

Dorri, A., Kanhere, S. and Jurdak, R. (2017), "Blockchain for IoT security and privacy: The case study of a smart home", *Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*.

Gartner (2017), "Gartner says 8.4 billion connected 'things' will be in use in 2017", Up 31 Per cent From 2016, available at: www.gartner.com/newsroom/id/3598917

Gervais, A., Capkun, S., Karame, G.O. and Gruber, D. (2014), "On the privacy provisions of Bloom filters in lightweight bitcoin clients", *Proceeding of the 30th Annual Computer Security Applications Conference (ACSAC'14)*, pp. 326-335.

Huh, S., Cho, S. and Kim, S. (2017), "Managing IoT devices using blockchain platform", *Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT)*.

LoRa Alliance (2015a), "LoRaWAN specification V1.0", available at: www.lora-alliance.org/portals/0/specs/LoRaWAN%20Specification%201R0.pdf

LoRa Alliance (2015b), "LPWA technologies unlock new IoT market potential", Machina Research, available at: www.lora-alliance.org/portals/0/documents/whitepapers/LoRa-Alliance-Whitepaper-LPWA-Technologies.pdf

LoRa Alliance (2017a), "LoRa alliance technology", available at: www.lora-alliance.org/What-Is-LoRa/Technology

LoRa Alliance (2017b), "LoRaWAN security full end-to-end encryption for IoT application providers", available at: www.lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN_Security-Whitepaper_V6_Digital.pdf

Morabito, V. (2017), "Blockchain value system", *Business Innovation through Blockchain*, pp. 21-39.

Nakamoto, S. (2008), "Bitcoin: a peer-to-peer electronic cash system".

Samaniego, M., *and.*, and Deters, R. (2016a), "Blockchain as a service for IoT", *Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*.

Samaniego, M. and Deters, R. (2016b), "Using blockchain to push software-defined IoT components onto edge hosts", *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies*.

Sinha, R., Wei, Y. and Hwang, S. (2017), "A survey on LPWA technology: LoRa and NB-IoT", *ICT Express*, Vol. 3 No. 1, pp. 14-21.

About the authors

Jun Lin is a Research Fellow of the Joint NTU-UBC Research Centre of Excellence in Active Living for the Elderly (LILY), Nanyang Technological University, Singapore, and an Associate Professor of College of Software, Beihang University, China. He holds a PhD degree from the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His current research interests include LoRaWAN, Blockchain, Internet of Things, Crowd Science, Software Engineering and AI technologies. Jun Lin is the corresponding author and can be contacted at: junlin@ntu.edu.sg

Zhiqi Shen is a Senior Scientist of School of Computer Science and Engineering, Nanyang Technological University, Singapore. He obtained his BSc degree in Computer Science and Technology from Peking University, MEng in Computer Engineering from Beijing University of Technology, and PhD from Nanyang Technological University. His research interests include artificial intelligence, software agents, multi-agent systems, goal oriented modeling, agent oriented software engineering, semantic web/grid, e-Learning, Bioinformatics and Bio-manufacturing, agent augmented interactive media, game design and interactive storytelling.

Chunyan Miao is a Professor in the School of Computer Science and Engineering (SCSE), Nanyang Technological University. Professor Miao is currently serving as the Founding Director of the Joint NTU-UBC Research Centre of Excellence in Active Living for the Elderly (LILY). LILY is one of the first research centers focused on artificial intelligence technologies for helping the elderly lead an active, healthy and dignified lifestyle.

Siyuan Liu got her BSc and MSc degrees in Computer Science from Peking University, China in 2002 and 2005, respectively. She obtained her PhD degree from Nanyang Technological University (NTU), Singapore, in 2013. She is currently a Research Fellow in Joint NTU-UBC Research Centre of Excellence in Active Living for the Elderly (LILY). Her research interest includes trust and reputation in multi-agent systems and incentive mechanism design in crowdsourcing.