Post-Quantum Blockchain for a Scalable Smart City

Abir EL Azzaoui, Jong Hyuk Park

Department of Computer Science and Engineering, Seoul National University of Science and Technology, South Korea
{abir.el, jhpark1}@seoultech.ac.kr

Abstract

Smart Cities enclose various industries, sectors, and components. A Smart City application benefits from the data collected using a tremendous number of sensors serving to establish an accurate corporative decision. However, the communication between different components and application of a Smart City exhort security measures as it faces critical security attacks and integrity issues. To medicate this dilemma, researches have used the assistant of Blockchain to secure Smart Cities and improve its decision's accuracy. Yet, with the recent development of Quantum Computers, Quantum-based algorithms are certainly menacing the security of classical encryption together with Blockchain itself. Thus, threaten the insurance of Blockchain-based application including critical applications such as Smart Cities. In this paper, we demonstrate the Blockchain-based Smart Cities' framework and we present an understanding overview that encloses the menaces of a Quantum computer on Blockchain and Blockchain-based applications essentially Smart City. We explain as well some Post-Quantum solutions concerning the security of Blockchain-based Smart City.

Keywords: Post-Quantum Blockchain, Quantum Blockchain, Smart City, Quantum Computers

1 Introduction

The subject of Quantum computing brings together ideas from classical information theory, computer science, and Quantum physics [1]. Theatrically, a Quantum computer is capable of solving problems that would be intractable on conventional computers. Russian-German mathematician Yuri Manin was the first to propose the idea of Quantum computing in his book Computable and Non-computable [2] published in 1980. 2 years later, the Nobel Prize winner physicist Feynman [4] published an article when he noticed that a Quantum physical system of R particles cannot be simulated by an ordinary computer without an exponential slowdown in the efficiency of the simulation [3]. However, a system of $\mathbb{R}$ particles in classical physics can be simulated well with only a polynomial slowdown. Accordingly, the reason is that the description size of a particle system is linear in $\mathbb{R}$ in classical physics but exponential in $\mathbb{R}$ in Quantum physics. Thus, Feynman proposed the use of a computer-based on Quantum physics laws to solve this problem.

A classical computer uses transistors to process information in the form of various combinations of 0 and 1 to accomplish the calculations, the computer processing power depends on the number of transistors. On the other way, a Quantum computer uses the Quantum mechanical states of elementary particles, specifically the internal angular momentum known as spin. In this case, a spin-up accorded to binary 1 and spin down is accorded to binary 0. According to Quantum physics laws, every elementary particle can be in multiple states simultaneously. Thus, the spin can be up and down at the same time, introducing the concept of Qbit. Instead of two values 0 or 1, a Qbit store proportion of the two values 0 and 1 at the same time. A computer with *n* Qbit is capable of performing 2^n combinations synchronously. This functionality speeds up the computations exponentially, allowing a Quantum computer to solve hard mathematical problems in a short time.

Nowadays, numerous applications and frameworks are remarkably using Blockchain as a security platform [31]. In practically Smart Cities, which were planned to rely on Blockchain to secure data communication between its different layers and components. The development of a Quantum computer creates a prodigious and critical security threat on Blockchain-based Smart Cities. Thus, we discuss in this paper the potential Post-Quantum solutions to secure Blockchain-based Smart Cities against Quantum attacks.

Research contribution: the main contribution of our research is as follows:

- We demonstrate Blockchain-based Smart Cities' framework and its components in section two.
- We present an overview of Quantum threats on classical encryption methods including Blockchain in the third section.
- We mitigate and discuss some Post-Quantum solutions that are able to secure Blockchain-based Smart Cities against Quantum attacks in the fourth

*Corresponding Author: Jong Hyuk Park; E-mail: jhpark1@seoultech.ac.kr
DOI: 10.3966/160792642020072104025

section.

The main focus of this work is to present an overview of the potential Post-Quantum solution to secure Blockchain-based Smart Cities as the risk of Quantum attacks on Smart Cities is critical. Thus, the selection of consensus algorithms and key management methods fall out of the scope of our work.

2 Blockchain-Based Smart City

Blockchain as a distributed peer-to-peer secure ledger technology was adopted by multiple works of literature and applications into Smart Cities [25] to securely manage, and organize data communication between a different component in a Smart City without compromising its privacy and security. In this section, we present an overview of the security problems in a Smart City and some of the related works where Blockchain is used to improve the Smart Cities' environment. We discuss as well the Blockchain-enabled Smart City framework and explain its component.

