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 pose higher trust risks to application customers and network operations.

Design/Methodology/Approach – The authors proposed a blockchain built-in solution for LoRaWAN network servers.

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 blockchain; Internet of Things; LoRa; LoRaWAN.

Paper type Conceptual paper
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 $2 trillion 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 at 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.

Table I. Comparison of LPWAN Technologies.

<table>
<thead>
<tr>
<th>Technology</th>
<th>LoRaWAN</th>
<th>SigFox</th>
<th>NB-IoT</th>
<th>LTE Cat M1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency Band</td>
<td>433/868/780/915 MHz (Unlicensed ISM)</td>
<td>868 MHz/902 MHz (Unlicensed ISM)</td>
<td>Cellular (Licensed ISM)</td>
<td>Cellular (Licensed ISM)</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>500 Hz - 125k Hz</td>
<td>100k Hz</td>
<td>180k Hz</td>
<td>1.08M Hz</td>
</tr>
<tr>
<td>Data Rate</td>
<td>0.3 - 50k bps</td>
<td>10 - 100k bps</td>
<td>&lt;250k bps</td>
<td>1 M bps</td>
</tr>
<tr>
<td>Range (km)</td>
<td>2 - 5 (urban)</td>
<td>3 - 10 (urban)</td>
<td>2.5 - 5</td>
<td>2.5 - 5</td>
</tr>
<tr>
<td>Coverage</td>
<td>157dB</td>
<td>149dB</td>
<td>164dB</td>
<td>160dB</td>
</tr>
<tr>
<td>Capacity</td>
<td>40k/cell</td>
<td>50k/cell</td>
<td>200k/cell</td>
<td>1M/cell</td>
</tr>
<tr>
<td>Battery Life</td>
<td>&gt;10 years</td>
<td>&gt;10 years</td>
<td>&gt;10 years</td>
<td>&gt;10 years</td>
</tr>
<tr>
<td>Mobility Support</td>
<td>Yes</td>
<td>No</td>
<td>Idle Mode</td>
<td>Connected+Idle Mode</td>
</tr>
<tr>
<td>Location Support</td>
<td>Yes</td>
<td>No</td>
<td>Needs GPS</td>
<td>Needs GPS</td>
</tr>
<tr>
<td>Device cost</td>
<td>1-5$</td>
<td>5$</td>
<td>&lt;5$ per module</td>
<td>&lt;5$ per module</td>
</tr>
<tr>
<td>Governing Body</td>
<td>LoRa Alliance</td>
<td>Sigfox</td>
<td>3GPP</td>
<td>3GPP</td>
</tr>
</tbody>
</table>
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 kilometers 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 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), the LoRaWAN, the network used by LoRa technology, is capable of providing data rates from 0.3kbps to 50kbps, which vary based on the required range and interference. Some experimental research shows that unlicensed LoRa has advantages in terms of battery lifetime, capacity, and cost. Meanwhile, licensed NB-IoT offers benefits in terms of QoS, latency, reliability, and range (Sinha et al., 2017). NB-IoT is a narrowband radio technology designed for the Internet of Things (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 notes, gateways, network servers (including network controller, join server, etc.), application servers and customer servers (optionally) as shown in Figure 1.

![LoRaWAN Architecture](image_url)
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 of 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 typically laid out in a star-of-stars topology in which gateways is a transparent bridge relaying messages between end notes 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 notes and overall network capacity, the LoRaWAN network server is able to manage the data rate and RF output for each end note individually by means of an adaptive data rate (ADR) scheme (LoRa Alliance, 2015a). In some LoRaWAN implementations, the network controller is used for adapting the algorithms to end note specific radio parameters and the application type [6], as well as 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 https://www.thethingsnetwork.org/, the network servers are designed as Internet-facing web services which the gateways can connect via cellular networks.

Compared with other IoT solutions, the LoRaWAN protocol has equipped with very good built-in security mechanisms based on proven AES cryptography, including the considerations of mutual authentication, integrity protection and confidentiality etc. 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 application 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 4 byte message integrity code (MIC). The server should check the values and then re-calculate the MIC 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 calculate the end node’s two new 128-bit keys: the AppSKey and the NwkSKey. Once an end node has joined a LoRaWAN network, either through 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 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 clear-text data. Even the network server cannot decrypt the application data when it has no the AppSKey in some LoRaWAN deployments (LoRa Alliance, 2017b).

