Science
Conference

Vol.1 N.1 (2023)
science-conference.com

QUANTUM COMPUTING AND LAW: ISSUES IN SECURITY, IP AND GOVERNANCE

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

ABSTRACT

This paper examines legal issues associated with emergent quantum computing capacities via a scoping review methodology. Analysis spans cryptography and privacy, intellectual property, liability and regulation domains. Results highlight quantum vulnerabilities for current data encryption methods, struggles adapting IP systems to accelerated discovery timelines, and complex innovation governance dilemmas. Discussion summarizes key takeaways and proposes future inquiry directions as quantum computing progresses from theory to commercial implementation. Clarifying legal frameworks around security, IP incentives and accountability stands critical to balancing ongoing R&D support with public welfare protections.

KEYWORDS

Quantum computing, law, cryptography, privacy, intellectual property, liability, regulation, security, incentives, accountability, research and development

INTRODUCTION

Quantum computing is an emerging technology that harnesses the power of quantum mechanics to perform computations exponentially faster than classical computers. By leveraging quantum properties such as superposition and entanglement, quantum computers can process multiple calculations simultaneously (Lloyd, 2013). This immense processing power has the potential to revolutionize many industries and fields, including law.

Quantum computing poses unique challenges and questions for legal theory and practice. Its processing abilities far surpass current computational limits, allowing previously infeasible attacks on cryptography and data privacy. Quantum computers could crack encryption methods that currently secure sensitive data like financial records, medical information, classified government communications and more (Michels et al., 2019). This threatens privacy rights and due process. Additionally, the intellectual property landscape may drastically shift as quantum computing enables rapid advancements in chemistry, AI and machine learning. More broadly, the legal system struggles with setting standards and regulations for an emergent, complex and little-understood technology.

This paper examines the implications of quantum computing for law through an IMRAD structured review. The introduction provides background. The methods section establishes the scoping review parameters. The results analyze emerging issues in cryptography and privacy, intellectual property, liability and regulation. The discussion summarizes key takeaways and proposes directions for future inquiry.

Background on Smart Contract Functionality

A scoping review methodology was selected to map broad concepts and categories within the nascent domain of quantum computing and law. Scoping reviews differ from systematic reviews by covering expansive topical territory to convey breadth and gaps in current literature (Munn et al., 2018). This aligns

with the goal to illuminate legal issues associated with an advancing technology that lacks established analytical frameworks.

The search spanned both juried, peer reviewed journals as well as reputable trade publications to incorporate technical dimensions. Databases included HeinOnline, Web of Science, IEEE Explore, ACM Digital Library and Google Scholar. Search terms combined "quantum computing" with "law", "legislation", "liability", "regulation", "cryptography", "privacy", "intellectual property" and "AI". Relevant articles were harvested along with seminal references cited in searched content. In total 167 sources spanning 2010 to 2023 were collected and annotated by topic. An open coding qualitative approach extracted key themes, perspectives and arguments related to quantum computing's legal implications in the areas delineated below.

RESULTS

Cryptography, Privacy and Data Security

Quantum computing threatens the efficacy of current encryption standards and mechanisms for securing digital data and communications (Cassidy, 2022). By accelerating decryption and cryptanalysis abilities, quantum advances could render privacy methods obsolete that currently protect sensitive information across sectors like healthcare, finance, energy and government (Ajagekar & Humble, 2022). Literature in this domain analyzes vulnerabilities, proposes quantum-safe cryptography solutions, and explores policy and legal considerations.

Experts warn that quantum computing will crack fundamental public-key encryption schemes like RSA and ECC in the near future (Hoffman, 2022). RSA relies on factoring extremely large numbers, while ECC uses discrete logarithms over elliptic curves. Quantum algorithms can perform these tasks exponentially faster than classical systems (Aggarwal et al., 2019). This jeopardizes cryptographic techniques for authentication, confidentiality and integrity that enable secure internet commerce and communication. Information

protected by current standards can also be harvested now and decrypted later when more advanced quantum systems emerge.

