# Towards a Post-Quantum Resistant Ethereum

## 1 Project Abstract

Quantum computers scalable enough to defeat modern public-key cryptosystems—and seriously compromise other security methods—are expected to become available in the next ten to fifteen years[4;6]. For several reasons, discussed at length in a previous paper[4], cryptocurrencies and other systems built on blockchain technologies are particularly susceptible to quantum attacks.

In this work, we propose to narrow our focus to the Ethereum network, in order to deliver a more complete and thorough study. We will analyse the vulnerability to quantum attacks of the Ethereum blockchain as it exists today. We will also study currently proposed changes to the network, and analyse their impact on Ethereum's quantum-security. Finally, we will provide our own proposals for how to improve the quantum-security of Ethereum, and provide an impact assessment of these proposed changes.

## 2 Objectives

The main objective of the proposed work is to create a road map for the Ethereum Network to become quantum-safe. To this end, we will study the vulnerabilities of the Ethereum network, as it currently exists, and as it is planned to, is likely to, change in the upcoming years. We will then propose changes to the network that would mitigate these vulnerabilities.

We will study what costs and overheads these changes would cause for the network; this would include changes to block sizes, transaction message propagation and the cost of sending transactions. This work will look primarily at the digital signature schemes used as well as the P2P network.

The success of this project will lead to publishable results, that will be presented in suitable venue(s) such as a conference or journal. All results will be published with gold open-access and all work material will be open-sourced.

## 3 Outcomes

Given that, as it currently stands, the entire Ethereum network is vulnerable to collapsing entirely with advent of scalable quantum computers, it is hard to overstate the potential impact of our work to the Ethereum network. Our work could potentially lay the groundwork for a fully quantum-safe Ethereum network—a goal which either is, or should be, of the highest priority to the Ethereum Foundation.

## 4 Grant Scope

If funded, these are the questions we propose to tackle: *what vulnerabilities to quantum attacks does Ethereum currently suffer?*[1] *How can these security concerns be mitigated? What is the implication of Ethereum becoming post-quantum resistant?*

The output from this research grant will be 1-2 published works that will answer these questions.

## 5 Project Team

The proposed research is to be carried at the University of Kent. The team currently includes Carlos Perez-Delgado as the principal investigator (PI) investing $20\%$ of his time, and Joseph Kearney as a post-doctoral research assistant (PDRA), fully focused on the project for the duration. If funded, we will leverage this funding against other funders to seek to hire one more PDRA.

### 5.1 The University of Kent *(Host Institution)*

The University of Kent has extensive practical experience in the cyber security and pattern recognition field through its established Kent Interdisciplinary Research Centre in Cyber Security (KirCCS). The Centre, established in 2012, has grown into a vibrant centre for technical and interdisciplinary research with high external visibility. It has attracted several million pounds in external funding in the period since its inception and it has pioneered the development of novel hardware-based device authentication techniques. It harnesses expertise across the University to address current and potential cyber security challenges and represents the University of Kent as a UK government recognised ACE-CSR (Academic Centre of Excellence in Cyber Security Research), one of only 19 such centres in the UK. Its strategic objective is to promote wide-ranging

[1] This question has been answered to some extent.

multidisciplinary research, and to provide a vibrant and expanding environment capable of strongly supporting its members in their research activities.

### 5.2 Carlos A. Perez-Delgado *(Principal Investigator)*

The proposed PI for this project, Carlos A. Perez-Delgado has extensive research and supervision experience in the proposed research area, and its encompassing fields. He received his Ph.D. in November 2007 from the University of Waterloo, in Canada[7]. He has subsequently worked as a postdoctoral researcher at the University of Sheffield, the National University of Singapore and as a senior research fellow at the Singapore University of Technology and Design.

In that time he has published dozens of articles in refereed journals and conference proceedings, a book chapter, received roughly 900 citations (h-index 14), supervised and co-supervised four PhD students and three postdoctoral research fellows, and supervised various MSc students and undergraduates. His publications touch various areas of quantum information and computation, including algorithms[12], models of computation[8], metrology[13], quantum software engineering[10] and most relevant to this project, secure computation[3–5;9;11].

