**PhD Research Proposal**

**Title:** Evaluating the Performance of Quantum-Resistant Lattice-Based Blockchain Frameworks Utilising Direct Acyclic Graph (DAG) Systems for Healthcare Environments

**Applicant:** Callum Turino

# Introduction

Blockchain technologies offer potential revolutionary improvements to various sectors. A particular focus can be placed on its use within healthcare environments as various solutions can provide secure, private, and trusted methods of processing patient data using current cryptographic primitives. With progress in the field of quantum computing, the realisation of Shor’s algorithm is of concern, rendering asymmetric and hashing algorithms insecure. Solution blockchain frameworks have been proposed that utilise the hard problems presented in lattice cryptography which provides quantum-resistance. These are presented with issues however of scalability and performance on a larger scale, which is pertinent within healthcare environments. The use of direct acyclic graphs (DAGs) in conjunction within blockchain shows potential in improving these systems. However, there is a current gap in research in its benefit to quantum-resistant frameworks, specifically in healthcare environments. This proposal aims to address this gap and offer solutions based upon its findings.

# Overview of Problem Area

## Blockchain within Healthcare

Since blockchain’s initial development, much research has been conducted on creating the standards as seen today. These technologies may offer advancements within multiple sectors such as agriculture, energy, finance, and healthcare [1]. A particular focus can be placed on blockchain’s use within healthcare. The data that is processed and transferred across hospital networks contains sensitive data pertaining to patients’ medical information. A system in which this data can be shared privately and securely is of high value. This interest can be seen in a systemic review conducted in [2] which found an increasing trend of academic research and development in the area. This research has yielded an array of proposed frameworks, each offering differing solutions.

Data management systems used within healthcare pose several issues due to their current design. Firstly, single points of failure and potential data leakages facilitated by a centralised topology are present in these systems. Also, the management lacks transparency, traceability, immutability, and auditing provisions [3]. Security and privacy issues are also present as discussed in [4] which highlights concerns surrounding aspects such as authentication techniques, anonymity, and confidentiality. Blockchain technologies have been proposed to resolve these issues as they can offer decentralisation, tamper resistance improved auditing, and increased accuracy in health data among many others [3], [4]. However, these proposed solutions have limitations which must be addressed, such as throughput and latency when implemented into larger environments [5] and the cryptographic primitives used are susceptible to quantum attacks [4].

## Quantum Resistant Solutions

The cryptographic primitives found within current blockchain frameworks are a security concern, moving forward, as quantum computing technologies continue to advance. Asymmetric cryptography and hashing function algorithms, that use RSA and ECC respectively, relied upon the hardness of prime factorisation and logarithmic problems to ensure security. However, as the realisation of Shor’s algorithm occurs with the advancement of quantum computing, these algorithms will no longer be secure against attack [6]. This threatens the security of patient data and the level of trust in the systems that process it [7].

To combat this concern posed to blockchain networks, several replacement solutions have been proposed that utilise the desirable characteristics of lattice based PQC algorithms. This is due to these algorithms showing consistent favourable performance and security, allowing for use on a wide array of systems [8]. Varying approaches have been taken to resolve this issue such as the work in [6] and [9] which use novel quantum-resistant aggregate signature schemes, showing improved performance and security when compared to their counterparts. Other proposed schemes can be seen in [10] which uses a NTRU crypto system for hierarchal deterministic key generation, showing improved performance over the traditional ECC scheme. There is also a healthcare specific blockchain scheme seen in [7] which uses a public key searchable encryption to facilitate the accessing of medical data in a secure manner. This scheme also shows promise in its ability to improve computational expense and efficiency as the number of retrieving keywords increase. Finally, healthcare systems that utilise lattice algorithms can benefit from the potential use of homomorphic encryption which would allow for the processing of patient data without the need to be decrypted first, ensuring privacy and security throughout. However, this can be very computationally expensive and further research is required in this area [11]. It is important to consider that despite the proposed systems previously discussed showing improvements to their respective counterparts and original systems, issues are still present that may limit their integration into healthcare systems, particularly regarding areas such as scalability and interoperability .

