Blockchain-based system for IoT devices using post-quantum cryptography

By Bakhtiyor Yokubov, Lu Gan, Cong Ling

Electronic and Computer Engineering Department, Brunel university London, UK;
Electrical and Electronic Engineering Department, Imperial College London, UK

Abstract

Blockchain is a distributed ledger maintained by network nodes, which records transactions executed between nodes (in the form of messages sent from one node to another). Information inserted in the blockchain is public, and cannot be modified or erased. Smart contracts are self-executing contracts (generally saved on a blockchain) whose terms are directly written into lines of code. Blockchain infrastructure is built with several elements of network protocols, cryptographic concepts, and mining hardware. All these elements depend on each other in some sense. If we look into the layered architecture of blockchain, each layer is dependent on its upper and lower layers for some input/output. Thus, there are many infrastructure dependencies in blockchain. For instance, the data from the smart contract layer is an input to the transaction layer that outputs actual transactions; the data from the consensus layer results in an input to the network layer through a communication protocol; and the data from the network layer data is sent to the database through database storage management. These dependencies must be taken into account while building a comprehensive blockchain framework for any use case; otherwise, some of the blockchain functionalities will not be fulfilled. Blockchain technology has gained significant prominence in recent years due to its public, distributed, and decentration characteristics, which was widely applied in all walks of life requiring distributed trustless consensus. However, the most cryptographic protocols used in the current blockchain networks are susceptible to the quantum attack. Recent advances in quantum computing pose a severe threat to classical cryptography, as most of the widely used cryptography is based on the hardness of some problem which can be efficiently solved using quantum computers. Thus, research in the Post-Quantum cryptography has taken a massive leap. The security impact of breaking public key cryptography by quantum computers would be tremendous. Elliptic curve cryptography (ECC), which is an approach to public key cryptography, is mostly used in blockchain applications. Using a variant of Shors algorithm, a quantum computer can easily forge an elliptic curve signature that underpins the security of each transaction in blockchain and so breaking of ECC will affect blockchain in terms of broken keys, hence, digital signatures. In our paper, we provide description of how blockchain works, integration of blockchain with IoT and use of post-quantum cryptography in blockchain.

1. INTRODUCTION

A rapid increasing number of physical devices are being connected to the Internet at an unprecedented rate realizing the idea of the Internet of Things (IoT) [Al-Fuqaha et al]. Some estimates approximate more than 30 billion devices will be registered as IoT devices by the end of 2020 and it might increase up to 75 billion by 2025 generating trillions of transactions and producing huge amount of data. IoT devices are any devices which are connected to the internet and able to talk each other without user interaction. There are several domains and environments which IoT can play main role and improve quality of human lives. These application domains include transportation, healthcare, industry, smart home and many others. IoT aims to improve operation efficiency and production throughput, reduce the machine downtime and enhance product quality.

From security and privacy point of view, the main drawback of the IoT applications and platforms is their dependence on a centralized communication. Lack of security measure may lead to critical issues like persons subjected to physical damage such as burglary due to the hacking of smart alarm system of house. Considering the limitations of existing clientserver and cloud technologies, combined with rapid scalability of IoT, many researchers have suggested using blockchain as a potential solution for security and privacy issues.

Blockchain and distributed ledgers are fast becoming a key instrument in triggering different projects in majority of industries, such as, finance, healthcare, education and the government sector. One of the main reasons for this explosion of interest is using blockchain system it will be possible to share transactions and validate them in a distributed and decentralized manner without need of central authority. Unlikely with previous applications that could run only through trusted third party, blockchain can achieve decentralized transaction validation saving cost and time spent at the central agency. In addition, blockchain can ensure immutability, integrity, nonrepudiation and traceability of the transactions.

Blockchain is essentially a perfect complement to IoT with the improved interoperability, privacy, security, reliability, and scalability. However, due to rapid development of quantum computers, the most cryptographic protocols used in the current blockchain networks are susceptible to the quantum attack. Some of researchers believe that using post-quantum cryptography over existing channels will resist blockchain system from quantum attacks [Li et al].

The goal of this paper is to provide description of how blockchain works, integration of blockchain with IoT and use of post-quantum cryptography in blockchain.

The rest of this paper is organized as follows: Section II provides brief description of blockchain system. In Section III, we look into how IoT and blockchains can be used together, and highlight existing blockchain integrated IoT applications. In section IV, we introduce some lattice problems and some lemmas. In section V, we analyse potential solution using post-quantum cryptography in blockchain system. Section VI presents summary, concludes this study and introduces future work open issues.

