Volume: 5, Issue: 3
Page: 116-125
2021

International Journal of
Science and Business
Journal homepage: ijsab.com/ijsb

IJSAB International

Resistant Blockchain Cryptography to Quantum Computing Attacks

Zhwan Mohammed Khalid & Shavan Askar

Abstract:

Due to the need to maintain confidentiality, redundancy, and openness, the usage of Blockchain and other DLTs has dramatically advanced in recent years, and is being recommended for various applications. In blockchain, these capabilities are supplied by means of hash functions and public-key encryption. However, the rapid development of quantum computation in the near future has opened the door to the Grover and Shor algorithms. These algorithms challenge both public and hash encryption, causing blockchains to redesign and use quantum attack-tolerant cryptosystems; this produces cryptosystems which are considered post-quantum cryptosystems, which are quantum-resistant. This paper reviews current scientists on quantum blockchain for such purposes. In addition, the major challenges are studied with the most important post-quantum blockchain systems. In addition, the most promising post quantum signature encryption and digital blockchain signature schemes are detailed in terms of the functionality and durability of the most promising public signatures. In this article, researchers and developers in blockchain have an extensive perspective and practical advice on post-quantum blockchain protection.

IJSB
Literature review
Accepted 1 February 2021
Published 3 February 2021
DOI: 10.5281/zenodo.4497732

Keywords: *Blockchain, cryptography, post-quantum, quantum-resistant, quantum computing, blockchain security*

About Author (s)

Zhwan Mohammed Khalid, Raparin University, Sulaimany, Iraq.
Email:eng.zhwan90@uor.edu.krd.
Shavan Askar (Corresponding Author), Assistant Professor, Erbil Polytechnic University, Erbil, Iraq. Email shavan.askar@epu.edu.iq.

1. Introduction

Blockchain is planned for cryptocurrency support, such as bitcoin, but a blockchain can be accessed. It is worth noting that Bitcoin is generally recognized as a bank and Wall Street market, but its real meaning still needs to be grasped and has no definitive future (Dasgupta, Shrein, & Gupta, 2019). The blockchain consists of a series of blocks between publicly available nodes that are stored on and copied. Every block is made up of four basic elements: a) the hash of the block before it. b) The data content of the chain (i.e. the database entries, c) nonce required to provide the basic form to the hash. d) the hash of the block (Rodenburg & Pappas, 2017). Public-key cryptographic is being used by Blockchain to provide security and anonymity. There are currently two major public key cipher suites for Transport Layer Authentication (TLS): the cipher sequences based on the Rivest and Shamir Adleman (RSA) and the main algorithm for exchange using RSA; the Elliptic Curve, Diffie-Hellman Exchanges (ECDHE). (Fraga-Lamas & Fernández-Caramés, 2019). The minimum information of cryptography of the elliptic curve, which is the underlying system, makes the whole system safe and necessary for the digitally signed algorithm. The reliability of the blockchain protocol relies entirely on the security of the elliptical curve cryptography (Ikeda, 2018; Sulaiman & Askar, 2015; Fares & Askar, 2016).

The theory of quantum algorithms has grown dramatically in 20 years since Shor's discovery. For several issues related to physics simulation, number theory, and topology, quantum algorithms reaching exponential speed were found. However, a relatively limited list of issues with the admission of exponential quantum machine acceleration exists. In comparison, a wide range of search, collision finding and Boolean formula measurement problems have been moderated by speed-ups. Grover's search algorithm offers a quadratic speedup on unstructured search queries, in particular. Although such a speedup does not make cryptographic technologies redundant, greater key sizes could be required for an analysis of the details. The impact of massive quantum processors on popular cryptographic algorithms for example, the RSA and the Advanced Encryption Standard (AES), see Table 1. It is not clear how far these quantum advantages can be progressed or how long the gap between feasibility exists in classical and quantum models (Chen et al., 2016). It is difficult and controversial to inquire whether a large-scale quantum computer can be designed. While in the past it was less clear that massive quantum computers are a physical reality, many physicians now believe that they are only a huge engineering problem. Any scientists still predict that strong quantum computers will be built to easily crack all the core public networks currently in operation in the next 20 years or so(Mosca, 2018). Our advanced public key cryptography infrastructure has taken nearly 20 years to deploy. It will require tremendous effort to ensure a smooth and stable migration to their quantum computing tolerant counterparts from the latest commonly used cryptosystems. Whether we can then forecast precisely the time of the advent of the quantum computing era, we must continue preparing our information security programs in order to avoid quantum computation.