## DAGs Potential to Improve Healthcare Blockchains

Current and newly proposed blockchain systems suffer from issues in terms of scalability and throughput which can be of concern in large scale and time constrained environments such as healthcare [3]. An approach that can be considered to resolve these challenges is the use of DAG within blockchain systems [3], [6]. When used within blockchain, DAG systems can provide several benefits such as improved throughput by allowing multiple transactions confirmed within a singular round as opposed to linear systems, fewer communications by nodes and reduced storage overhead [12]. Furthermore, some proposed systems have shown these benefits as seen in [13] improving vehicular social networks and in [14] improving throughput in a personal healthcare information system. However, DAG systems do not come without issues that must be addressed first before its adoption within healthcare. A survey of proposed DAG systems conducted in [12] showed that many did not include privacy properties and were not able to simultaneously achieve higher throughput, scalability, and higher confirmation time. However, something that must be considered is the use of DAGs within quantum-resistant lattice frameworks, which is an area that has not been extensively researched. This proposed research aims to address this gap and hopes to present a system with DAG integration that’s provides a scalable, efficient quantum-resistant blockchain framework within healthcare to improve and protect the processing of patient data.

# Research Aims and Outcomes

The research proposal aims to bridge the gap in current research on the potential use of DAG within quantum-resistant lattice blockchain frameworks. The proposal will do this by conducting an extensive evaluation of the performance of frameworks with DAG integration to determine its effect. Overall, it aims to answer the following research questions:

1. Would integration of a DAG system in current and future proposed quantum-resistant frameworks improve performance without a cost to overall security and functionality?
2. Would that integration be both practical and beneficial within healthcare environments?
3. Would the improved performance allow for the inclusion of homomorphic encryption?
4. How can the data gathered be used to improve current and future designs?

The outcomes of this research would allow for the improvement of current and future framework designs and provide a means for their integration into healthcare environments. The data presented could allow for a more scalable and secure system to be created. The creation of a feasible design will provide security in the sector and ultimately lead to the overall improvement of healthcare as the secure processing of patient data can be conducted on a larger scale. Furthermore, it is possible that the use of a DAG design would allow for an increase in interoperability as the makeup of healthcare devices continues to evolve, including the potential wide use of IoT devices in the sector. Finally, as homomorphic encryption can provide greater security in the sector, the data gathered could provide a foundational basis for any future design that would include the technology.

# Research Methodology

To answer the research questions previously mentioned, the preliminary research methodology can be broken down into the following phases:

* A comprehensive literature review of the current state of research on quantum-resistant frameworks utilising lattice-base cryptography, DAG systems and their use within blockchain and the application of them within healthcare.
* Evaluation of current framework designs using a DAG system with any modifications if required. This would include the performance metrics of the blockchain design itself including latency, throughput, transactions per second among any other relevant metrics. Alongside this, the computational performance of the design on relevant standard and medical devices typically found in healthcare systems using metrics such as processing speed and memory usage will be evaluated.
* Using the data gathered, perform a comparative study against designs which do not utilise DAG systems, to better understand if it is a beneficial solution in the context of healthcare.
* Provide reccomendations to improve current and future framework designs based upon the results of the evaluation and comparative study.

# Candidate Information

Previous experience in the area has presented the candidate with an understanding of the work that is to be carried out. This is in the form of an honour’s dissertation conducting an evaluation of the computational performance for various PQC algorithms on multiple processor architectures. Furthermore, the candidate has gained knowledge and experience in networking and cryptography through previous educational experience. To be able to conduct and achieve the outcomes of the proposed research the candidate would be seeking a scholarship position with the university upon completing their current degree.

# Summary

Blockchain within healthcare shows great promise in improving the overall quality of the health care by providing a secure and audited way in which patient data can be processed. However, current designs are susceptible to scalability issues and quantum attacks using standard cryptographic primitives. This research proposal aims to address these concerns by determining the potential use of DAG systems within current quantum-resistant blockchain frameworks and ultimately provide a series of reccomendations for their improvement and integration into healthcare environments.