2.1 Security Threats in Smart City and Blockchain Solutions

The heterogeneous nature of the Smart City makes it vulnerable to attacks. Especially at the level of resource-constrained devices where high-level security protocols cannot be applied. Moreover, the centralized structure of the Smart City creates an illegal upholding of data or data manipulation by certain individuals or groups, these groups can even deny the transmission of messages from one participant to another. Figure 1 presents the security threats that face a Smart City.

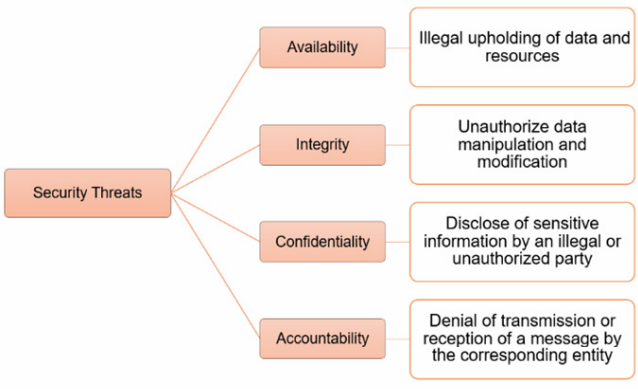

Figure 1. Security threats categories for a Smart City

These issues can be sorted using Blockchain technology. Rahman et al. [32] used Blockchain-based infrastructure to support security-and privacy-oriented Spatio-temporal Smart Cities. The proposed framework uses Artificial Intelligent (AI) for extracting significant event information and saves results in Blockchain for more accurate security. Sharma et al. [19] used Blockchain to create a vehicle network architecture in Smart City named Block-VN. The proposed architecture proved to be secure and operates in a distributed way to build a new distributed transport management system. Various other researches and papers have usefully managed to converge Blockchain into Smart Cities to create secure and private environment for data communication. However, as we argued above in the previous section, a Quantum -based algorithm can successfully break the security of Blockchain.

2.2 Blockchain-Enabled Smart City Framework

With the fast development of Smart Cities nowadays, information technology has been integrated to manage physical, social, and business infrastructures [18] including Blockchain technology. But firstly, we have to define the classical architecture for a Blockchain-enabled Smart City environment. Figure 2 presents the classical architecture which is composed of four layers:

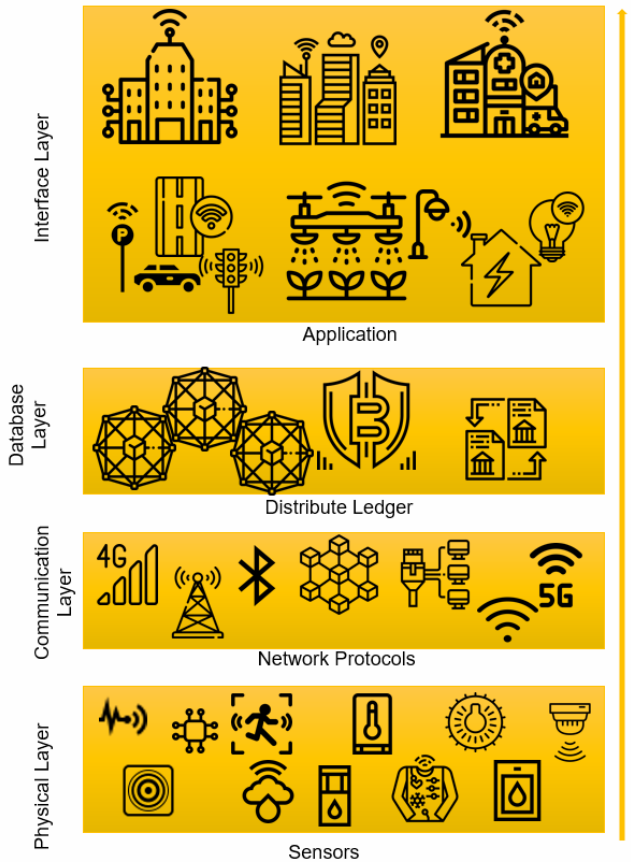

Figure 2. Blockchain-Enabled Smart City Framework

(1) Physical Layer: In the physical layer, the sensors and actuators collect massive amount of data [26]. These data are used to create an intelligent infrastructure that allows sharing information between legal parties to understand and develop the environment of a Smart City [30].

(2) Communication Layer: The data collected using the sensors in the application layer are forwarded to the database layer through the medium of the communication layer [27]. This layer uses heterogeneous communication and network protocols

including 5G networks, Wi-Fi, Ethernet, and so on. Blockchain ledger should be merged with the communication layer to ensure the security and integrity of data communication. Biswas et al. [20] proposed to use Telehash to create blocks that can record transactions and broadcast them in the network.

