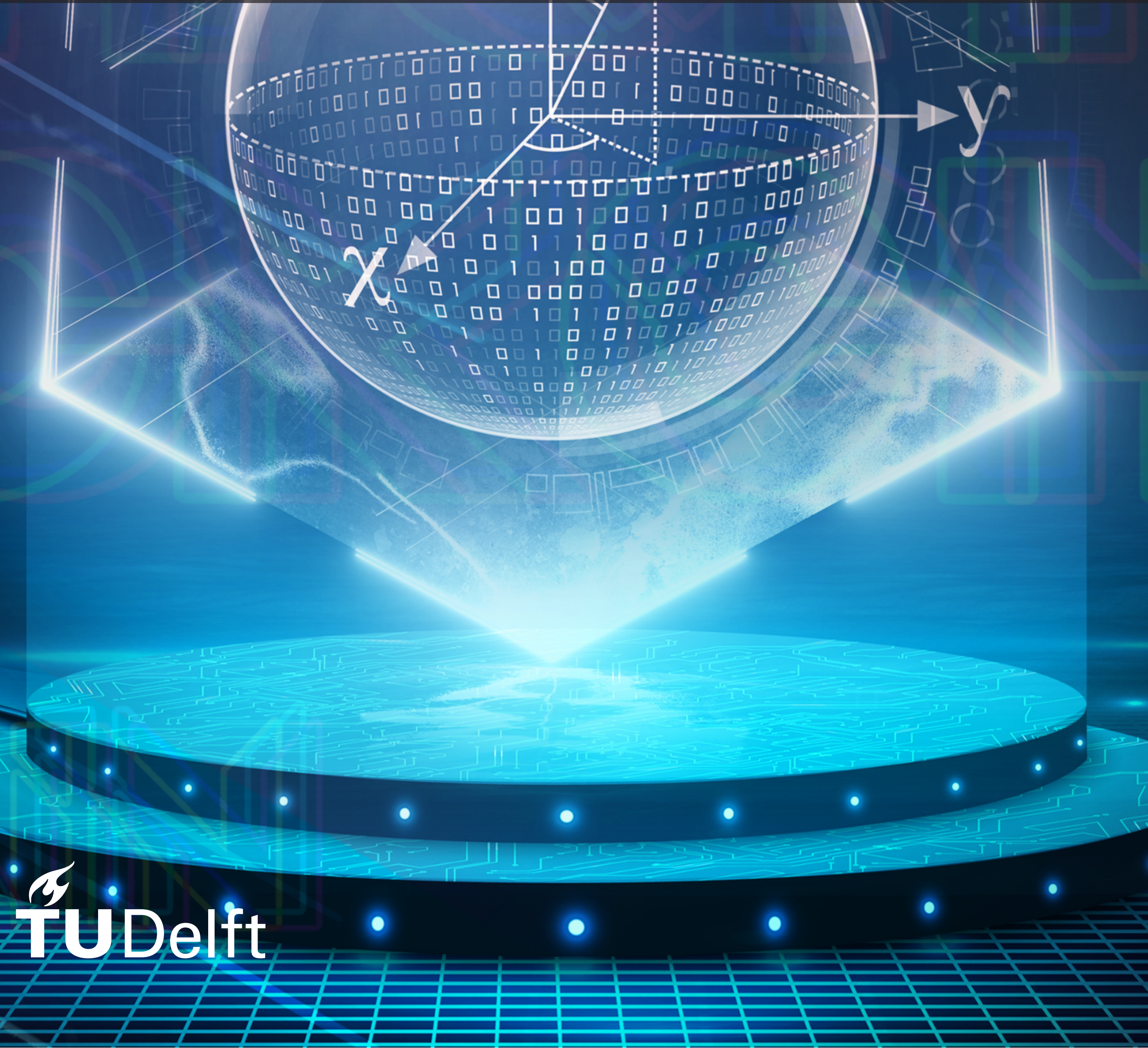
The Cryptogeddon of Blockchain

Designing policy recommendations for public blockchains to transition towards a quantum-safe environment.