However, the public LoRaWAN networks operated by one single organization are facing not only the security issue but also the trust issue. People trust mobile operators as they have cost 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 in 2008 that underpins Bitcoin the first crypto-currency system (Nakamoto, 2008), 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, 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 makes it to be a sharing LoRaWAN system.

The rest of this paper is structured as follows. In Section II, we review the state of art for the integration of blockchain and IoT technologies and highlight existing IoT-on-the-blockchain applications. In Section III, we propose our blockchain based LoRaWAN server architecture design, including the network server inner architecture, message process flow and blockchain data structure. In Section IV, 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 happening by creating an irrefutable record in a public ledger.

A blockchain is a mechanism using a P2P that has functions of 1) enabling the transactions whose authenticity is guaranteed (prevent double spend); 2) ensuring traceability of data and enabling transparent transactions (tamper-proof); 3) stably maintaining the ecosystem against any attacks by malicious users without a central authority. Attacking a blockchain system has to compromise 51% 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: 1) hash; 2) public-key cryptography and digital signature; 3) P2P; 4) Proof of Work (Nakamoto, 2008). Blockchain technology provides an indisputable mechanism to verify that the data of a transaction has existed at a specific time in the block. Moreover, because each block in the chain contains information about the previous block, then, the history, position and ownership of each block are automatically authenticated, and cannot be altered. Blockchain resilience stems from its structure since 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: 1) facilitate the sharing of services and resources leading to the creation of a marketplace of services between devices and 2) 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 Muthukumarasamy 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 are 1) the resilience against many threats; 2) improved reliability; 3) better fault tolerance capability; 4) faster and efficient operation, and 5) 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 Muthukumarasamy, 2016)

Dorri et al. 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 to 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. 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 using an Ethereum account, a meter constantly sends electricity use and smart phone sends policies for air conditioner and light bulb. And air conditioner and light bulb constantly checks 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. (Huh et al., 2017)

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 onto edge hosts helps in reducing overall network traffic and thus minimizes latency. But 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 above researchers have explored the integration even implementation of the blockchain and IoT technologies, they seldom target the LoRaWAN. As the LoRaWAN and especially LPWA are new emerging technologies in recent years, and also as we discussed before, the LoRaWAN has already 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, smart parking etc., the network coverage is very important for the QoS. It requires a big union network for LoRaWAN to provide consistent services, such as the roaming service for end user, accounting and settlement service for each party etc.

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.

![Blockchain Architecture for LoRaWAN Server](image_url)
In Figure 2, the blockchain system is built in the network server layer of LoRaWAN. The reasons are listed below.

1. 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 etc.

2. 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.

3. 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 the blockchain’s functions. Figure 3 is the LoRaWAN network server inner architecture.

The blockchain manager component implements the blockchain functions of packaging transaction, hashing transaction, verify transaction, making block and storing blockchain etc. A message process flow is shown in Figure 4 below. If the message is sent from the ABP mode, then the steps of joining network can be ignored.
End Note

Fig. 4. Message Process Flow

Figure 5 below shows how the blockchain data structure is stored in each NS node. The hash values on the block head will be different in implementation. In Figure 5, the number of transaction in one block is 2000, which also can be changed when necessary. For some lightweight client of the network server, it allows only storing the block heads without the full blockchain, and 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)

Fig. 5. Example of Blockchain Data Structure
4. Conclusion

It should be clear to all developers of LoRaWAN solutions that LoRa and the LoRaWAN protocol 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.

Acknowledgments

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

References

LoRa Alliance (2015a), LoRaWAN Specification V1.0, Jan., 2015 [Internet]. Available: https://www.lora-alliance.org/portals/0/specs/LoraWAN%20Specification%201R0.pdf
LoRa Alliance (2017a), LoRa Alliance Technology [Internet]. Available: https://www.lora-alliance.org/What-Is-LoRa/Technology
Nakamoto, S. (2008), "Bitcoin: A peer-to-peer electronic cash system".
Samaniego, M. and Deters, R. (2016a), "Blockchain as a Service for IoT", in 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).

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 got the PhD degree in 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 B.Sc. in Computer Science and Technology from Peking University, M.Eng. in Computer Engineering in Beijing University of Technology, and Ph.D. in Nanyang Technological University respectively. His research interests include Artificial Intelligence, Software Agents, Multi agent Systems (MAS); 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. Prof. 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 (AI) technologies for help the elderly lead an active, healthy and dignified lifestyle.
Siyuan Liu got her B.Sc and M.Sc 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. Currently she is 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 system and incentive mechanism design in crowdsourcing.