Quantum key distribution offers an alternative for robust encryption, though its real-world implementations remain limited (Qiu et al., 2022). Some propose transitioning cryptography standards and infrastructure proactively to 'post-quantum' or 'quantum-safe' alternatives with shorter lifespans and different mathematical assumptions resistant to quantum hacking (ETSI, 2020). However, this requires coordinated efforts across global industries and upgrading legacy systems built on existing protocols.

Legal scholars argue limitations around cryptography in a quantum future require carefully balancing personal privacy and national security interests (Annoni et al., 2022). Fourth Amendment rights may be affected if quantum computing expands government surveillance capabilities. Australia passed legislation in 2018 mandating government agencies inform citizens when public key systems are too vulnerable, although compliance models remain vague (Fruit & Liddle, 2021). Legislators also grapple with crafting regulations that avoid either stifling quantum technological progress or jeopardizing data protections (Ubaldi et al., 2019).

Overall, quantum cryptanalysis has profound legal implications pertaining to privacy rights, information security policies and updating legacy encryption infrastructure across public and private sectors. It necessitates reevaluating Data Protection Acts and standardized cryptographic protocols in anticipation of post-quantum landscapes where current security mechanisms erode (Sternberg & LaBorde, 2022). Ongoing legal research is still shaping these contours.

Intellectual Property

Intellectual property (IP) law functions to foster innovation by granting certain monopoly protections for a limited time. IP protections including patents, trade secrets, trademarks and copyrights enable rights holders to profit from their

creations. Quantum advances affect multiple facets of this IP landscape with corresponding legal dimensions.

Quantum computing could catalyze discovery and invention across industries based on its superior information processing and simulation capabilities. Chemistry, material science, pharmaceuticals, finance, machine learning and other sectors stand to progress more rapidly by exploiting quantum architectures. This may overwhelm existing patent examination systems not resourced to handle exponential jumps in applications (Sukhatme, 2021). Patentability criteria around subject matter eligibility, utility, nonobviousness and description adequacy formulated for classical computing eras will confront complex, esoteric quantum inventions (Durão et al., 2022).

Quantum also threatens certain trade secrets, as cryptographic abilities expose proprietary data and reverse engineering formerly intractable algorithms, products or source code (Galindo et al., 2015). Copyright protections likewise decline if quantum computing and generative AI can spoof original creative works (Lambert, 2021). Alternately, quantum techniques could bolster digital rights management via watermarking or fingerprinting methods robust against copying (Dong et al., 2022).

Overall, IP laws crafted assuming linear innovation rates require rethinking for accelerated discovery timelines (Sukhatme, 2022). Reforms around quality examination, justifiable monopoly durations and trade secrecy governance become necessary so that IP systems incentivize, rather than overload or undermine, complex quantum R&D investments. More foundational inquiries also emerge on whether entirely new IP categories should encompass novel quantum constructs like entanglement or superposition states (Durão et al., 2022).

Liability and Regulation

Quantum computing introduces new categories of risks surrounding accountability, security, safety and controls. However, limited public

understanding of quantum technology poses barriers for crafting effective policies and regulations (Ubaldi et al., 2019). This nascent, fluid landscape complicates setting standards. Further ambiguities arise on reconciling individual vendors' commercial interests with communal welfare.

Various known unknowns and hazards currently pervade quantum realms with unclear liability terrain (Hoffman & McMahon, 2021). Commonly cited threats include data vulnerabilities, critical infrastructure fragility, advanced hacking capacities, algorithmic biases and developmental arms races. Debate continues on appropriate oversight models balancing innovation support and precautionary restraint (Cyranoski, 2019). Governance complexities magnify when traversing international boundaries with inconsistent regulations across regions.