# References

[1] U. Bodkhe *et al.*, ‘Blockchain for Industry 4.0: A Comprehensive Review’, *IEEE Access*, vol. 8, pp. 79764–79800, 2020, doi: 10.1109/ACCESS.2020.2988579.

[2] H. S. A. Fang, T. H. Tan, Y. F. C. Tan, and C. J. M. Tan, ‘Blockchain Personal Health Records: Systematic Review’, *J Med Internet Res*, vol. 23, no. 4, p. e25094, Apr. 2021, doi: 10.2196/25094.

[3] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, ‘Blockchain for healthcare data management: opportunities, challenges, and future recommendations’, *Neural Comput Appl*, vol. 34, no. 14, pp. 11475–11490, 2022, doi: 10.1007/s00521-020-05519-w.

[4] M. S. Arbabi, C. Lal, N. R. Veeraragavan, D. Marijan, J. F. Nygård, and R. Vitenberg, ‘A Survey on Blockchain for Healthcare: Challenges, Benefits, and Future Directions’, *IEEE Communications Surveys & Tutorials*, p. 1, 2022, doi: 10.1109/COMST.2022.3224644.

[5] D. Khan, T. J. Low, and V. T. B. Dang, ‘Challenges and Application of Blockchain in Healthcare Systems’, in *2022 International Conference on Digital Transformation and Intelligence (ICDI)*, 2022, pp. 15–20. doi: 10.1109/ICDI57181.2022.10007295.

[6] R. Saha *et al.*, ‘A Blockchain Framework in Post-Quantum Decentralization’, *IEEE Trans Serv Comput*, vol. 11, no. 4, 2021, doi: 10.1109/TSC.2021.3116896.

[7] G. Xu *et al.*, ‘PPSEB: A Postquantum Public-Key Searchable Encryption Scheme on Blockchain for E-Healthcare Scenarios’, *Security and Communication Networks*, vol. 2022, p. 3368819, 2022, doi: 10.1155/2022/3368819.

[8] D. C. Q. D. T. D. J. Kelsey, Gorjan Alagic Daniel Apon, J. L. Y.-K. L. C. Miller, D. M. R. P. R. Perlner, and A. R. D. Smith-Tone, ‘Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process’, 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf%0Ahttps://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8309.pdf

[9] Q. Li, M. Luo, C. Hsu, L. Wang, and D. He, ‘A Quantum Secure and Noninteractive Identity-Based Aggregate Signature Protocol From Lattices’, *IEEE Syst J*, vol. 16, no. 3, pp. 4816–4826, 2022, doi: 10.1109/JSYST.2021.3112555.

[10] S. Banupriya, K. Kottursamy, and A. K. Bashir, ‘Privacy-preserving hierarchical deterministic key generation based on a lattice of rings in public blockchain’, *Peer Peer Netw Appl*, vol. 14, no. 5, pp. 2813–2825, 2021, doi: 10.1007/s12083-021-01117-2.

[11] K. Munjal and R. Bhatia, ‘A systematic review of homomorphic encryption and its contributions in healthcare industry’, *Complex & Intelligent Systems*, 2022, doi: 10.1007/s40747-022-00756-z.

[12] Q. Wang, J. Yu, S. Chen, and Y. Xiang, ‘SoK: Diving into DAG-based Blockchain Systems’, *CoRR*, vol. abs/2012.0, 2020, [Online]. Available: https://arxiv.org/abs/2012.06128

[13] W. Yang, X. Dai, J. Xiao, and H. Jin, ‘LDV: A Lightweight DAG-Based Blockchain for Vehicular Social Networks’, *IEEE Trans Veh Technol*, vol. 69, no. 6, pp. 5749–5759, 2020, doi: 10.1109/TVT.2020.2963906.

[14] T. Zhou, X. Li, and H. Zhao, ‘Med-PPPHIS: Blockchain-Based Personal Healthcare Information System for National Physique Monitoring and Scientific Exercise Guiding’, *J Med Syst*, vol. 43, no. 9, p. 305, 2019, doi: 10.1007/s10916-019-1430-2.