Carlos has also done consulting work for large energy corporations in the UK, advising them on the impact of quantum technologies on their business. He's been invited to address business leaders on the same topic, namely at TEISS. Most notably he has been invited, on now multiple occasions, to address and advise the the UK intelligence community at GCHQ headquarters in Cheltenham on these topics. Carlos has been described by one high-ranking UK intelligence member as *"one of the few people in the world who has both the cybersecurity and the quantum theory expertise[..] needed to tackle the most important questions in this field."*

### 5.3 Joseph Kearney *(Postdoctoral Research Associate)*

Joseph J. Kearney received a BSc in biomedical science from the University of Kent in 2014 and an MSc in computer science in 2018. From 2014 to 2017 he was owner and director of the Red Brewery. From 2018 to 2020 he worked at Atlas City Global as a Blockchain Researcher. In September 2020 he re-joined University of Kent as a PhD Candidate. He is the lead author of one of the seminal papers in the proposed research area[4]. Joseph is expected to complete his PhD in September 2023.

## 6 Background

In 2017 Aggarwal *et. al.*[1] published a paper drawing the attention to the vulnerability of the Bitcoin network to various quantum-technological attacks.

In 2021 Kearney and Perez-Delgado[4] extended the vulnerability analysis to other major (at the time) blockchain based crypto-currencies—including Ethereum. This work concluded that, in the case of Ethereum, quantum computers could viably attack the transaction mechanism, and through that, compromise individual accounts. Another vector of attack was Ethereum's use, at that time, of a proof-of-work (PoW) system for its consensus mechanism.

Ethereum, by its nature, is a system that is designed to evolve and adapt to technological changes. Already, since the publication of the above paper in 2021, Ethereum has changed drastically, by for example dropping PoW in favor of proof-of-stake consensus protocol. The existing changes, and proposed changes to the protocol, change and will change the nature of the Ethereum network's vulnerability to quantum attacks. Currently, the precise nature of these vulnerabilities, to the best of our knowledge, are not known.

## 7 Methodology

We will study the current state of the Ethereum network, and proposed changes from various important sources. We will apply the analysis pioneered by Aggarwal *et. al.*[1], and further developed Kearney, Bard, and Perez-Delgado in papers since then[2;4].

## 8 Timeline

Below is a summary of the two project work-packages, associated milestones, and expected results. Research on WP1 should be completed about half-way through the project, with publication of results before the end of the project. Research work on WP2 will be finished by the end of the one-year project, though publication of results could be delayed further due to usual scientific peer-review lead-times.

### 8.1 Work-package 1: Ethereum Vulnerabilities to Quantum Attacks

In early 2021, Kearney and Perez-Delgado published a paper[4], based on earlier work by Aggarwal *et. al.*[1] on the vulnerabilities of what were then some of the major cryptocurrencies, to quantum attacks—including Ethereum. Two years later, the Ethereum has changed. We will answer these questions: how do these changes, and future changes, affect our previous analysis? What need to be done to ensure that the current, and future, version of Ethereum be quantum safe? The end-result of this WP will be the production of a white-paper—to be made publicly available upon completion—detailing a full audit of the quantum vulnerabilities of the full Ethereum eco-system. This risk-analysis will include methods of attack, predicted timeline on which these attacks will become viable, and ultimate cost/impact to the Ethereum network and ecosystem.

Besides the production of a white-paper, we will also seek to publish our results in a suitable scientific venue.

### 8.2 Work-package 2: Implications of Post-Quantum Resistance for the Ethereum Ecosystem

Post-quantum cryptography, the usual mechanism by which networked systems like blockchains can be secured against quantum attacks, is generally less efficient, requires more overheads, and has greater costs in terms of device memory, computational power, and communication between parties, than traditional cryptography. The precise impact of making a system quantum-secure can vary widely depending on the system.

