Using Blockchain Technology to Build Trust in Sharing LoRaWAN IoT

Jun Lin
The Joint NTU-UBC Research Centre of Excellence in Active Living for the Elderly
Nanyang Technological University
Singapore
junlin@ntu.edu.sg

Zhiqi Shen
School of Computer Science and Engineering
Nanyang Technological University
Singapore
zqshen@ntu.edu.sg

Chunyan Miao
The Joint NTU-UBC Research Centre of Excellence in Active Living for the Elderly
School of Computer Science and Engineering
Nanyang Technological University
Singapore
ascymiao@ntu.edu.sg

ABSTRACT

With[1] 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. Comparing to NB-IoT network that mainly built and managed by mobile network operators, LoRa wide-area network (LoRaWAN) is mainly operated by private companies or organizations, which will bring the trust issues between application customers and network operations. In this paper, we proposed a blockchain technology based solution to build an open, trusted, decentralized and tamper-proof system for LoRaWAN. To the best of our knowledge, this is the first work that integrating blockchain technology and LoRaWAN IoT technology.

CCS CONCEPTS

• **Computer systems organization → Embedded and cyber-physical systems**

KEYWORDS

Blockchain, Internet of Things, LoRa, LoRaWAN

ACM Reference format:

J. Lin, Z. Shen, and C. Miao. 2017. Using Blockchain Technology to Build Trust in Sharing LoRaWAN IoT. In *Proceedings of 2nd International Conference on Crowd Science and Engineering, Beijing, China, July 6-9, 2017 (ICCSE'17)*, 6 pages. https://doi.org/10.1145/3126973.3126980.

1 INTRODUCTION

As a major research branch 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 by making them more intelligent and efficient. According to Gartner, the total spending on devices and services will reach almost $2 trillion in 2017. And by 2020, there will be more than 20 billion connected things all over the world [1].

Different IoT technologies can be applied to different application areas and practical scenarios. As different application areas have specific requirements and considerations which mean different technology is needed. 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 5th generation (5G) solution based on cellular technology can provide large coverage but it consumes a lot of power. Low-Power Wide-Area Network (LPWAN) technologies are targeting at these emerging applications and markets.

As recently as early 2013, the term "LPWAN" did not even exist [2]. However, as the IoT market rapidly grown, LPWAN became one of the faster growing areas in IoT. Many of the LPWAN technologies depicted in Tab. 1 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 a LPWAN solution intended for systems that 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 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

ICCSE'17, July 6–9, 2017, Beijing, China
© 2017 Association for Computing Machinery.
ACM ISBN 978-1-4503-5375-5/17/07…$15.00
https://doi.org/10.1145/3126973.3126980

environment. It is a spread spectrum solution which uses wide bandwidth to help protect against deliberate interference or environmental noise. According to LoRa’s documentation [3], the LoRaWAN, network used by LoRa technology, is capable of providing data rates from between 0.3kbps to 50kbps which varies based on 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 [4]. 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 [5]. 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 be burdened by customers and end users.

Table 1: Comparison of LPWAN Technologies

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 - 125k Hz	100k Hz	180k Hz	1.08M Hz
Data Rate	0.3 - 50k bps	10 - 100k bps	<250k bps	1 M bps
Range (km)	2 - 5 (urban) 15 (suburban) 45 (rural)	3 - 10 (urban) 30 - 50 (rural)	2.5 - 5	2.5 - 5
Coverage	157dB	149dB	164dB	160dB
Capacity	40k/cell	50k/cell	200k/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