(3) Database Layer: Blockchain ledger resides in this layer to store the data transmitted from the sensors. Practically, we can define four types of Blockchain. Public or permission-less Blockchain in which anyone can join the network. Private or permissioned Blockchain in which a certain entity makes a restriction. A Smart Contract where the included acts are automatically executed without the intervention of a third party. And the consortium or semi-decentralized Blockchain that is controlled by an assortment of the approved entity and not just one. For security and scalability reasons, we believe that a private Blockchain is extremely advantageous in the database layer as it requires less time to perform the consensus between participated nodes meanwhile ensuring the security of the data.

(4) Interface Layer: The smart application in this layer are used conjointly to make decisions based on the information collected from the physical layer. The interface layer includes smart homes, smart farms, smart health care, smart transportation, and so on.

The heterogeneous nature of the Smart City creates several issues with key management and security. Knowing that a Smart City encloses a variety of sectors including financial sectors, industry, transportation, health-care systems, and general urban environments including smart homes. The threats of a Quantum attack are critical.

3 Quantum Threats on Blockchain-Enabled Smart City

Sign et al. [5] defined Blockchain as a collection of blocks; each block contains four parts: details of the transaction, the hash value of the present block and previous block, and the timestamp of the transaction. The transactions are signed with a hash value and verified by the participant miners. Blockchain platforms use the elliptic curve public key cryptography or the large integer factorization problem RSA to create a digital signature and secure the blocks [6]. These algorithms are based on the complexity of certain mathematical problems. In RSA encryption, the multiplication of large primes is easy and fast, however, factoring large composite numbers into two prime factors is a difficult mathematical problem and it took an exponential time that can last for hundreds of years to solve using classical computers. However, the general promise of Quantum computation is that such speedups for those difficult problems are guaranteed [8], thus breaking the RSA, DSA and similar encryption such as Elliptic Curves Cryptography, which is used in Blockchain, is possible and executable using a Quantum computer. In this section, we present two fundamental Quantum-based algorithms that create a potential risk on classical encryption algorithms and Blockchain.

3.1 Shor's Algorithm

Shor's algorithm can be used to attack RSA encryption as it provides a remarkable improvement in the efficiency of factoring large numbers [7]. Shor's algorithm is polynomial in the input length; thus, the calculation speed is exponentially higher than any other existing algorithms. To determine the prime factors of an odd integer N, you have to choose a co-prime of N, x. The order r relates x to N according to :

$$x^r \bmod N = 1 \tag{1}$$

And can be used to obtain the factors given by the greatest common divisor [9].

$$\gcd(x^{\frac{r}{2}} \pm 1, N) \tag{2}$$

In practical terms, the process to find r can only be done using a Quantum computer; however, this can make an RSA key of 4096 bits breakable.

3.2 Gover's Algorithm

Lov Grover dealt with another important problem of conducting a search through unstructured search space [33]. Supposing that we have an unsorted database with N elements counted from 0 to N-1. Using classical methods, to find a certain element E, we will have to test all the elements in the database one by one, which will take as average between $\frac{N}{2}$ and N attempts. However, using Quantum mechanics laws, Gover's algorithm was capable of noticeably reducing the number of attempts needed for this problem. This algorithm can reach square-root speedup $O\sqrt{N}$ over classical algorithms that can overtake the complexity of $O(N)$ in the unsorted database searching problem. Gover's algorithm has high potentials to successfully break a hashing function. However, the probability of finding the target result is not always 1.

Long [10] proposed a modified version of Grover's algorithm that can perform a searching function with a full successful rate by replacing the phase inversion in the original Grover' algorithm by the phase rotation through angle ϕ such as:

$$\phi = 2\arcsin(\frac{\sin[\frac{\pi}{4J+6}]}{\sin\beta}) \tag{3}$$

Where $\sin\beta = \frac{1}{\sqrt{N}}$ and J is an integer equal to or

greater than the integer part of: $\frac{[\frac{\pi}{2}-\beta]}{2\beta}$.

Accordingly, this version is appreciated in cases where the certainty is critical, and the preparation of the initial state and the change of the experimental setting during the computation process is complex.