This article is arranged as follows. Introduction in section 1, Section 2 quantum-resistant cryptography in this section discuss many important classes of cryptographic systems also in section 3, give a short description about Blockchain security primıtives (public-key security, Hash function) for which post-quantum primitives have been suggested in the section. Section 4, discuss about blockchain proposals post-quantum. Sections 5 discuss issues and studies future in blockchain, section 6 result and findings after study and review literature, section 7 concludes the paper.

Table 1 - Effect on Common Cryptographic Algorithms in Quantum Computing

Algorithms	Purpose	Type	Effects of massive quantum computers
SHA-2, SHA-3 (Dworkin, 2015; Semmouni, Nitaj, & Belkasmi, 2019)	Hash functions	----------	Larger production needed
AES(Mohsin et al., 2019)	Encryption	Symmetric key	Bigger key sizes expected
RSA (X. Zhou & Tang, 2011)	Signatures, key establishment	Public key	Do not safe any longer
ECDSA, ECDH (Elliptic Curve Cryptography) (Stewart et al., 2018)	Signatures, main change	Public key	Do not safe any longer
DSA (Finite Field Cryptography)(Jirwan, Singh, & Vijay, 2013)	Signatures, main change	Public key	Do not safe any longer

2. Quantum-Resistant Cryptography

The quest for algorithms considered to be resistant to both traditional and quantum computers attacks has also cantered on public key algorithms. I provide a brief summary in this chapter of the main families that were proposed for after quantum primitives in the next chapter. Other groups include lattices, codes and multivariate polynomials, which are essential to the crypto graphing systems beyond RSA, DSA and ECDSA, and several others, Based on prior literature. For more information see (Chunnilall, 2015; Rodenburg & Pappas, 2017) (Perlner & Cooper, 2009). (i)Encryption based on hash. The standard example is the Merkle hash tree system for public signatures, based on the Lamport and Diffie one-post theory. (ii) Cryptography based on code. McEliece's secret form of public key data encryption is the classic example. (iii) Cryptography based on lattice. The Hoffstein-Pipher-Silverman "NTRU" public-key-encryption scheme is the instance that has perhaps drawn the most interest, not the first instance historically. (iv) Cryptography of multivariate, quadratic equations. The Patarin secret field equations scheme (defined as minus variants) is one of the related examples of the Publicized Main signature. (v) Other — Different schemes were suggested that do not complement the above families. One is focused on the assessment of super singular, elliptical curves with isogenes. Even if Shor's algorithm succeeds in overcoming an elliptical curve discrete log problem on a quantum computer, there is not a problem in super singular curves with a similar quantum attack on isogeny. Like some other theories, such as the problem of conjugation and similar problems inside braid groups.(Chen et al., 2016).

Table 2 Performance descriptions of the processes referred to above

Approach	Advantages	Disadvantages
Code-based encryption cryptography;	Strong security confidence; Short chips. (Bernstein & Lange, 2017)	very fast major public keys
Lattice-based encryption	Short cipher texts and keys; very fast encryption	Require more security analysis
Lattice-based signatures analysis;	Short keys and signatures; fast side-channel attacks on discrete Gaussians	Require more security
Multivariate-quadratic- equation signatures	Signatures very short	Require more security analysis
Hash-based signatures	Clear description: confidence	Management of state
Hash-based signatures	Clear description: confidence	Large signatures