2. BLOCKCHAIN OVERVIEW

In general, blockchain can be considered as distributed timestamped data structure. Blockchain allows non-trusted members to interact with each other verifiable manner without need of third-party authority [Christidis et al]. Bitcoin is the first electronic peer-to-peer cash system in blockchain context which introduced by Nakamoto in 2008 [Satoshi Nakamoto]. Each block in blockchain is identified with its cryptographic hash. Each block references to the hash of previous block, all the way back to the first (genesis) block, thus creating blockchain or chain of blocks - see Figure 1.

There are two types of blockchain available based on its functioning: permissionless and permissioned. In permissioned or private blockchain, only the limited number of users can participate in consensus and have right to validate transactions while in per-

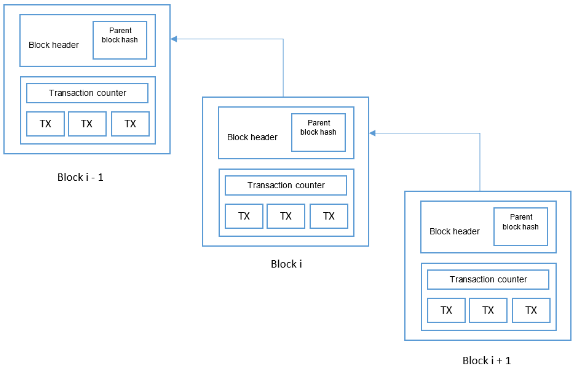

FIGURE 1. A block structure in blockchain

missionless or public blockchain, anyone can join the network and validate transactions. Well-known implementations of public blockchains include Bitcoin, Ethereum, Litecoin and, in general, most cryptocurrencies. Multichain is an example of an open platform for building and deploying private blockchains.

One of the main advantages of blockchain technology is to validate transactions trustfulness in a decentralized environment without need of any middlemen authority using consensus algorithms. The different consensus mechanisms can be used depending on blockchain type. The most common ones are Proof-of-Work (PoW), Proof-of-Stake (PoS) and Byzantine Fault Tolerance (BFT). PoW protocols require miners to solve computational hard task in order to create a block. PoS protocols divide stake blocks proportionally to the miners taking into account their current wealth.

In order to illustrate how an asset transfer works, it is easy to understand with example of banking world. Let's assume Alice wants to transfer some amount of her digital currency to Bob. She first initiates a transaction using his digital wallet. The transaction includes information about sender's address, receiver's address (public key of the receiver), and amount of money. Then, she broadcasts the initiated transaction to other participants in the blockchain network. When transaction is validated, it is appended to the end of chained transactions. Once a miner successfully solves the puzzle, the block is added into blockchain and every participant saves a replica of updated blockchain. Finally, Bob gets the amount of assets to his digital wallet.

One of the main advantages of blockchain is use of smart contracts in its applications. An idea of smart contract first introduced by Nick Szabo in 1994. It was defined as a computerized transaction protocol that executes the terms of a contract. Smart contact satisfies common contractual conditions minimizing the need for trusted intermediaries. In simply term, it can be considered as a digitized form of a legal contract. Smart contracts have the following properties: autonomy, trust, backup, savings.

3. BLOCKCHAIN AND IoT

There are different research works available which address the usage of blockchain IoT domains.

[Novo] proposed new decentralized access control architecture for IoT based on blockchain. By the help of management hub, the numerous constrained networks can be connected to the blockchain at the same tame. Moreover, the different management hubs nodes can be spread through blockchain network giving high flexibility to their solution. They believe, their solution gives considerable results by applying different IoT domains. In [Sharma et al], blockchain and SDN based new secure distributed IoT network architecture has been proposed which improves performance and capacity of the system. One of the main role of this model is to resist attacks like poising/ARP spoofing, DDoS/DoS attacks, and detect security threats. In [Li et al], authors proposed integration of satellite chain with Hyperledger Fabric v0.6 which can transfer assets without compromising security and soundness of the system. [Dwivedi et al] introduced a new approach by developing a patient-centric access control for electronic medical records using lightweight cryptographic primitives which provides security and privacy. From authors point of view, elimination of Prove of Work (PoW) consensus mechanism concept makes blockchain suitable for IoT devices. [Biswas et al] proposes blockchain based framework which connects smart city devices without compromising privacy and security. [Gao et al] proposed blockchain based payment system securing important information while sending data. They used Hyperledger to evaluate its feasibility and effectiveness.

In summary, Blockchain is essentially a perfect complement with reducing the cost for trusted third party, assuring security, improving data traceability, and verifying the data authenticity and preserving privacy.

4. PRELIMINARIES

In this section we introduce descriptions of lattice-based cryptography and some lemmas.