4 Post-Quantum Blockchain-based Smart City Solutions

Quantum computers are being rapidly developed in the recent years. Google has reportedly managed to create a Quantum supremacy computer called "Sycamore". The computer uses 53 qubits and was able to solve in 200 seconds a complex computation that, accordingly, will take 10000 years to complete using the most powerful supercomputers of today. Google is not alone in the Quantum race, IBM has opened the "IBM Q Network" which is a global community of companies, academic institutions, startups and research laboratories working all together to improve and advance Quantum computing. Apple, Intel, Microsoft, Amazon, and many more companies joined the competition to develop the future of computers. Those computers are certainly able to compute the above-mentioned algorithms in exponential time, which threaten the security of nearly all the encryption algorithms including Elliptic Curves Cryptography (ECC) on which Blockchain security is based. Thus, security measures must be taken before the menaces become true. In this section, we present some of the newly developed algorithms and methods that has been proved, based on the relevant related works, to be prone to Quantum attacks on Blockchain.

4.1 Lattice-based Cryptography

To define the lattice in this section, we use $\mathbb{R}$ as a set of all reals and $\mathbb{Z}$ as a set of positive integers. $\mathbb{R}^m$ is the m-dimensional Euclidean vector space where: $m \in \mathbb{Z}$, $n \in \mathbb{Z}$ and $m \geq n$.

Definition 1 (General lattice definition):

Lattice is a set of points in *n*-dimensional space with a periodic structure [11]. Giving independent vectors *b,* the lattice generated by them is the set of vectors such as:

$$\mathcal{L}(b_1, b_2, \ldots, b_n) = \sum_{i=1}^{n} [x_i b_i : x_i \in \mathbb{Z}, b_n \in \mathbb{R}^m] \quad \textbf{(4)}$$

The basis of the lattice $\mathcal{L}$ is $B = (b_1, b_2, \ldots, b_n)$ and the same lattice could be represented by different lattices.

Definition 2 (Lattice Short Integer Solution Problem [12]): Giving integer *i*, matrix $m \in \mathbb{Z}_i^{n*m}$, a real constant *c > 0*, find a nonzero vector $V \in \mathbb{Z}^m$ such as:

$$MV \equiv 0 \bmod i \text{ and } |V| \leq c \quad \textbf{(5)}$$

Based on the hardness of SIS problem, for any polynomial-bonded *m, c* and any prime:

$$i \geq c \cdot \varpi \sqrt{n \log n} \quad \textbf{(6)}$$

Solving the SIS problem is as hard as approximating the shortest independent vector problem (SIVP) in the worst case.

Ajtai [13] was the first to use lattice for cryptosystem as they adopt a random lattice as a public key with an n^c unique nonzero shortest vector, where the constant $c > \frac{1}{2}$ can be picked arbitrarily close to $\frac{1}{2}$. The lattice is picked according to the distribution described in their proposal. Lattice-Based cryptography was then adopted in numerous researches as it is believed to be secured against Quantum computers. Typically, it can be used to secure Blockchain against the Quantum attacks that can break Elliptic Curves Cryptography (ECC). Torres et al. [14] proposed a lattice-based on one-time Linkable Ring Signature (L2RS) scheme. This proposed scheme will enable the public to verify if two or more signatures were generated by the same signatory while assuring the anonymity and security using the Ring Short Integer Solution lattice hardness assumption. The proposal devises as well a new cryptocurrency privacy-preserving protocol called Lattice RingCT v1.0 using the Post-Quantum L2RS as a basis for block building along with homomorphic commitment primitive to ensure the Post-Quantum secure confidential transactions. Li et al. [15] deployed a new lattice-based signature scheme based on the SIS problem and proved to be prone to future Quantum attacks. The proposed scheme uses Bonsai Tree technology to generate the sub-public and sub-private keys, which help to create a lightweight wallet. The security proof of this proposal indicates that the lattice-based signature scheme is secure against the adaptively chosen message attack in the random oracle model, which makes it more suitable for transaction implementation in the Post-Quantum Blockchain network. Gao et al. [12] proposed another signature scheme based on the lattice problem as well, the authors used the lattice-based delegation algorithm to generate secret keys by selecting a random value. The security of this proposal can be reduced to the lattice SIS problem. The message is signed by the preimage sampling algorithm. Moreover, to reduce the correlation between the message and the signature, a double-signature was adopted using the first and last signature design. Applying this signature scheme on Blockchain creates a Post Quantum Blockchain (PQB). The analysis shows that the proposed cryptocurrency scheme is able to resist Quantum computing attacks.