Both these schemes must be resisted by classical computers and quantum computers. None of these structures have been found to use the 'shor' algorithm,' a discrete quantum computer algorithm dividing RSA, DSA and ECDSA. These systems with other quantum algorithms, 'grover algorithms,' have many implementations, but the grover algorithm is no quicker than Shor and cryptographers can easily solve it by picking a slightly larger environment. Is it better attacked on these systems? Perhaps it is. This is a popular encryption of vulnerabilities. So, the party invests a great deal of time and power on crypt research. Crypt analysts often experience a catastrophic attack that reveals that a system is worthless for encryption; for instance, any useful selection of public-key cryptography parameters of Merkle–Hellman is quickly violated. Crypt scientists also do not find attacks as devastating, but they do drive large sizes.(Bernstein, 2009)

3. Blockchain security primıtives

Public/asymmetrical cryptography and hash functions ultimately help blockchain encryption, as is outlined in the next sections for blockchain security.

3.1 Blockchain public-key security

A blockchain uses publicly identified key cryptosystems by authenticating transactions through digitally identified signatures to ensure knowledge sharing between parties. The signatory signs with a private key during the signature process. To ensure that the signature is accurate, the public key is exchanged publicly. The algorithm is built only by the individual with a private key. It can be encrypted. Bitcoin uses ECDSA signatures to verify Koblitz signatures for the signing of messages on a private and public basis. Hash is also used to keep documents credible, i.e. to ensure that the evidence is improperly abused. The hash value also adjusts appropriately as the verified data changes. The integrity of data is therefore detectable, as the data is located in an unstable environment, Based on the data's hash value. The user must demonstrate that he has a private key to bitcoin spending. Each Bitcoin receiver uses the public key to ensure the obtained currency validates the digital signature. (Fernández-Caramès & Fraga-Lamas, 2020). In 2009, Perlner & Cooper (2009) Any of the public key cryptographic algorithms which have developed and are considered immune from quantum calculation-based attacks are given. The supposed quantic resistance of these algorithms is based on the absence of a quantum computation model of any known attacks or solutions to the related problems. This implies no threat, but offers some faith. An attack never can be identified. In the classical programming model, the same kind of logic is used to justify the protection of a few or a few primitive machines. They have also identified the issue for limited memory or bandwidth computers, if the keyboards are a lot greater than any thousand bits if public keys, key exchanges or signatures. Significantly more time can also be a challenge than basic cryptographic tasks.

3.2 Hash function

The hash algorithm consists of susceptibility, directionality, collision resistance, and high meaning, mapping a set of messages with a shorter fixed-length value, of any duration. (Xiaofei, 2017). Hash is often used to protect record credibility, i.e. to guarantee no information is manipulated inappropriately. As the checked data is changed, the hash value changes accordingly. Therefore, the integrity of the data should be appreciated when taking into account the fact that the data is incomplete. SHA is the cryptographic hash form function with general characteristics of the cryptographic hash function of the National Standard Institute and Technology (NIST) (Zhai et al., 2019). Blockchain can use hash functions to perform verification of blocks and transaction integrity. The hash value of past block information is stored in the header of a block of the blockchain. Each user compares the hash

value measured to the hash value stored. Trade observes the validity of the previous block. It can also be used to build open-ended key pairs with a Hash function. The Hash Pointer is a code structure with certain data information and password hash, in addition to the regular markers (Wang & Wu, 2017). A list of hash points, each linked with a hash value, is a blockchain, as seen in Figure 3. The hash value checks whether the block data have been changed to ensure that the block information is reliable (Zhai et al., 2019).

