QUANTUM SUPREMACY AND ITS IMPLICATIONS FOR BLOCKCHAIN REGULATION AND LEGISLATION

Islombek Abdikhakimov
Cyber Law Department of Tashkent State University of Law
islombekabduhakimov@gmail.com

ABSTRACT

Recent advances demonstrating quantum supremacy pose potential threats to the cryptographic integrity underpinning blockchain technology. As quantum computers progress towards realizing cryptographic breaks, blockchain networks face risks of compromise. This indicates an urgent need to upgrade cryptographic schemes securing blockchain ledgers and smart contracts. Understanding the nature and timeline of quantum threats will be critical for blockchain governance and protocols to properly prepare defenses. Additionally, the advent of quantum attacks requires reassessing legal frameworks and policies governing blockchain infrastructure. Regulations must address quantum risks, provide guidance to blockchain networks, stimulate research, and enhance consumer protections in a post-quantum era. By analyzing technical dimensions around quantum and blockchain while exploring policy implications, recommendations emerge for blockchain regulation and legislation for the coming quantum computing age.

Keywords: *Quantum computing, Blockchain, Cryptography, Quantum supremacy, Post-quantum cryptography, Blockchain regulation*

INTRODUCTION

The concept of quantum supremacy reflects the potential for quantum devices to surpass the capabilities of classical supercomputers at certain tasks [1]. Recent empirical demonstrations of quantum supremacy by firms such as Google highlight rapid practical progress in quantum information processing [2]. As quantum computing matures, one major application includes breaking the public-key cryptography underlying most current blockchain implementations [3]. This poses serious integrity and security risks to blockchain networks and related legal frameworks. Examining technical dimensions around quantum computing alongside governance and policy considerations provides insights into upgrading blockchain defenses and pertinent regulatory issues. This analysis intends to assess quantum threats to blockchain while exploring implications for regulation and computer security legislation across the emerging quantum risk landscape.

Background

Blockchain technology utilizes distributed ledger architectures, consensus mechanisms, and cryptographic techniques to enable decentralized, transparent networks with inherent integrity [4]. Various public-key schemes secure blockchain ledgers, assets, and communications, including elliptic curve digital signature algorithm (ECDSA) and secure hash algorithm 2 (SHA-2) [5]. However, Grover's and Shor's quantum algorithms allow quantum computers to conduct brute force attacks against elliptic curve cryptography, SHA-2, and other associated schemes [6]. As quantum computers scale up sufficiently over the next decade, they could compromise blockchain cryptographic integrity.

Quantum Threat Analysis

The potential quantum risk landscape includes multiple attack vectors against blockchain cryptography as quantum algorithms run on larger qubit machines over time. Applicable risk scenarios incorporate hybrid attacks combining quantum and classical techniques alongside pure quantum cryptanalysis [7]. This section analyzes various technical threats metastasizing in the quantum vector against blockchain systems. All major public-key algorithms rely on difficulty of certain mathematical problems regarding prime factoring or discrete logarithms [8]. Quantum algorithms specially crafted to solve such problems efficiently thus endanger the entire public-key infrastructure. Once adequately scaled, quantum computers can retroactively break previous blockchain transactions protected only by vulnerable cryptography [9].

Empirical demonstrations show controllable quantum computers currently operating at the 65 qubit level while calculations estimate the timeline for breaking popular 256-bit schemes ranges between 2030 to 2040 [10]. However, substantially less qubits are necessary to endanger weaker cryptosystems such as stranding assets in Bitcoin addresses using fragile 160-bit keys [11]. Combined classical and quantum techniques allow adversaries to harvest encrypted data now for retrospective decryption later on scaled-up quantum machines. Public keys previously considered secure become compromised [12]. Without additional defenses, entire blockchain histories face potential unraveling by adversaries capturing transactions secured by fragile cryptography. Programmable ledger functionality through smart contracts relies on the same public-key infrastructure. Researchers already propose methods enabling quantum algorithms to manipulate smart contract execution for malicious extensions, deletions, and other exploits [13]. Quantum breaks of signatures, keys, and hashes could allow adversaries to reliably commit various types of fraud – moving assets not belonging to them, double-spends across forked chains, balance falsifications, and other integrity failures [14].