Definition 1 (Lattice [Micciancio et al]): Given n-linearly independent the set of vectors $\mathbf{v_1}, \mathbf{v_2}, ..., \mathbf{v_n} \in \mathbb{R}^m$, lattice L generated by them is the set of vectors

$$\mathbf{L}(\mathbf{v_1}, \mathbf{v_2}, ..., \mathbf{v_n}) = \{\sum_{i=1}^{n} a_i \mathbf{v_i} | a_i \in \mathbb{Z}, i = 1, ..., n\} \qquad (1)$$

$V = [\mathbf{v_1}, \mathbf{v_2}, ..., \mathbf{v_n}]$ is known as a basis of the lattice L. The same lattice can be represented by different lattice bases. Given a prime number q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, define:

$$\Lambda_q(\mathbf{A}) = \{y \in \mathbb{Z}^m | y = \mathbf{A}^T x \mod q, x \in \mathbb{Z}^n\}, \qquad (2)$$

$$\Lambda_q^{\perp}(\mathbf{A}) = \{y \in \mathbb{Z}^m | \mathbf{A}_y = 0 \mod q\}. \qquad (3)$$

Definition 2 (Lattice SIS Problem): Given an integer q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and a real constant $v > 0$, find a nonzero vector $\mathbf{x} \in \mathbb{Z}^m$ such that $\mathbf{A}\mathbf{x} \equiv 0 \mod q$ and $\|\mathbf{x}\| \leq v$.

Based on the hardness of SIS problem, for any polynomial-bounded m, v and any prime $q \geq v \cdot w\sqrt{n \log n}$, solving SIS on the average is as hard as approximating the shortest independent vector problem (SIVP) in the worst case.

Definition 3 ([Micciancio et al] Smoothing Parameter): For an m - dimensional lattice Λ, and positive real $\varepsilon > 0$. Its smoothing parameter $\eta_\varepsilon(\Lambda)$ is the smallest s such that $\rho_{1/s}(\Lambda^\star \backslash \{0\}) \leq \varepsilon$

Lemma 1 [Gentry et al]: For a lattice L with dimensional m and rank n, $\mathbf{c} \in \mathbb{Z}^m$, positive real $\varepsilon < \exp(-4\pi)$ and $s \geq \eta_\varepsilon(L)$, for random $\mathbf{x} \in L$ such that $D_{L,s,\mathbf{c}}(\mathbf{x}) \leq \frac{1+\varepsilon}{1-\varepsilon}2^{-n}$.

Lemma 2 [Micciancio et al]: For any lattice L with dimensional m and rank n, $\mathbf{c} \in span(L)$, a real $\varepsilon \in (0,1), s \geq \eta_\varepsilon(L)$, we have

$$\Pr_{x \leftarrow D_{L,s,c}}[\|\mathbf{x} - \mathbf{c}\| > s\sqrt{m}] \leq \tfrac{1+\varepsilon}{1-\varepsilon}2^{-n}. \tag{4}$$

Gentry et al. proposed an algorithm *SampleD* that samples from a discrete Gaussian over any lattice. *SampleD* takes some n - dimensional basis $\mathbf{A} \in \mathbb{Z}^{n\times m}$ of rank m, Gaussian parameter s that is related to the length $\|\mathbf{A}\|$ of the basis, a centre $\mathbf{c} \in \mathbb{R}^n$, and efficiently outputs a sample from (a distribution close to) $D_{L(\mathbf{A},s,\mathbf{c})}$.

Lemma 3 [Gentry et al]: For any lattice basis $\mathbf{A} \in \mathbb{Z}^{m\times n}$, any real $s \geq \|\mathbf{A}\|\omega(\sqrt{\log n})$ and any $\mathbf{c} \in \mathbb{Z}^m$, the output distribution of $SampleD(\mathbf{A}, s, \mathbf{c})$ is within negligible statistical distance of $D_{\mathbf{L(A)},s,\mathbf{c}}$

Lemma 4 [Gentry et al]: Let $q > 2$, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{B}$ is a basis of $\Lambda_q^\perp(\mathbf{A})$, and Gaussian parameter $s \geq \|\widetilde{\mathbf{B}}\|\omega(\log m)$. Then any vector $\mathbf{y} \in \mathbb{Z}_q^n$, algorithm $SamplePre(\mathbf{A}, \mathbf{B}, \mathbf{y}, s)$ outputs a vector $\mathbf{e} \in \mathbb{Z}_q^m$ from a distribution that is statistically close to $D_{\Lambda_q^\perp(\mathbf{A}),s}(x)$.

Lemma 5 [Gentry et al]: For any prime $q = poly(n)$ and any $m \geq 5n\lg q$, there is a probabilistic polynomial-time algorithm $TrapGen(1^n)$ that outputs a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and a full-rank set $\mathbf{S} \subset \Lambda^\perp(\mathbf{A}, q)$. The distribution of $\mathbf{A}$ is statistically close to uniform over $\mathbb{Z}_q^{n\times m}$ and the length $\|\mathbf{S}\| \leq L = m^{1+\varepsilon} \wedge \varepsilon > 0$.