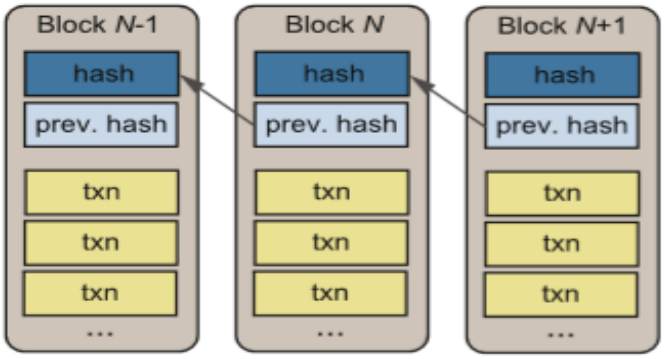

Figure 3. Blockchain structure.

4. Blockchain proposals post-quantum

Several academics suggested blockchains for post-quantum or improvements to existing blockchains to counter the quantum danger (Baldi, Santini, & Cancellieri, 2017; Clupek, Malina, & Zeman, 2015) Descriptions were also, Preece & Easton (2018) proposed architecture accessible networks to exchange critical industrial data. This code will work with the IPFS and Ethereum and implements the SIDH Key Exchanged Diffie-Hellman. Also in modified Ethereum (Shen, Xiang, Zhang, Cai, & Xiang, 2019) But with Rainbow multivariate cryptosystem, the output of which is contrasted with the present Ethereum edition of the quoted article (based on ECDSA). In the situation that the (Semmouni et al., 2019) The authors suggest that Bitcoin (using Koblitz secp256k1 and SHA-256 during the signing step of ECDSA be improved). Where BLAKE2 is used (Aumasson, Neves, Wilcox-O'Hearn, & Winnerlein, 2013) and SHA-3 (Dworkin, 2015) The work still deserves mention(S. Gao, Zheng, Guo, Jing, & Hu, 2019) It uses Niederreiter's coded-basis cryptosystem to test the computer against quantum attacks to implement a transparent e-voting protocol based on the blockchain. İn 2018, Geo et al.(Y.-L. Gao et al., 2018) Present the (PQB) concept and suggest a stable PQB-based cryptocurrency scheme that can with stand quantum computing assaults. First, a lattice issue-based signature scheme was proposed. The lattice base delegation algorithm was used to generate hidden keys using a random value selection. Second, By integrating a proposed blockchain signature scheme, the proposed cryptocurrency scheme will help escape a quantum computing assault, The signature scale and hidden keys are comparatively shorter as that of some, as compared to prior signature systems, thus minimizing the computer complexity. Our cryptocurrency system is safer and more efficient.
In 2018, Chao et al. (Li, Chen, Chen, Hou, & Li, 2018) Presented Vulnerabilities of existing blockchain networks against a quantum competitor and simple future methods for postquantum mitigation. Then a new grid-based scheme to protect the blockchain network using traditional conventional grids is suggested. Meanwhile, public and private keys consist of the root keys of Bonsa Trees, which not only preserve randomness but also create light weight non-definite wallets, using the Rand Base algorithm. The suggested scheme can be considered protected in the random oracle model. This analysis would also contribute to

better studies of the future quantum blockchain (PQB). In 2018, Stewart at el. (Stewart et al., 2018) It is proposed that Bitcoin may be challenged to sign contracts, currently using ECDSA It has proposed a simple but slow commit delay protocol that allows users to safely move their money from old products to those in a quantum digital signature structure (not resistant to the amount). The optimal waiting time for future discussion and review can also be extended. Also In 2019, Campbell and Robert (Campbell Sr, 2019) Assesses cyber security risk with a wide variety of usage in the operation of (ECDSA) cryptograph algorithms, such as Bitcoin Heart, Ethereum, Bitcoin Money and corporate packages like Mega-Link, Hyper-Ledger, Fabric and Sawtooth Pool. The second aim is to measure ECDSA against quantity risk and explain the most practical national risk. Cryptographic counter structures that can be used for the short term and form the basis of the establishment of structured, open-ended, industrially-wide barrels Post-quantum algorithms based on Institute of Standards and Technology Lattices (NIST)

5. Key subject issues and studies future in blockchain post-quantum

5.1 Quick evolution computing

Quantum computing is a hot subject now attracting great interest from academics and business. More attacks on post-quantum cryptosystems are likely to evolve, so researchers need to pay attention to the quantity and its development.