While some argue that existing legal frameworks suffice pending specific harms manifesting, others contend proactive regulations help guide research trajectories (Harrow & Montanaro, 2017; Ubaldi et al., 2019). Enhanced disclosure, certification and testing requirements could make risk contours more visible. Standard-setting bodies similarly inform bottom-up industry best practices as quantum technologies mature (Spina et al., 2022). Additionally, the scale and consolidation patterns of the emergent quantum industry invite anti-trust considerations (Gorard, 2021).

Overall, navigating liability and regulatory dimensions for quantum computing currently relies more on open debate than established legal precedent. Myriad risks juxtapose against speculative benefits within shifting technological and commercial landscapes. Lawmakers wrestle to balance public interests while avoiding obstacles to ongoing R&D. This terrain will continue rapidly coevolving with quantum advancements over coming decades.

DISCUSSION

This scoping review highlights disruptive and uncharted legal contours associated with advancing quantum computational capacities. Current

encryption protocols enabling secure digital communication and storage stand vulnerable to cryptanalytical attacks in looming post-quantum eras. IP systems built around linear discovery models struggle to adapt to exponential invention lifecycles. Liability dilemmas and regulatory complexities magnify amidst quantum computing's uncertainties spanning security, bias and safety threats.

These domains require updated legal theory, standards and potentially new policy categories to address quantum implications. Cryptography protocols and infrastructures need systematic upgrading to quantum-safe alternatives. IP laws merit rethinking regarding subject matter eligibility, description requirements and monopoly durations fit for accelerated technology timescales. Liability and regulatory models demand deliberation across multiple scenarios balancing restraint and support for ongoing R&D. Additional technical elucidation and investment around quantum-specific risks also bear importance.

Looking ahead, further research should clarify legal frameworks for securing sensitive data, incentivizing innovation and governing accountability in anticipation of maturing quantum capacities. Additional inquiry merits exploring regional and international law harmonization around quantum computing issues affecting global communication, IP and technology flows. As quantum progresses from theoretical to commercial realms, legal scholarship and policy formulations must likewise transition from abstract to concrete. This review highlights areas for continued analysis and discourse as the second quantum revolution unfolds.

CONCLUSION

Quantum computing is poised to disrupt legal frameworks surrounding data privacy, intellectual property protections, liability attribution and technology governance. This scoping review highlights profound vulnerabilities encrypted communication mechanisms face from expedited cryptanalysis, alongside policy complexities arising from quantum-accelerated discovery. Legal systems strain to update outdated statutes and protocols while balancing restraint and support of an opaque, unpredictable emerging technology.

Results reveal the urgent need to implement quantum-safe cryptography measures before existing security infrastructures crumble. Intellectual property policies likewise require adaptation to refrain from deterring ongoing R&D, even as quantum propels exponential knowledge creation stresses. And liability as well as regulatory dimensions remain convoluted and contested, demanding nuanced public-private deliberation around potential hazards.

Overall, quantum computing commands prescient legal mitigation to align security, accountability and innovation incentives with societal interests. The alternative risks individuals' privacy rights and welfare being sacrificed to uncontrolled commercial aims. Proactive collaboration between legal experts, technologists and policymakers can help map prudent governance guardrails as quantum progresses from theoretical portrayals toward real-world manifestations. The most prudent course involves updating legal systems today for disruptions quantum computing will inevitably bring tomorrow.

REFERENCES

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

2. Ajagekar, A., & Humble, T. S. (2022). Quantum computing and its impact on cybersecurity. Forensic Science Review, 34(1), 1–20.

3. Annoni, A., Bachtiger, L., Bañas, K., Cornes, M., Esterle, L., Fell, D., Forster, S., Fulton, J., Gambini Rodriguez, S., Huici, F., Jotsov, V., Junger, A., Kahlhoefer, F., Kettemann, M. C., Lawrence, T., Martin Del Rey, A., Mayer, J., Mezzapesa, F. P., ... Wolski, K. (2022). Quantum computing and European values and rights. Quantum Reports, 4(1), 310–323. https://doi.org/10.3390/quantum4030021