MSc. Engineering and Policy Analysis
Yunus Sezer

Delft University of Technology



TU Delft

The Cryptogeddon of Blockchain

Designing policy recommendations for public blockchains to transition towards a quantum-safe environment.

An MSc thesis submitted to Delft University of Technology
for the degree of Master of Science

by

Yunus Sezer

Student Number: 5416035
MSc Engineering and Policy Analysis
Faculty of Technology, Policy and Management
Project Duration: October 2022 - March 2023
Cover Image: Chad Soren Harper, Orchid Labs

To be defended in public on March 20th, 2023

TU Delft	Chair:	Haiko van der Voort
	1st Supervisor:	Yury Zhauniarovich
	2nd Supervisor:	Jolien Ubacht
Deloitte	1st Supervisor:	Itan Barmes
	2nd Supervisor:	Bram Bosch

TU Delft

Preface

In the summer of 2022, I joined Deloitte as a working student, and on the very first day, they encouraged all new joiners to write an introductory email to all colleagues, outlining our interests, skill sets, and ambitions, so, I did. Two days later, my laptop started ringing, and I received a call through MS Teams from Itan Barmes. Although I was somewhat confused, as I did not know him by then, I decided to pick up. We talked for a bit, got along, and he told me that he was working on a Quantum Security Lab with Anne Ardon and asked whether I would be interested to work on this. I was very happy with the provided opportunity, and this became the very first (big) project that I participated in. Before the call ended, Itan asked more about the topic of my original MSc thesis proposal and we got to talking. Although my original proposal was also tied to blockchain, it was a completely different topic (and to be completely fair, not that exciting). He told me about the two Deloitte articles that he and Bram Bosch had written on the quantum threat for the Bitcoin and Ethereum blockchains and my interest peaked. After the call ended, I read those two articles, did more research on my own, and was completely in shock. I have been involved with blockchain technology since 2017 and I have been following its adoption and (technological) developments very closely, and never had I come across this particular topic. Shortly after, I met Bram Bosch, a blockchain expert whose technical understanding seems to have no limits. We discussed the topic of the quantum threat to blockchain more in-depth and he told me that overcoming the quantum threat in an effective and timely manner would be one of the most challenging questions for blockchain organizations to answer in the coming decade(s). Meanwhile, as I was helping to design the Quantum Security Lab, I found out that there were significant efforts out there that aid large organizations, institutions, and governments with preparing for the upcoming quantum threat, and although it is not yet at the stage where it should be, progress was occurring. Unfortunately, to my surprise, this was not the case for blockchain, and that worried me. By now, it was the end of summer, and I had to start working on my original thesis topic, but I could not let this topic go. So, I decided to change my MSc thesis topic and I am very happy that I made that decision.

Although the topic of the quantum threat to blockchain is very demanding and challenging, let alone the complexity of designing recommendations that can aid the blockchain space to transition safely in time, I was not alone in this endeavor. This MSc thesis would not have been possible without the supervision and support that I was provided. Firstly, I would like to thank Haiko van der Voort for chairing the Committee and providing me with the necessary perspectives for steering the research. Yury Zhauniarovich has been incredibly helpful, as he has been following the work closely since the start and has always provided me with immense levels of valuable advice and (technical) support. Jolien Ubacht's eye for detail and academic experience has really improved the quality of the work. Moreover, I would like to extend my gratitude to my two supervisors at Deloitte Netherlands, Itan Barmes and Bram Bosch. Itan's expertise and vision make him an excellent supervisor, overseeing the progress and ensuring that it adheres to professional standards is what sets him apart. Bram Bosch, a walking Google (Scholar), was always ready to answer any type of question and always made time for me when I needed his support. I would also like to extend my gratitude to Tommie van der Bosch and Kim Schneider, the Director and Manager of Deloitte's Blockchain Team, as their close mentorship and encouragement were highly appreciated. I also wish to thank all 30 interviewees for sharing their valuable expertise and knowledge. Lastly, my friends have also been an incredible source of support and encouragement and I feel incredibly lucky to have such great people in my life. Thank you all!