5.2 Transition from pre-quantum to blockchain post-quantum

Involves careful studies for these purposes, many researchers have developed techniques. In (Sato & Matsuo, 2017) The authors suggest a way of extending the authenticity of previous blockchain blocks in terms of the protection of hash or digital signatures. to prevent this(F. Chen, Liu, Long, Liu, & Ding, 2018). There will be another process (Stewart et al., 2018) where the common-delay-revealing protocol helps blockchain users to safely move money from pre-quantum Bitcoin into a version incorporating the post-quantum digital signature method.

5.3 signature sizes and big keys

Generally speaking, quantitative crypto schemes need significantly greater sizes than existing public key encryption systems (between 128 and 4,096 bits). Structures such as those focused on super singular isogenes are promising for signature in terms of their size, but generate broad signatures. In-depth scheme (Yoo et al, 2017) For 128-bit quantum authentication, the 2688-bit public keys and 384-bit private keys are used but the signature level is 120 KB, a difficulty for similar systems capable of containing a large amount of such signatures. Hash schemes are also relatively limited in scale but also have more than 40 KB of signature (Gheorghiu et al., 2017). In comparison, a few multivariate-based signatures are possible, but many kilo bytes will take up keys used to produce and validate these signatures. Regarding grid based systems; there are DILITHIUM variants that are very fast but with around 1.500 bytes in key size and 2,701 bytes in signature length. Regarding the public key solutions after quanta encryption, some simpler versions such as Round5 are good enough to preserve the size of the most recent node hardware, since their performance is good enough to keep them (2,736 bits for the public key and only128 bits for the private key). Nevertheless, further study is also required in postquantum systems to ensure that key sizes and protection for blockchains are well matched.

5.4 Unsuitability blockchain hardware

Any post quantum cryptosystems are computationally heavy and may not be appropriate for any devices used to deploy blockchain nodes currently. Post-quantum systems can then allow a distinction between security and device sophistication such that future hardware which can communicate with the blockchain cannot be diminished.

5.5 Reflects the contribution cipher text

Some cryptosystems create high overheads that can influence a blockchain's efficiency. In order to fix this, prospective developers after quantity would need to circumvent cipher text and consider potential compression strategies.

5.6 Competence and Performance of Energy

Any post-quantum schemes take substantial time to implement, store and computing resources. Such criteria also contribute to increased energy usage. In order to improve computing, energy performance, and ultimately, efficiency of the blockchain, potential engineers would have to search at innovative ways to optimize cryptosystem.

5.7 Slow key generation

Any post quantitative schemes restrict the number of messages signed to boost stability. As a result, new keys must be generated on a continuous basis which implies slowing down some blockchain processes by using computer-related resources. Blockchain developers would then need to decide if these key generation processes can be modified to boost blockchain performance.

5.8 Quantum blockchain

Almost every researchers suggested quantum-based blockchains in addition to using cryptosystems for transformation from pre-quantum to post-quantum blockchain(Ikeda, 2018; Sun et al., 2019). For instance, In (Ikeda, 2018a; Jogenfors, 2019) Bitcoin migration to quantum computers was advocated by the authors; Others addressed how mining can be enhanced by modifying the Grover algorithm (Jogenfors, 2019) In addition, some scholars proposed the deployment of smart contracts(Coladangelo, 2019) using quantum cryptography. In addition, more research on key methods focused on physics institutions collectively known as quantum key distribution is required (QKD)(Alléaume, 2018).

6. Result and Findings

The following findings after the comprehensive literature review done in this article: No other analysis which the following main inputs were included together.

6.1 A detailed analysis of the effects of quantum attacks on public dangerous structures in a blockchain. An analysis of the most important projects and standardization efforts in the post-quantum blockchain. At present, there are no smaller key size post-quantum blockchain algorithms, shorter signature/hash sizes, high performance, fast rollout and low cost simultaneously. For resource-constrained embedded devices such as those found in the Internet of Things, such variables are extremely crucial (Askar, 2017; Fizi & Askar, 2016; Askar, 2016; Keti & Askar, 2015).