Governance and Upgrade Planning

As quantified by robust threat analysis, blockchain systems require coordinated governance to plan iterative upgrades preventing quantum breaks through an agile migration process to post-quantum cryptography. However, this governance transition faces issues around coordination complexity, upgrade timing, and algorithm analysis. Quantum-resistant upgrades require modifying consensus rules, necessitating hard forks clearly disjoint from previous ledgers creating additional privacy risks [15]. Strategies based on soft forks maintaining backwards compatibility slow adaptation down with only partial node adoption. Hybrid models attempt balancing between sufficient quantum protections and maximizing user base continuity. Disparate node upgrade participation rates may temporarily dilate consensus producing network forks during cryptographic transitions. This risks ledger state divergence resulting in reconciliation problems around quantum-forked chains [16].

Iteratively swapping cryptographic schemes proving vulnerable requires built-in modularity and agility within blockchain protocols known as crypto-agility [17]. Governance guidelines must assess optimal mechanisms for testing and integrating post-quantum algorithms based on external audits and published research.

Legal and Regulatory Considerations

Currently sparse governance around blockchain primarily focuses on immediate issues like cryptocurrency crime and tokens as asset classes rather than technical computing risks [18]. However, the advent of progressed quantum computers expands legal issues around blockchain infrastructure. The multinational nature of distributed blockchain networks coupled with uncertainties around exact quantum risk timelines creates complex jurisdictional questions regarding appropriate policy updating, enforcement, and international law harmonization. As blockchain cryptography and assets fall prey to quantum attacks, questions emerge around attributable fraud liability and consumer protections given the pseudo-anonymous nature common to most blockchain ecosystem participants [19]. Quantum threats exist on a rapidly shortening timeline lagging behind sufficiently nimble regulatory guidance for blockchain networks. This risks government guidelines perpetually remaining behind the curve of quantum risks.

Recommendations

Technical evaluation of prospective quantum threats alongside policy dimensions point towards recommendations in codifying blockchain regulation for the quantum age. Suggestions include specifying quantum-specific protections, delineating distributed liability, providing legal clarity, and identifying international harmonization pathways. Regulations should define “quantum-resistant cryptography” with minimum thresholds against different quantitative attack models – pure brute force, hybrid, etc. This allows standardized assessment while stimulating ongoing cryptographic research. Require hard forks enacting quantum-resistant cryptography once external audits demonstrate vulnerabilities in existing ledger schemes surpassing pre-defined risk thresholds. Provide optional guidance and liability clarification for temporary soft fork usage enabling hybrid cryptographic environments during network upgrades towards required hard forks. Standardize mechanisms and procedures for iterative cryptographic transitions based on external quantum threat assessments. Foster built-in blockchain ledger agility through emphasis on modularity and pluggable designs. Spread liability across protocol developers, node operators, hardware manufacturers, and foundations during attribution of compromises enabled by quantum attacks depending on demonstrated negligence per coded governance standards.

Enable policy knowledge transfer and best practice sharing around blockchain technology regulations across international jurisdictions to pre-empt fragmented or contradictory quantum readiness strategies. Incorporate latest cryptosecurity research insight into continually updated recommendations around blockchain technology policy in a responsively adaptive manner as external quantum assessments shift.

CONCLUSION

Emerging quantum computers capable of breaking the public-key cryptographic infrastructure supporting blockchain networks pose serious technical threats to integrity, stability, and reliability. These risks require updated governance procedures and policies guiding legislative treatment of blockchain technology for sufficient quantum readiness. By delineating recommendations around hard fork needs, distributed liability, crypto-agility principles, and global regulatory coordination pathways, governments can undertake efforts safeguarding consumers and infrastructure for an impending quantum future. As quantum computers accelerate alongside blockchain adoption, policymakers must prioritize addressing the potential for catastrophic quantum risk scenarios.