That being said, I dedicate this MSc thesis to my mother and father, Semra Bohurler Sezer and Ibrahim Sezer. Thank you for always believing in me and being the driving force of my motivation.

Yunus Sezer
Delft, March 2023

Disclaimer: This research does not reflect the views and opinions of the institutions that are listed on this report, including the (company) supervisors, but solely the main author.

Executive Summary

Since Bitcoin's genesis block validated the concept of blockchain technology, the domain has developed an enormous amount. There are still developments to be made in its architecture to lead the way to mass adoption, but a variety of different applications have already been built with enormous (future) potential. By many, this domain is recognized to be the front line of technological developments by either leading the advancements or adopting them relatively quickly. Although this domain started off with decentralization and establishing individual freedom, without (the need for) any outside interference in the form of policies and regulations, it is slowly moving away from these elements. Mainstream institutional adoption of the technology, along with a substantial amount of retail and institutional investments in this domain, has led the space to leave its mark on society. (Un)fortunately, depending on one's view, this has led to many proposals for regulating this space. Accordingly, many are asking the following question: *"For what reasons, and to what extent, should one regulate the blockchain domain?"*

This research has put this question in the context of the upcoming quantum threat to the blockchain domain. The capabilities of quantum computers are reaching new milestones on a yearly basis, and their computational power has exceeded Moore's Law in terms of growth rate. It is expected that in the decade(s) to come, quantum computers will reach a point of sufficient size and sophistication, in which they can be deemed as Cryptographically Relevant Quantum Computers (CRQCs). At that point, they can utilize Shor's and Grover's quantum algorithms to break most of today's public-key cryptography, and this also applies to blockchain technology. If the blockchain domain fails to transition towards a quantum-safe environment, it renders the technology useless, and if the transition does not occur in time, the trust in this technology will be broken as the infrastructure will collapse and most of the funds will be stolen. Meaning, the future of this technology is at serious risk, and preparations must be made.

The aim of this research is to add to the existing body of knowledge and provide an overview of recommendations that can aid the blockchain space in its transition towards a quantum-safe environment in time. The recommendations take many different forms, ranging from discussions on regulations and policies to proposals and suggestions for guidance and support. The findings can be presented to policy experts and stakeholders from the blockchain domain. The methods that were used for this research include literature analysis, secondary data analysis, market analysis, case studies, and interviews.

This paper first discusses the technical side of the problem and the mitigation strategies. It provides an overview of the technical tradeoffs of the most prominent post-quantum cryptography systems, along with a set of technical implications and considerations one has to take into account when transitioning towards a quantum-safe environment. As a result, a technical framework emerges that provides the reader with an overview of the most relevant technical aspects. After the technical chapter, the organizational side has been investigated, in which blockchain's (decentralized) governance is discussed, along with different ways of implementing change through a variety of on-chain and off-chain methods. Furthermore, the most prominent stakeholders that were capable of driving change in this environment were identified. Taking the top 100 cryptocurrency projects into consideration, a large-scale market analysis was conducted on their current state of public quantum awareness, research, and adoption, which was the foundation of the creation of the N.A.R.A.Q. framework. Taking the aforementioned elements into consideration, 30 interviews were conducted with industry leaders and experts in the blockchain and cryptography domain, ranging from co-founder, project lead, CEO, and CTO to cybersecurity experts and designers of (post-quantum) cryptosystems. This was done in order to get a better understanding of how they perceived the current and future state of this domain in light of the quantum threat, along with their views on (the different types of) regulations and policies versus guidance and support, and the respective barriers and obstacles for transitioning towards a quantum-safe environment.