4.2 Quantum Distributed Key

Another approach to finding a solution prone to Quantum attacks is to use a Quantum Distributed Key (QDK). QDK use generally individual photons to exchange cryptographic key data between users. Each photon represents a single bit of data that can be 1 or 0. Based on the theory of Quantum physics, the value of each bit is determined based on the state of the photon (the spin and polarization). To create the QDK, a laser is used at the sender-end to generate a series of single photons. The photon should be in one state of the polarization, horizontal or vertical, and this state will be measured again at the receiver-end. This method is considered to be highly secure as if an eavesdropper tries to measure the state of a single photon, the photon will be destroyed. Moreover, an eavesdropper can never generate the same photon again with the same polarization and the same spin. Thus, the receiver will notice an error in the received series of photons. The QDK stands behind the Heisenberg uncertainty principle, which states that it is impossible to measure both the velocity and position of certain Quantum particle at the same time.

QKD guarantees information-theoretic and unconditional security based on the laws of Quantum physics. Numerous researches and works have deployed this technique to secure the Blockchain network. Kiktenko et al. [16] used QKD as well to generate a secret key between two parties connected by a Quantum channel to transmit Quantum state and a public classical channel for post-processing procedures. The paper merged the QKD network layer into the current Blockchain system to protect the relevant sub-algorithm against the Quantum attacks. Accordingly, the technology enabling QKD networks have been demonstrated in many experiments and is now available through multiple commercial suppliers. The potential applications of QKD include securing critical infrastructures such as smart grids, financial institutions, and national defense [17]. However, QKD may not be viable for securing a full-scale cryptocurrency system as it consumes more computation power for the block creation procedure, but it can still be very useful to secure smaller distributed database.

4.3 Quantum Entanglement in Time

The term entanglement was used in Quantum mechanics after the famous paper published by Einstein, Podolsky, and Rosen [21] in 1935. The paper states that in spatially separated Quantum systems, there a "spooky action at a distance" as Einstein described it. This spooky action involves nonclassical correlations [22]. Rajan et al. [23] have deployed this ramification to create a Quantum Blockchain. This method is based on encoding Blockchain into a temporal Greenberger-Horne-Zeilinger (GHZ) state of photons that cannot coincide at the same time. The authors replaced the components of a classical Blockchain with a Quantum system, where they used a super-dense coding concept to use the Quantum Blockchain and convert the classical information into spatially entangled Bell states as follows:

$$|\beta_{xy}\rangle = \frac{1}{\sqrt{2}}(|0\rangle|y\rangle + (-1)^x|1\rangle|\bar{y}\rangle) \quad \textbf{(7)}$$

Where *xy* are two classical bits such as *xy = 00, 01, 10, 11.* and $\bar{y}$ is the negation of *y*. Based on that, the authors converted each block in the chain to a Quantum block record into a temporal Bell state, and they recorder the time of block creation such as the first block is created at time t=0:

$$|\beta_{r_1 r_2}\rangle^{0,\tau} = \frac{1}{\sqrt{2}}(|0^0\rangle|r_2^\tau\rangle + (-1)^{r_1}|1^0\rangle|\bar{r}_2^\tau\rangle) \quad \textbf{(8)}$$

With $r_1 r_2$ referring to the record.

Through the projection of temporal Bell state on two photons at the time $t = \tau$, entanglement is created between the two later photons absorbed consecutively at time $t = \tau$ and $t = 2\tau$. Notwithstanding that the two photons have never coexisted.

Using this record generation system, the authors encoded the whole Blockchain into temporal Bell states such as:

$$|\beta_{00}\rangle^{0,\tau}, |\beta_{10}\rangle^{\tau,2\tau}, |\beta_{11}\rangle^{2\tau,3\tau} \quad \textbf{(9)}$$

The Quantum Blockchain-based entanglement in time is a strong solution to secure Blockchain based-Smart Cities. Deploying this method, the records are still existent and can be readable but they cannot be touched as the photons that contain it do not exist anymore. Which will guaranty the integrity and confidentiality of Blockchain-based Smart Cities.

4.4 General Overview

Apart from the above mentioned Post-Quantum cryptosystem, we can find in the literature four other main schemes that can be applied on Blockchain including Code-base cryptosystem, Multivariate-based cryptosystem, Supersingular Elliptic Curve Isogeny cryptosystem and Hybrid cryptosystem. However, the encryption and decryption's performance of these mechanisms is limited and create restrictions on resource constraint devices. Further researches must be conducted before adopting these four Post-Quantum cryptosystem for Blockchain-based Smart Cities. Figure 3 present a summary of these schemes with the advantage and disadvantage of using them. Interested reader may refer to the study [28-29] for more details about the encryption, decryption and performance of these Post-Quantum cryptosystems.