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

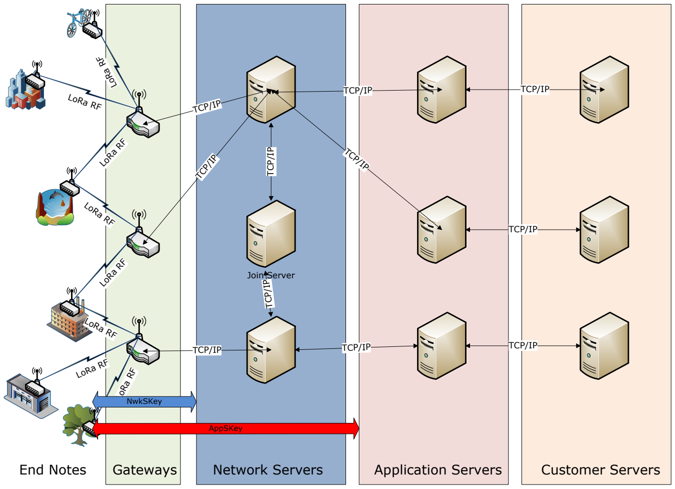

Figure 1: LoRaWAN Architecture.

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 [6].

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 specification 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 [6]. In some LoRaWAN implementation, the network controller is used for adapting the algorithms on end note specific radio parameters and application type [6], as well as the join server is used for security key provisioning during the network join procedure [7]. In several systems already deployed in industry, 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 them via cellular networks.

Comparing with other IoT solutions, the LoRaWAN protocol has equipped 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 (Activation-By-Personalisation). 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 join procedure. Another way is OTAA (Over-the-Air Activation). 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 note'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, as well as 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 man in the middle attack to recover the clear-text data. Even for the network server also cannot decrypt the application data when it has no the AppSKey in some LoRaWAN deployments [7].

However, the public LoRaWAN networks operated by one single organization are facing not only the security issue but the trust issue. People trust mobile operators as they have invested a lot of cost on the spectrum resource and telecommunication infrastructure that makes customer believe that operators will not be evil under the strict supervision by the government. But how to let people trust a public LoRaWAN can help them to transport data from gateways to application servers without stealing, tampering and cheating? That is our vision in this paper. The blockchain technology proposed by Nakamoto in 2008 that underpins Bitcoin the first cypto-currency system [8], 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. Not only this, the architecture should allow any existing server to join into this peer to peer network when it follows the design, which will quickly expand the data processing capacity of whole network and makes it to be a sharing LoRaWAN system.

The rest of this paper is structured as follows. In Section II, we survey 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 [9]. 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. The blockchain contains a certain and verifiable record of every single transaction ever made.

Blockchain originally is developed to support crypto-currency, Bitcoin [8], 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 wide range of applications in both financial and non-financial world. The main hypothesis of 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 happened 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 to 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 [8]. 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 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 [10].

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 many researchers who have studied the integration of blockchain and IoT technology.

In [9], authors discussed how a blockchain-IoT combination: 1) to facilitate the sharing of services and resources leading to the creation of a marketplace of services between devices and 2) to allows 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.

In [11], authors 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 city are 1) the resilience to 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 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.

In [12], authors discussed that IoT security and privacy remain a major challenge, mainly due to the massive scale and distributed nature of IoT networks. The blockchain technology provides decentralized security and privacy, but they involve significant energy, delay, and computational overhead that is not suitable for most resource-constrained IoT devices. So they proposed a lightweight instantiation of a blockchain particularly geared for use in IoT by eliminating the Proof of Work (POW) and the concept of coins. Their approach was exemplified in a smart home setting and consists of three main tiers namely: cloud storage, overlay, and smart home. In their 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.

In [13], authors 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 smart contract script to save data coming from meter and smart phone. Their experiment shows using Ethereum account, meter constantly sends electricity use and smart phone sends policies for air conditioner and light bulb. And air conditioner and lightbulb constantly checks the values on Ethereum to update their devices. When necessary, they switch their mode from normal to energy-saving. This is a good application example for the integration of blockchain and IoT.

In [14], author 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. In another paper [15], the same authors discussed the idea of using blockchain as a service for IoT and evaluated the performance of a cloud and edge hosted blockchain implementation.