6.2 It is important to research how blockchain security can be strengthened by incorporating such features that were seldom seen in non-academic blockchain upgrades and validating their post-quantum safety. The most important qualities are:

Signatures Combine. They allow a unique signature to be produced from many of them. For blockchain, this principle is appealing because it requires quicker authentication and reduces capacity and bandwidth(Zhao, 2018).

Homomorphic enciphering. It helps the processing of a transaction by third-party providers without exposing unencrypted data to them(Hayouni & Hamdi, 2016). To improve the Bitcoin protocol(França, 2015) and for blockchain-based IoT applications(L. Zhou, Wang, Sun, & Lv, 2018; Askar et al., 2011; Al Majeed et al., 2014), this form of encryption has already been suggested.

7. Conclusion

The recent advancements in quantum computing were carried out by researchers and developers working with DLTs such as the block chain which focuses mainly on public key encryption and hash functions. The article examines how quantum cryptosystems, based on

Grover and Sher algorithms, can be used to address such challenges. The main post-quantum systems were updated and their application and key problems analyse. Accessibility and efficiency were contrasted with the most promising public key encryption and digital systems after quantity. This study therefore offers a broad perspective and guidance for researchers and developers on the quantum danger blockchain and the next quantum-resistant blockchain wave.

References

Al Majeed, S., Askar, S., Fleury, M. (2014). H.265 Codec over 4G Networks for Telemedicine System Application. UKSim-AMSS 16th International Conference on Computer Modelling and Simulation (UK), Cambridge (pp. 292-297), doi: 10.1109/UKSim.2014.59.

Alléaume, R. (2018). Implementation Security of Quantum Cryptography: Introduction, challenges, solutions. ETSI White Paper, 27, 28.

Askar S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Evaluation of Classified Cloning Scheme with self-similar traffic. 3rd Computer Science and Electronic Engineering Conference (CEEC), Colchester, 2011, pp. 23-28, doi: 10.1109/CEEC.2011.5995819.

Askar, S. (2016). Adaptive Load Balancing Scheme For Data Center Networks Using Software Defined Network. Journal of University of Zakho, Vol. 4(A), No.2, Pp 275-286,

Askar, S. (2017). SDN-Based Load Balancing Scheme for Fat-Tree Data Center Networks. Al-Nahrain Journal for Engineering Sciences (NJES), Vol.20, No.5, pp.1047-1056

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Service differentiation for video applications over OBS networks. 1*6th European Conference on Networks and Optical Communications*, Newcastle-Upon-Tyne, pp. 200-203.

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). A novel ingress node design for video streaming over optical burst switching networks. Optics Express, Vol. 19 (26), pp. 191-194

Askar, S., Zervas, G., Hunter, D. K., & Simeonidou, D. (2011). Adaptive Classified Cloning and Aggregation Technique for Delay and Loss sensitive Applications in OBS Networks. in Optical Fiber Communication Conference/National Fiber Optic Engineers Conference 2011, OSA Technical Digest (CD) (Optical Society of America, 2011), paper OThR4.

Aumasson, J.-P., Neves, S., Wilcox-O'Hearn, Z., & Winnerlein, C. (2013). BLAKE2: simpler, smaller, fast as MD5. Paper presented at the International Conference on Applied Cryptography and Network Security.

Baldi, M., Santini, P., & Cancellieri, G. (2017). Post-quantum cryptography based on codes: State of the art and open challenges. Paper presented at the 2017 AEIT International Annual Conference.

Bernstein, D. J. (2009). Introduction to post-quantum cryptography Post-quantum cryptography (pp. 1-14): Springer.

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188-194.

Campbell Sr, R. (2019). Evaluation of post-quantum distributed ledger cryptography. The Journal of The British Blockchain Association, 2(1), 7679.