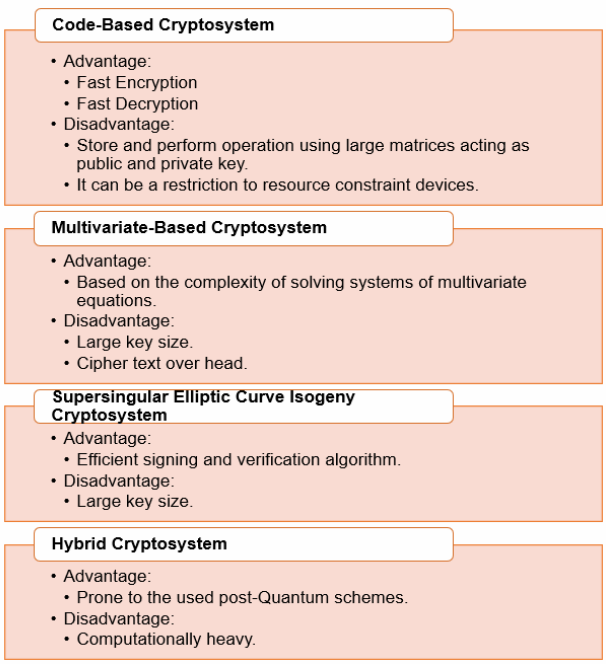

Figure 3. Post-Quantum cryptosystems for blockchain

5 Discussion and Open Research Challenges

The researches have proposed the integration of Blockchain into Smart Cities' applications to secure the communication between its components.

However, as Quantum computers are developing in a noticeable speed, the risk of a Quantum attack and breaking classical security algorithms is now censorious.

5.1 Discussion

Due to the heterogeneous nature of a Smart City, communication between its components and applications is mandatory to make an accurate decision. A smartphone in a Smart City can communicate with the smart home and send the owner's location immediately so thus the smart home can turn on the air conditioner for example. A healthcare sensor can regularly monitor the user's health condition and immediately seek virtual medical assistant in urgent cases. These types of communication are perilous as they hold critical information. An illegal upholds of data and resources, unauthorized data manipulation, or the denial of the message's communication between different components are all considered as risky security threats for Smart Cities. To solve this problem, a distributed ledger technology, such as Blockchain, is adopted. Numerous works have been conducted to prove the usability of Blockchain and to create Blockchain-based Smart Cities. However, in recent years, the development of Quantum computers is noticeable. A Quantum computer is able to accelerate exponentially the speed of breaking classical encryption algorithms using a Quantum algorithm such as Shore's algorithm and Grover's algorithm. The algorithms associated with Blockchain, such as SHA-1, SHA-2, SHA-256 and Elliptic Curve based schemes such as ECDSA and BLS are vulnerable against a Quantum attack. For a Smart City's level, any sort of attack or security threats is critical as it can modify, manipulate or monitor user's sensitive data. Thus, this work believes that securing Blockchain against the Quantum attack's threat is crucial and fundamental step before creating the Blockchain-based Smart Cities. Diverse methods have been deployed to create the Post-Quantum Blockchain including lattice-based cryptography to generate a Blockchain signature prone against Quantum attacks, Quantum key distribution to handle secure key management in Blockchain-Smart City's heterogeneous environment and Quantum Blockchain-based Smart Cities to insure and guaranty the integrity and confidentiality of Smart Cities.

Securing Blockchain against Quantum attacks is a cornerstone, future works should focus more on the potential of Quantum attacks against Blockchain and create a Post-Quantum Blockchain based-application to avoid any future risk.

5.2 Open Research Challenges

Although Quantum computing is considered as a promising technology with an exponential speed of computing and performing a complex calculation, there are still various challenges to move from pre-Quantum to Post-Quantum Blockchain.

Quantum states are considerate fragile and the bits have to operate in a very low temperature's environment, which makes it expensive to manufacture and test. Moreover, Quantum computers still face high error rates and are architecturally complicated [24]. Figure 4 summarize some of the challenges that may slow down the development of Quantum computers and the transmission from pre-Quantum to post-Quantum Blockchain-based Smart City.