Although above researchers have explored the integration even implementation of blockchain and IoT technologies, those research seldom target the LoRaWAN. As the LoRaWAN even 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, current main issue for LoRa technology is not the security concerns, but the network coverage issue. Big mobile operators tend to choose cellular technology based NB-IoT as they already have the licensed spectrum resources. The expensive cost of building network can be earned back 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 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 server, which can utilize both advantages of blockchain technology and LoRaWAN technology to provide an open, trusted, decentralized and tamper-proof network system.

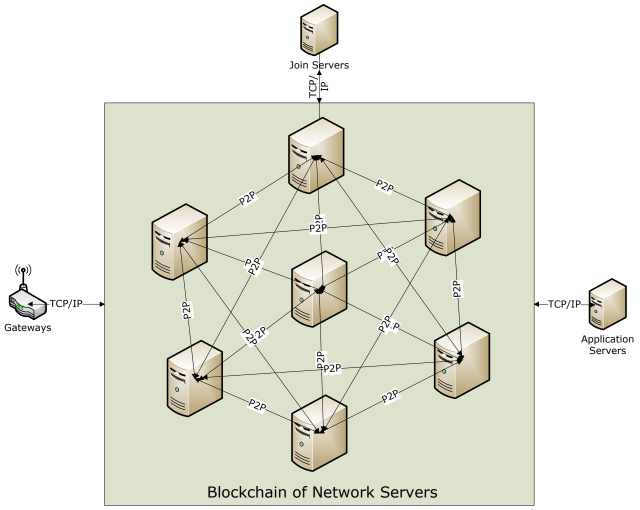

Figure 2: Blockchain Architecture for LoRaWAN Server

In Fig. 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 storaging etc.
2) For Join Servers: LoRaWAN's join servers normally are provided by end note'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. Fig. 3 is the LoRaWAN network server inner architecture.

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

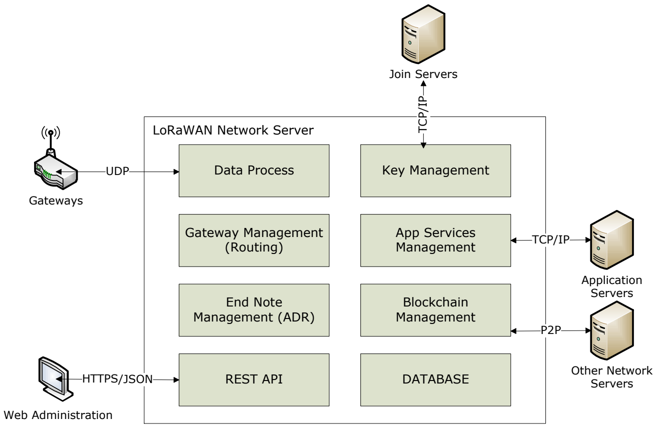

Figure 3: LoRaWAN Network Server Inner Architecture

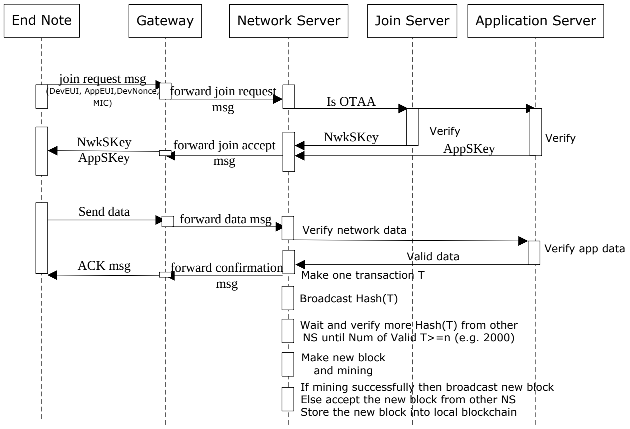

Figure 4: Message Process Flow.