Ultimately, all of these elements were tied together in the last chapter. Here, the Quantum-Secure Stamp of Approval (QSSA) was proposed, alongside a more extensive version of the N.A.R.A.Q. framework. The aspect of using and investing in Non-Quantum-Secure Blockchain Technologies (NQSBT) was discussed and several considerations were made for each different element and target group, which ultimately resulted in a set of policy recommendations for these specific areas. The topic of external institutional technical support was discussed, as to what extent it could aid the blockchain space, and the blockchain community and stakeholders were addressed and proposals were made for more collaborative efforts. The most prominent barriers and obstacles were analyzed and the final remarks were made.

As we are not living in a utopian society, it is great to have some level of regulation that protects the users and investors. However, these regulations should not harm the development and innovation of this space. This research was constantly treading this fine line. Individuals and organizations look up to regulatory bodies for guidance, but if they do not understand the technology well, or are out of touch with the opinions and views of industry leaders and experts, the results will be ineffective, as they could be over-regulating the (wrong segments of the) space. The results of this research can be seen as a foundation from which policymakers and stakeholders from the blockchain community can be guided, and has hopefully opened the floor for a healthy discussion on how the blockchain space can successfully transition towards a quantum-safe environment in time without an overburden of regulation.

Contents

Nomenclature

Abbreviation	Definition
AICA	American Innovation and Competitiveness Act
BFT	Byzantine Fault Tolerant
BIP	Bitcoin Improvement Proposal
BT	Blockchain Technology
CIA	Confidentiality, Integrity and Availability
CRQC	Cryptographically Relevant Quantum Computer
CVP	Closest Vector Problem
DAO	Decentralized Autonomous Organization
DORA	Digital Operational Resillience Act
EC	European Commission
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
EIP	Ethereum Improvement Proposal
EPA	Engineering and Policy Analysis
ESO	European Standards Organisation (ESO)
ETSI	European Telecommunications Standards Institute
MICA	Markets in Crypto-assets
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
NQSBT	Non-Quantum Secure Blockchain Technologies
OTS	One-Time Signature
PQC	Post-Quantum Cryptography
QSSA	Quantum-Secure Stamp of Approval
RSA	Rivest–Shamir–Adleman
SHA	Secure Hash Algorithm
SVP	Shortest Vector Problem
WEF	World Economic Forum

List of Figures

List of Tables

1 Introduction

Blockchain technology (BT) has garnered a tremendous amount of attention in the past couple of years and its technological potential and ”bright” future is constantly being discussed. Bibliometric analyses [22] has shown that the number of scientific publications on BT has been increasing every single year. Similarly, for the past five years, global spending on blockchain solutions has had an average annual growth rate of 63% [23], and over 320 million people worldwide have already interacted with an element of BT by either owning or using a particular cryptocurrency [24]. Gartner expects this technology to mature around 2025 [25], and has sent one clear message to the executives: *”Don't ignore blockchain”* [26]. But what happens if we ignore one of the biggest threats to BT, i.e., the quantum threat imposed by quantum computers? Will BT still be able to utilize its technological potential and have its ”bright” future if its underlying cryptography is not quantum secure?

Fortunately, there has been extensive research conducted on how quantum computers could theoretically break certain types of cryptography [27]. Accordingly, the cryptographic community has also been been working continuously on Post-Quantum Cryptography (PQC) to advance the use of quantum-resistant primitives that can secure our digital infrastructure against classical and quantum computers [28]. However, the journey of transitioning towards quantum safety has its difficulties [29], and taking the unique technological and organizational properties of blockchain into consideration, it is expected that the journey for BT will bring unique challenges to light. The World Economic Forum (WEF) has created a Centre for the Fourth Industrial Revolution and is currently focused on shaping policies and strategies that aid in accelerating the necessary changes for BT to reach its full potential [30]. However, with the introduction of quantum computing, these have to be adjusted accordingly. This research aims to build upon the existing body of knowledge and put the quantum threat in the context of BT. As a result, this report aims to design recommendations that are aimed (mostly) at policy experts that can aid with the (acceleration of the) process of transitioning towards a quantum-safe environment in time.