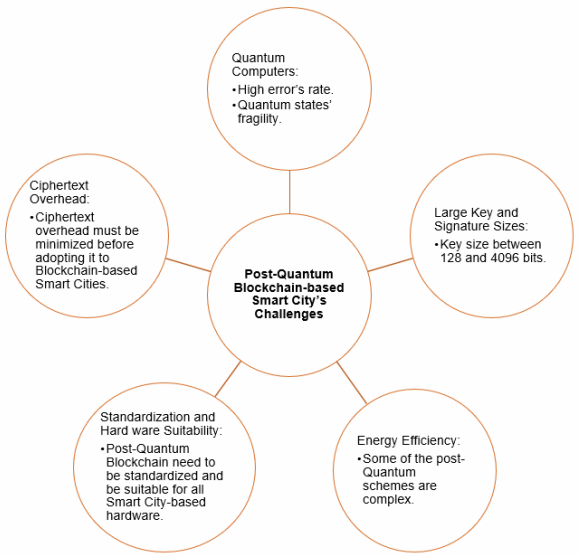

Figure 4. Post-Quantum Blockchain-based Smart-City's challenges

Nevertheless, the risk of a Quantum attack still critical and need to mitigate before the area of Quantum computers rises.

6 Conclusion

Quantum computers and Quantum-based cryptography conceive a sharp risk on classical encryption and security protocols including Blockchain. Blockchain-based Smart Cities are a critical application that needs to be secured against future Quantum attacks, as it holds sensitive information and data about users and their different components. In this paper, we present a general overview to understand the potential future risks of Blockchain-based Smart Cities. We discussed as well the classical Blockchain-based Smart Cities framework and presents some of the effective promising Post-Quantum solutions such as lattice-based cryptography, Quantum key distribution, and entanglement in time-base Quantum Blockchain. Those solutions are experimentally prone against Quantum attacks and are auspicious to be deployed to create a Post-Quantum Blockchain-based Smart City before the propitious advancement of Quantum computers occurs.

Acknowledgments

This study was supported by the Research Program funded by the SeoulTech (Seoul National University of Science and Technology).

References

[1] D. S. Abrams, S. Lloyd, Simulation of Many-body Fermi Systems on a Universal Quantum Computer, *Physical Review Letters*, Vol. 79, No. 13, 2586, September, 1997.

[2] Y. I. Manin, *Computable and Noncomputable*, Sovetskoye Radio, 1980.

[3] M. Hirvensalo, *Quantum Computing*, Springer-Verlag Berlin Heidelberg, 2013.

[4] R. P. Feynman, Simulating Physics with Computers, *International Journal of Theoretical Physics*, Vol. 21, No. 6-7, pp. 467-488, June, 1982. http://doi.org/10.1007/BF02650179

[5] S. K. Singh, S. Rathore, J. H. Park, BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence, *Future Generation Computer Systems*, Vol. 110, pp. 721-743, September, 2020. http://doi.org/10.1016/j. future.2019.09.002

[6] J. H. Witte, The Blockchain: A Gentle Four Page Introduction, ArXiv: 1612.06244, December, 2016.

[7] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM Journal on Computing*, Vol. 26, No. 5, pp. 1484-1509, October, 1997.

[8] B. Rodenburg, S. P. Pappas, *Blockchain and Quantum Computing*, MTR170487, June, 2017.

[9] E. Martín-López, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, J. L. O'Brien, Experimental Realization of Shor's Quantum Factoring Algorithm Using Qubit Recycling, *Nature Photonics*, Vol. 6, No. 11, pp. 773-776, November, 2012. http://doi.org/10.1038/nphoton.2012.259

[10] G. L. Long, Grover Algorithm with Zero Theoretical Failure Rate, *Physical Review A*, Vol. 64, No. 2, 022307, August, 2001.

[11] D. Micciancio, O. Regev, Lattice-based Cryptography, in: D. J. Bernstein, J. Buchmann, E. Dahmen (Eds.), *Post-Quantum Cryptography*, Springer, Berlin, Heidelberg, 2009, pp. 147-191.

[12] Y.-L. Gao, X.-B. Chen, Y.-L. Chen, Y. Sun, X.-X. Niu, Y.-X. Yang, A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain, *IEEE Access*, Vol. 6, pp. 27205-27213, April, 2018.

[13] M. Ajtai, Representing Hard Lattices with O(n log n) Bits, *Thirty-Seventh Annual ACM Symposium on Theory of Computing - STOC '05*, Baltimore, MD, USA, 2005, pp. 94-103. http:doi.org/10.1145/1060590.1060604

[14] W. A. A. Torres, R. Steinfeld, A. Sakzad, J. K. Lui, V. Kuchta, N. Bhattacharjee, M. H. Au, J. Cheng, Post-Quantum One-Time Linkable Ring Signature and Application to Ring Confidential Transactions in Blockchain (Lattice RingCT v1.0), *23rd Australasian Conference on Information Security and Privacy (ACISP* 2018), Wollongong, NSW, Australia, 2018, pp. 558-576.