Chen, F., Liu, Z., Long, Y., Liu, Z., & Ding, N. (2018). Secure scheme against compromised hash in proof-of-work blockchain. Paper presented at the International Conference on Network and System Security.

Chen, L., Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., . . . Smith-Tone, D. (2016). Report on post-quantum cryptography (Vol. 12): US Department of Commerce, National Institute of Standards and Technology.

Chunnilall, C. J. (2015). Metrology for quantum communications. Paper presented at the 2015 Conference on Lasers and Electro-Optics (CLEO).

Clupek, V., Malina, L., & Zeman, V. (2015). Secure digital archiving in post-quantum era. Paper presented at the 2015 38th International Conference on Telecommunications and Signal Processing (TSP).

Coladangelo, A. (2019). Smart contracts meet quantum cryptography. arXiv preprint arXiv:1902.05214.

Dasgupta, D., Shrein, J. M., & Gupta, K. D. (2019). A survey of blockchain from security perspective. Journal of Banking and Financial Technology, 3(1), 1-17.

Dworkin, M. J. (2015). SHA-3 standard: Permutation-based hash and extendable-output functions.

Fares, N., Askar, S. (2016). A Novel Semi-Symmetric Encryption Algorithm for Internet Applications. Journal of University of Duhok, Vol. 19, No. 1, pp. 1-9

Fernández-Caramès, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access, 8, 21091-21116.

Fizi, F., & Askar, S. (2016). A novel load balancing algorithm for software defined network based datacenters, International Conference on Broadband Communications for Next Generation Networks and Multimedia Applications (CoBCom), Graz, 2016, pp. 1-6, doi: 10.1109/COBCOM.2016.7593506.

Fraga-Lamas, P., & Fernández-Caramés, T. M. (2019). A review on blockchain technologies for an advanced and cyber-resilient automotive industry. IEEE Access, 7, 17578-17598.

França, B. (2015). Homomorphic mini-blockchain scheme: Apr.

Gao, S., Zheng, D., Guo, R., Jing, C., & Hu, C. (2019). An anti-quantum E-voting protocol in blockchain with audit function. IEEE Access, 7, 115304-115316.

Gao, Y.-L., Chen, X.-B., Chen, Y.-L., Sun, Y., Niu, X.-X., & Yang, Y.-X. (2018). A secure cryptocurrency scheme based on post-quantum blockchain. IEEE Access, 6, 27205-27213.

Gheorghiu, V., Gorbunov, S., Mosca, M., & Munson, B. (2017). Quantum-proofing the blockchain. Blockchain Research Institute (BRI), Toronto, ON, Canada.

Hayouni, H., & Hamdi, M. (2016). Secure data aggregation with homomorphic primitives in wireless sensor networks: A critical survey and open research issues. Paper presented at the 2016 IEEE 13th International Conference on Networking, Sensing, and Control (ICNSC).

Ikeda, K. (2018a). qBitcoin: a peer-to-peer quantum cash system. Paper presented at the Science and Information Conference.

Ikeda, K. (2018b). Security and privacy of blockchain and quantum computation Advances in Computers (Vol. 111, pp. 199-228): Elsevier.

Jirwan, N., Singh, A., & Vijay, D. S. (2013). Review and analysis of cryptography techniques. International Journal of Scientific & Engineering Research, 4(3), 1-6.

Jogenfors, J. (2019). Quantum Bitcoin: An Anonymous, Distributed, and Secure Currency Secured by the No-Cloning Theorem of Quantum Mechanics. Paper presented at the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).

Keti, F., Askar, S. (2015). Emulation of Software Defined Networks Using Mininet in Different Simulation Environments. *6th International Conference on Intelligent Systems, Modelling and Simulation*, Kuala Lumpur, 2015, pp. 205-210, doi: 10.1109/ISMS.2015.46.