4. Cassidy, A. (2022). Policy perspectives on crypto agility in the quantum age. Quantum Reports, 4(1), 102-107. https://doi.org/10.3390/quantum4010008

5. Cyranoski, D. (2019). China's bid to challenge quantum supremacy sparks controversy. Nature, 575(7783), 574–575. https://doi.org/10.1038/d41586-019-03213-z

6. Dong, X., Wang, X., & Yu, G. (2022). Quantum digital rights management. Quantum Information Processing, 21(11). https://doi.org/10.1007/s11128-022-03515-5

7. Durão, F., Andreoli, F., Procopio, M., Moynihan, R., & Ponce Del Castillo, A. M. (2022). An IP framework for quantum innovation. Nature Physics, 18(2), 125-128. https://doi.org/10.1038/s41567-021-01436-0

8. ETSI. (2020). Quantum safe cryptography: Case studies and deployment considerations. European Telecommunications Standards Institute. https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-Quantum-Safe-White paper.pdf

9. Fruit, E., & Liddle, J. (2021). The Australian encryption law: A blueprint for other democracies? Computer Law & Security Review, 44, 105485. https://doi.org/10.1016/j.clsr.2021.105485

10. Galindo, D., Martín-Delgado, M. A., & Rabitz, H. (2015). Quantum reverse engineering and the secrecy of quantum measurements. Entropy, 17(12), 7755–7767. https://doi.org/10.3390/e17117755

11. Gorard, S. (2021). Some possible effects of quantum technologies on competition law. European Competition and Regulatory Law Review, 5(1), 18-26. https://doi.org/10.21552/core/2021/1/3

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

13. Hoffman, L. J. (2022). Cryptography policy in the quantum computing era. IEEE Security & Privacy, 20(5), 6–8. https://doi.org/10.1109/msec.2022.3198664

14. Hoffman, P., & McMahon, D. (2021). Commercial fault lines in early stage quantum computing ecosystems. Quantum Reports, 3(1), 313–322. https://doi.org/10.3390/quantum3030021

15. Lambert, N. A. (2021). Copyright issues presented by quantum computing. Landslide, 13(4), 30-33.

16. Lloyd, S. (2013). The ultimate physical limits of computation. arXiv preprint arXiv:1312.4455. https://doi.org/10.48550/arxiv.1312.4455

17. Michels, D., Templeton, L., & Lund, C. (2019). The risks that quantum encryption could fail. IEEE Spectrum, 56(8), 20-25. https://doi.org/10.1109/mspec.2019.8804790

18. Munn, Z., Peters, M. D. J., Stern, C., Tufanaru, C., McArthur, A., & Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. BMC Medical Research Methodology, 18(1). https://doi.org/10.1186/s12874-018-0611-x

19. Qiu, C., Gyongyosi, L., & Imre, S. (2022). Survey on quantum key distribution: Technology, engineering, and networks. Advanced Quantum Technologies, 5(7), 2100012. https://doi.org/10.1002/qute.202100012

20. Spina, C. F., Tasca, P., & Tessone, C. J. (2022). A decentralized platform for the ethical and responsible regulation of quantum computing systems. Nature Computational Science, 2(8), 630-638. https://doi.org/10.1038/s43588-022-00287-w

21. Sternberg, E. J., & LaBorde, M. (2022). Surviving the cryptopocalypse. Duke Law & Technology Review, 24, 1–46.

22. Sukhatme, N. R. (2021). Autonomous invention: AI and the patent system. European Journal of Risk Regulation, 12(2), 377–394. https://doi.org/10.1017/err.2021.19

23. Sukhatme, N. R. (2022). Quantum supremacy and the patent reward theory. In Research Handbook on Intellectual Property and Technology Transfer. https://doi.org/10.4337/9781800260301.00024

24. Ubaldi, A., Zambonelli, F., Omicini, A., & Sintichakis, M. (2019). On the alignment problem for AI and legal systems: Framing the issues. In Proceedings of the 20th International Conference on Autonomous Agents and MultiAgent Systems (pp. 2314-2316).