[15] C. Li, X. Chen, Y. Chen, Y. Hou, J. Li, A New Lattice-Based Signature Scheme in Post-Quantum Blockchain Network, *IEEE Access*, Vol. 7, pp. 2026-2033, December, 2018.

[16] E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, A. S. Trushechkin, R. R. Yunusov, Y. V. Kurochkin, A. I. Lvovsky, A. K. Fedorov, Quantum-Secured Blockchain, *Quantum Science and Technology*, Vol. 3, No. 3, 035004, July, 2018.

[17] E. Diamanti, H. Lo, B. Qi, Z. Yuan, Practical Challenges in Quantum Key Distribution, *npj Quantum Information*, Vol. 2, No. 1, 16025, November, 2016.

[18] J. Wang, X. Gu, W. Liu, A. K. Sangaiah, H. J. Kim, An Empower Hamilton Loop Based Data Collection Algorithm with Mobile Agent for WSNs, *Human-centric Computing and Information Sciences*, Vol. 9, pp. 1-14, May, 2019.

[19] P. K. Sharma, S. Y. Moon, J. H. Park, Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City, *Journal of Information Processing Systems*, Vol. 13, No. 1, pp. 184-195, February, 2017.

[20] K. Biswas, V. Muthukkumarasamy, Securing Smart Cities Using Blockchain Technology, *14th IEEE International Conference on Smart City,* Sydney, NSW, 2016, pp. 1392-1393. http://doi.org/10.1109/HPCC-SmartCity-DSS.2016.0198

[21] A. Einstein, B. Podolsky, N. Rosen, Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?, *Physical Review*, Vol. 47, No. 10, 777, May, 1935.

[22] M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, UK, 2010.

[23] D. Rajan, M. Visser, Quantum Blockchain Using Entanglement in Time, *Quantum Reports*, Vol. 1, No. 1, pp. 3-11, September, 2019.

[24] D. Franklin, F. T. Chong, Challenges in Reliable Quantum Computing, in: S. K. Shukla, R. I. Bahar (Eds.), *Nano, Quantum and Molecular Computing*, Springer, Boston, MA, 2004, pp. 247-266.

[25] S. K. Singh, Y. S. Jeong, J. H. Park, A Deep Learning-based IoT-oriented Infrastructure for Secure Smart City, *Sustainable Cities and Society*, Vol. 60, 102252, September, 2020.

[26] J. Park, M. M. Salim, J. H. Jo, J. C. S. Sicato, S. Rathore, J. H. Park, CIoT-Net: A Scalable Cognitive IoT Based Smart City Network Architecture, *Human-Centric Computing and Information Sciences*, Vol. 9, 29, August, 2019. http://doi.org/10.1186/s13673-019-0190-9

[27] Y. Lee, S. Rathore, J. H. Park, J. H. Park, A Blockchain-based Smart Home Gateway Architecture for Preventing Data Forgery, *Human-Centric Computing and Information Sciences*, Vol. 10, 9, March, 2020. http://doi.org/10.1186/s13673-020-0214-5

[28] T. M. Fernández-Caramès, P. Fraga-Lamas, Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks, *IEEE Access*, Vol. 8, pp. 21091-21116, January, 2020. http://doi.org/10.1109/ACCESS.2020.2968985.

[29] D. J. Bernstein, J. Buchman, E. Dahmen, *Post-Quantum Cryptography*, Springer-Verlag, 2009.

[30] M. Liu, L. Cheng, M. Qian, J. Wang, J. Wang, Y. Liu, Indoor Acoustic Localization: A Survey, *Human-centric Computing and Information Sciences*, Vol. 10, 2, January, 2020. https://doi.org/10.1186/s13673-019-0207-4

[31] J. Zhang, S. Zhong, T. Wang, H. C. Chao, J. Wang, Blockchain-based Systems and Applications: A Survey, *Journal of Internet Technology*, Vol. 21, No. 1, pp. 1-14, January, 2020.

[32] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid, M. Guizani, Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City, *IEEE Access*, Vol. 7, pp. 18611-18621, January, 2019.

[33] L. K. Grover, A fast Quantum Mechanical Algorithm for Database Search, *28th Annual ACM Symposium on the Theory of Computing*, Philadelphia, Pennsylvania, USA, 1996, pp. 212-219.

Biographies

Abir EL Azzaoui is a master student in the department of Computer Science and Engineering, Seoul National University of Science and Technology, Korea.

James J. (Jong Hyuk) Park is a professor at the Department of Computer Science and Engineering, Seoul National University of Science and Technology, Korea.