For this work package, we will create a roadmap for implementing the necessary changes to the Ethereum blockchain to make it quantum-safe. This roadmap will consider the real-world costs and hurdles of implementing these major, and fundamental, changes to the massively distributed ledger that is Ethereum. We will build on the risk-analysis of WP1, and considering the costs mentioned in the previous paragraph, we will carry out an cost-benefit analysis of implementing the changes in our roadmap.

Like with WP1, we will make our findings public as a white-paper as soon as they are available; and we will further seek to publish our results in an appropriate scientific venue.

## 9 Budget

**The total economic cost for this project is $\$112,417.59$ (USD).** The budget is further split in the following way.

**Staff – Directly incurred posts:** $\$67,027.58$ One Post-doctoral research assistant (PDRA), for a period of 12 months.

**Staff – Directly allocated posts:** $\$19,811.25$ Dr. Perez-Delgado will spend 20% of his time on this project throughout its lifespan. This time will be split between outreach, administrative, supervisory, and mentorship roles as well as—and to the largest extent—research.

**Conference Travel and Subsistence:** $\$9,240.00$ This is to cover attendance at major conferences for both the PDRA and PI. The target conferences will include *Financial Cryptography and Data Security* and *QCrypt*.

**Other directly incurred costs:** $\$7,920.00$ These include publication costs, including open-access fees, and equipment costs (mostly computing) for the PI and PDRA over the lifetime of the project, and includes VAT at $20\%$

**Indirect costs:**
**Estates cost & Administrative support:** $\$8,418.76$

## References

[1] Divesh Aggarwal, Gavin K Brennen, Troy Lee, Miklos Santha, and Marco Tomamichel. Quantum attacks on bitcoin, and how to protect against them. *arXiv preprint arXiv:1710.10377*, 2017.

[2] Dan A Bard, Joseph J Kearney, and Carlos A Perez-Delgado. Quantum advantage on proof of work. *Array*, 15:100225, 2022.

[3] Michal Hajdušek, Carlos A Pérez-Delgado, and Joseph F Fitzsimons. Device-independent verifiable blind quantum computation. *arXiv preprint arXiv:1502.02563*, 2015.

[4] Joseph J Kearney and Carlos A Perez-Delgado. Vulnerability of blockchain technologies to quantum attacks. *Array*, 10:100065, 2021.

[5] Atul Mantri, Carlos A Pérez-Delgado, and Joseph F Fitzsimons. Optimal blind quantum computation. *Phys. Rev. Lett.*, 111(23):230502, 2013.

[6] M. Mosca. Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security Privacy*, 16(5):38–41, Sep. 2018.

[7] C. A. Pérez-Delgado. Quantum Cellular Automata: Theory and Applications, 2007.

[8] Carlos A. Pérez-Delgado and Donny Cheung. Local unitary quantum cellular automata. *Phys. Rev. A*, 76(3):032320, Sep 2007.

[9] Carlos A Pérez-Delgado and Joseph F Fitzsimons. Iterated gate teleportation and blind quantum computation. *Phys. Rev. Lett.*, 114(22):220502, 2015.

[10] Carlos A Pérez-Delgado and Hector G Perez-Gonzalez. Towards a quantum software modeling language. In *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, pages 442–444, 2020.

[11] Li Yu, Carlos A Pérez-Delgado, and Joseph F Fitzsimons. Limitations on information-theoretically-secure quantum homomorphic encryption. *Phys. Rev. A*, 90(5):050303, 2014.

[12] Liming Zhao, Carlos A. Pérez-Delgado, and Joseph F. Fitzsimons. Fast graph operations in quantum computation. *Phys. Rev. A*, 93:032314, Mar 2016.

[13] Marcin Zwierz, Carlos A. Pérez-Delgado, and Pieter Kok. General optimality of the Heisenberg limit for quantum metrology. *Phys. Rev. Lett.*, 105(18):180402, Oct 2010.