As an example, the blockchain data structure stored in each NS node is designed as Fig. 5. The hash values on block head will be different when implementing. In the example, the number of transaction in one block is 2000, which also can be changed when necessary. For some lightweight client of network server, it allows only storing the block heads without the full blockchain, and then it still can use the Simplified Payment Validation (SPV) method to verify that confirmed transactions are part of a block, but it cannot provide the full ledger to download. [16]

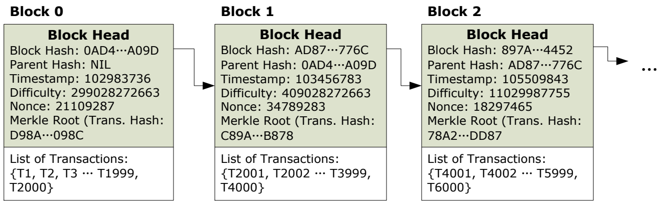

Figure 5: Example of Blockchain Data Structure.

4 CONCLUSIONS

It should be clear to all developers of LoRaWAN solutions that LoRa and the LoRaWAN protocol allow secure solutions to be developed that protect the company and the end user 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 integrating blockchain technology and LoRaWAN IoT technology. This integration utilize both advantages. 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 function 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 network 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

[1] Gartner. 2017. Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, Feb., [Internet]. Available: http://www.gartner.com/newsroom/id/3598917.

[2] LoRa Alliance, LoRa Alliance Technology [Internet]. Available: https://www.lora-alliance.org/What-Is-LoRa/Technology

[3] LoRa Alliance. 2015. LPWA Technologies Unlock New IoT Market Potential, Machina Research. [Internet]. Available: https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRa-Alliance-Whitepaper-LPWA-Technologies.pdf.

[4] R. Sinha, Y. Wei and S. Hwang. 2017. A survey on LPWA technology: LoRa and NB-IoT, Vol. 3, Issue 1, *ICT Express*, 14–21. DOI: https://doi.org/10.1016/j.icte.2017.03.004

[5] 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*.

[6] LoRa Alliance. 2015. LoRaWAN Specification V1.0. [Internet]. Available: https://www.lora-alliance.org/portals/0/specs/LoRaWAN%20Specification%201R0.pdf

[7] LoRa Alliance. 2017. LoRaWAN Security Full End-to-End Encryption for IoT Application Providers. [Internet]. Available: https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN_Security-Whitepaper_V6_Digital.pdf

[8] S. Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system.

[9] K. Christidis and M. Devetsikiotis. 2016. Blockchains and Smart Contracts for the Internet of Things, *IEEE Access*, Special section on the plethora of Research in IoT, 2292–2303. DOI: https://doi.org/10.1109/ACCESS.2016.2566339

[10] V. Morabito. 2017. Blockchain Value System, *Business Innovation Through Blockchain*, 21-39.

[11] K. Biswas and V. Muthukkumarasamy. 2016. Securing Smart Cities Using Blockchain Technology, in *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). DOI: https://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198

[12] A. Dorri, S. Kanhere and R. Jurdak. 2017. Blockchain for IoT security and privacy: The case study of a smart home, in *Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops* (PerCom Workshops). DOI: https://doi.org/10.1109/PERCOMW.2017.7917634

[13] S. Huh, S. Cho and S. Kim. 2017. Managing IoT Devices using Blockchain Platform, in *Proceedings of the 19th International Conference on Advanced Communication Technology (ICACT)*. DOI: https://doi.org/10.23919/ICACT.2017.7890132

[14] M. Samaniego and R. Deters. 2016. Using Blockchain to push Software-Defined IoT Components onto Edge Hosts, in *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies*. DOI: https://doi.org/10.1145/3010089.3016027

[15] M. Samaniego and R. Deters. 2016. 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)*. DOI: https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102

[16] A. Gervais, S. Capkun, G. O. Karame and D. Gruber. 2014. On the privacy provisions of Bloom filters in lightweight bitcoin clients, in *Proceeding of the 30th Annual Computer Security Applications Conference (ACSAC'14)*, 326-335. DOI: https://doi.org/10.1145/2664243.2664267