Li, C.-Y., Chen, X.-B., Chen, Y.-L., Hou, Y.-Y., & Li, J. (2018). A new lattice-based signature scheme in post-quantum blockchain network. IEEE Access, 7, 2026-2033.

Mohsin, A., Zaidan, A., Zaidan, B., Albahri, O., Albahri, A., Alsalem, M., & Mohammed, K. (2019). Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication. Computer Standards & Interfaces, 66, 103343.

Mosca, M. (2018). Cybersecurity in an era with quantum computers: will we be ready? IEEE Security & Privacy, 16(5), 38-41.

Perlner, R. A., & Cooper, D. A. (2009). Quantum resistant public key cryptography: a survey. Paper presented at the Proceedings of the 8th Symposium on Identity and Trust on the Internet.

Preece, J., & Easton, J. (2018). Towards encrypting industrial data on public distributed networks. Paper presented at the 2018 IEEE International Conference on Big Data (Big Data).

Rodenburg, B., & Pappas, S. P. (2017). Blockchain and quantum computing. Retrieved from.

Sato, M., & Matsuo, S. i. (2017). Long-term public blockchain: Resilience against compromise of underlying cryptography. Paper presented at the 2017 26th International Conference on Computer Communication and Networks (ICCCN).

Semmouni, M. C., Nitaj, A., & Belkasmi, M. (2019). Bitcoin security with post quantum cryptography. Paper presented at the International Conference on Networked Systems.

Shen, R., Xiang, H., Zhang, X., Cai, B., & Xiang, T. (2019). Application and Implementation of Multivariate Public Key Cryptosystem in Blockchain (Short Paper). Paper presented at the International Conference on Collaborative Computing: Networking, Applications and Worksharing.

Stewart, I., Ilie, D., Zamyatin, A., Werner, S., Torshizi, M., & Knottenbelt, W. J. (2018). Committing to quantum resistance: A slow defence for Bitcoin against a fast quantum computing attack. Royal Society open science, 5(6), 180410.

Sulaiman, S., Askar, S. (2015). Invetigation of the Impact of DDoS Attack on Network Efficiency of the University of Zakho. Journal University of Zakho, Vol. 3(A) , No.2, Pp 275-280.

Sun, X., Sopek, M., Wang, Q., & Kulicki, P. (2019). Towards quantum-secured permissioned blockchain: Signature, consensus, and logic. Entropy, 21(9), 887.

Wang, H., & Wu, T. (2017). Cryptography on the Blockchain [J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 6, 61-67.

Xiaofei, L. (2017). Research on blockchain performance improvement of Byzantine fault-tolerant consensus algorithm based on dynamic authorization [D]. Zhejiang University.

Yoo, Y., Azarderakhsh, R., Jalali, A., Jao, D., & Soukharev, V. (2017). A post-quantum digital signature scheme based on supersingular isogenies. Paper presented at the International Conference on Financial Cryptography and Data Security.

Zhai, S., Yang, Y., Li, J., Qiu, C., & Zhao, J. (2019). Research on the Application of Cryptography on the Blockchain. Paper presented at the J. Phys. Conf. Ser.

Zhao, Y. (2018). Aggregation of Gamma-Signatures and Applications to Bitcoin. IACR Cryptol. ePrint Arch., 2018, 414.

Zhou, L., Wang, L., Sun, Y., & Lv, P. (2018). Beekeeper: A blockchain-based iot system with secure storage and homomorphic computation. IEEE Access, 6, 43472-43488.

Zhou, X., & Tang, X. (2011). Research and implementation of RSA algorithm for encryption and decryption. Paper presented at the Proceedings of 2011 6th international forum on strategic technology.

Cite this article:

Zhwan Mohammed Khalid & Shavan Askar (2021). Resistant Blockchain Cryptography to Quantum Computing Attacks. *International Journal of Science and Business, 5*(3), 116-125. doi: https://doi.org/10.5281/zenodo.4497732

Retrieved from http://ijsab.com/wp-content/uploads/691.pdf

Published by

IJSAB International