REFERENCES

1. Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2019). Quantum attacks on Bitcoin and how to protect against them. Ledger, 4, 1-21. https://doi.org/10.5195/ledger.2019.140

2. Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., Boixo, S., Broughton, M., Buckley, B. B., Buell, D. A., Burkett, B., Chen, Y., Chen, Z.,

Chiaro, B., Collins, R., Courtney, W., Dunsworth, A., Farhi, E., Fowler, A. G., Foxen, B., Giustina, M., Graff, R., Guerin, K., Habegger, S., Harrigan, M. P., Hartmann, M. J., Ho, A., Hoffmann, M., Huang, T.... & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. Nature, 574(7779), 505-510. https://doi.org/10.1038/s41586-019-1666-5

3. Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

4. Gheorghiu, V., Mosca, M., & Parent, A. (2019). Quantum cybersecurity: Fundamental limits in quantum hacking and quantum privacy leakage. ACM Computing Surveys (CSUR), 52(6), 1-37. https://doi.org/10.1145/3338511

5. Harrow, A. W., & Montanaro, A. (2017). Quantum computational supremacy. Nature, 549(7671), 203-209. https://doi.org/10.1038/nature23458

6. Hughes, D. M., & Stebila, D. (2020). Quantum key distribution (QKD) and post-quantum cryptography for blockchain technologies. International Journal of Network Management, 30(5), e2095. https://doi.org/10.1002/nem.2095

7. Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Lvovsky, A. I., & Fedorov, A. K. (2017). Quantum-secured blockchain. Quantum Science and Technology, 3(3), 035004. https://doi.org/10.1088/2058-9565/aa8072

8. Londoño, J. P. R. (2019). Transitioning blockchain networks to post-quantum cryptography. IACR Cryptol. ePrint Arch., 2019, 1412. https://eprint.iacr.org/2019/1412

9. Mercer, D. (2020). Quantum computing and blockchain: Their impending collision and potential cybersecurity implications. Journal of Cyber Policy, 5(1), 141-164. https://doi.org/10.1080/23738871.2020.1728479

10. Miles, D., Sonika, R., Schoendube, J., & Hohenberger, S. (2022). Sok: On the difficulty of blockchain protocol changes. IACR Cryptol. ePrint Arch., 2022, 501. https://eprint.iacr.org/2022/501

11. Mohseni, M., Read, M., Neven, H., Boixo, S., Denchev, V., Babbush, R., Fowler, A., Smelyanskiy, V., & Martinis, J. (2017). Commercialize early quantum technologies. Nature News, 543(7644), 171. https://doi.org/10.1038/543171a

12. Reyes, C. L. (2020). Conceptualizing cryptolaw. Nebraska Law Review, 98(2). https://digitalcommons.unl.edu/nlr/vol98/iss2/6

13. Woolford, D., Setoco, C., Stein, S., Engelsen, K., Chen, Q. A., & Knottenbelt, W. J. (2021, May). Cryptocurrency security standard (CCSS) based on semiformal security modeling for blockchain and smart contracts. In International Conference on

Financial Cryptography and Data Security (pp. 230-249). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-63958-0_14

14. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2017). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375. https://doi.org/10.1504/IJWGS.2018.10016848

15. Londoño, J. P. R. (2019). Transitioning blockchain networks to post-quantum cryptography. IACR Cryptology ePrint Archive, 2019, 1412. https://eprint.iacr.org/2019/1412

16. Miles, D., Sonika, R., Schoendube, J., & Hohenberger, S. (2022). Sok: On the difficulty of blockchain protocol changes. IACR Cryptology ePrint Archive, 2022, 501. https://eprint.iacr.org/2022/501

17. Hughes, D. M., & Stebila, D. (2020). Quantum key distribution (QKD) and post-quantum cryptography for blockchain technologies. International Journal of Network Management, 30(5), e2095. https://doi.org/10.1002/nem.2095

18. Reyes, C. L. (2020). Conceptualizing cryptolaw. Nebraska Law Review, 98(2), 384-450. https://digitalcommons.unl.edu/nlr/vol98/iss2/6

19. Woolford, D., Setoco, C., Stein, S., Engelsen, K., Chen, Q. A., & Knottenbelt, W. J. (2021, May). Cryptocurrency security standard (CCSS) based on semiformal security modeling for blockchain and smart contracts. In International Conference on Financial Cryptography and Data Security (pp. 230-249). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-63958-0_14