5. LATTICE BASED BLOCKCHAIN

For quantum resistant methods, researchers is now focused on Lattice based cryptography, which has commonly used one that other theories in post-quantum cryptography and suitable for the blockchain systems. In 2008, [Gentry et al] proposed the first lattice-based signature scheme which is provable secure in the random oracle based on SIS problem.

[Yin et al] proposed a novel transaction authentication scheme using lattice-based cryptography which could resist quantum attack, while maintaining the wallet lightweight in blockchain system. The length of signature in their schema is O(1) which is more suitable for storage in blockchain comparing to other signature length. [Gao et al] use lattice basis delegation algorithm to generate secret keys with selecting a random value, and use preimage sampling algorithm to sign message. The authors believe that the size of signature and secret keys is shorter compared to previous signature schemes. [Ma et al] propose lattice-based multisignature scheme that is secure in the random oracle model under the ring version of the short integer solution (Ring-SIS) assumption. [Esgin et al] introduce an efficient and post-quantum1 RingCT protocol based on computational lattice problems like M-SIS and M-LWE. [Li et al] propose a new lattice-based signature scheme using bonsai tree technology for generating sub-private and sub-public keys. Moreover, security of the proposed signature scheme is based on the Short Integer Solution (SIS) problem.

6. CONCLUSION AND FUTURE WORKS

Blockchain is essentially a perfect complement to IoT with the improved interoperability, privacy, security, reliability and scalability. However, the most cryptographic protocols used in the current blockchain system are susceptible to quantum attacks with rapid development of sufficiently large quantum computers. In order to resist these quantum attacks we can use post-quantum cryptography in particular a new lattice-based cryptography in blockchain system.

As future work, there are exists challenging research problems in implementing blockchain based applications for IoT devices using post-quantum cryptography protocols.

REFERENCES

A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376, Fourthquarter 2015.

C. Li, X. Chen, Y. Chen, Y. Hou, and J. Li. A new lattice-based signature scheme in post-quantum blockchain network. *IEEE Access*, 7:2026–2033, 2019.

K. Christidis and M. Devetsikiotis. Blockchains and smart contracts for the internet of things. *IEEE Access*, 4:2292–2303, 2016.

Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Cryptography Mailing list at https://metzdowd.com*, 03 2009.

O. Novo. Blockchain meets iot: An architecture for scalable access management in iot. *IEEE Internet of Things Journal*, 5(2):1184–1195, April 2018.

P. K. Sharma, S. Singh, Y. Jeong, and J. H. Park. Distblocknet: A distributed blockchains-based secure sdn architecture for iot networks. *IEEE Communications Magazine*, 55(9):78–85, Sep. 2017.

Wenting Li, Alessandro Sforzin, Sergey Fedorov, and Ghassan Karame. Towards scalable and private industrial blockchains. pages 9–14, 04 2017.

Ashutosh Dwivedi, Gautam Srivastava, Shalini Dhar, and Rajani Singh. A decentralized privacy-preserving healthcare blockchain for iot. *Sensors*, 19:326, 01 2019.

K. Biswas and V. Muthukkumarasamy. Securing smart cities using blockchain technology. In *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, pages 1392–1393, Dec 2016.

Feng Gao, Liehuang Zhu, Meng Shen, Kashif Sharif, Zhiguo Wan, and Kaili Ren. A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. *IEEE Network*, PP:1–9, 04 2018.

Daniele Micciancio and Oded Regev. *Lattice-based Cryptography*, pages 147–191. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

D. Micciancio and O. Regev. Worst-case to average-case reductions based on gaussian measures. In *45th Annual IEEE Symposium on Foundations of Computer Science*, pages 372–381, Oct 2004.

Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. volume 14, pages 197–206, 05 2008.

W. Yin, Q. Wen, W. Li, H. Zhang, and Z. Jin. An anti-quantum transaction authentication approach in blockchain. *IEEE Access*, 6:5393–5401, 2018.

Yulong Gao, Xiubo Chen, Ying Sun, Xinxin Niu, and Yixian Yang. A secure cryptocurrency scheme based on post-quantum blockchain. *IEEE Access*, PP:1–1, 04 2018.

C. Ma and M. Jiang. Practical lattice-based multisignature schemes for blockchains. *IEEE Access*, 7:179765–179778, 2019.

Muhammed Esgin, Raymond K. Zhao, Ron Steinfeld, Joseph Liu, and Dongxi Liu. Matrict: Efficient, scalable and post-quantum blockchain confidential transactions protocol. pages 567–584, 11 2019.