2

Problem Analysis

2.1. Research Background

2.1.1. Introduction to Quantum Computers

In 1981, around 60 theoretical physicists and computer scientists had gathered at the MIT Endicott House to discuss the possibility of taking cues from the natural world for designing a more powerful and efficient ways of computing [31]. One of the attendees, Richard Feynman, proposed to build a new type of computer that takes advantage of quantum mechanics (*"because nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical."[32]).* His paper has been credited by many for the birth of quantum computation and simulation [33].

In 2019, almost 40 years later, Google announced that they achieved quantum supremacy with their *Sycamore* quantum computer. The processor obtained a million samples in 200 seconds, whereas it would have taken a state-of-the-art classical computer approximately 10.000 years [34]. Even though this claim has been heavily criticized, both in terms of the complicated nature of benchmarking the appropriate metrics [35], and playing around the definition of quantum supremacy that was originally coined by John Preskill [36], it has sparked worldwide discussion surrounding the potential of quantum computers. For decades, the field of theoretical computer science have operated under the assumption of the *"extended Church-Turing thesis"* [37], which states that a classical computer (Turing machine) can efficiently perform any type of calculation that any other kind of computer can efficiently perform. Google was one of the first to reject this, and in June, 2022, Xanadu, a quantum computing hardware and software company, announced that they have (also) violated the aforementioned assertion related to quantum supremacy, and have published peer-reviewed results of their tests [38][39]. It is only a matter of time before the assertion is completely disproven.

IBM has labeled this decade as the Quantum Decade, as they expect the technology to significantly accelerate viable solutions to increasingly complex societal, macroeconomic and environmental problems [40], and they are not the only ones looking into this. Large organizations are practically competing with one another for the future of computing [41], and nearly every single technologically developed country has its own national quantum initiative and/or is part of a global one [42].

2.1.2. Quantum Computers and Cryptography

The technology is improving rapidly [43], but unfortunately, there is a flip side to all the advances in computational power of quantum computers. A quantum computer of sufficient size and sophistication, which is also referred to as a Cryptographically Relevant Quantum Computer (CRQC), could have the potential of breaking most of today's public-key cryptography [44]. If this were to happen, it would have devastating affects on our society and economy, as it could jeopardize secure online communications, undermine critical infrastructure and defeat security protocols in place for most of the internet-based (financial) transactions [45]. Behind all of this, are certain quantum algorithms - algorithms that can be performed on a quantum computer, of which at least one step requires the use of quantum principles, such as superposition or entanglement [46]. There are a limited number of quantum algorithms that are relevant for the scope of this research in terms of the imposed risks on cryptography, in which Shor's and Grover's algorithm are the most prominent and relevant ones [47].

Asymmetric cryptography, also referred to as public-key cryptography, is a form of encryption that requires the creation of a mathematically related public and private key, designed to encode and decode a message, respectively [48]. There are several mathematical algorithms that are used to 'produce' the public and private key. These algorithms are, in crypto jargon, making use of a "*trapdoor*": functions that are easy to compute in one direction, yet extremely difficult to compute in the opposite direction [49]. The widely-used cryptosystem, RSA, relies on this principle, and fundamentally chooses two prime numbers (p and q) and publishes the product ($n = pq$) together with an integer (c). In order to break this code, one has to factor very large numbers in a reasonable length of time, and as p and q can be prime numbers with hundreds of digits, factoring $n = pq$ has been deemed to be infeasible, resulting in the encryption method being recognized as secure [50].

In 1994, Peter Shor devised a quantum algorithm that could (theoretically) solve the discrete logarithm problem and the aforementioned factorization problem in polynomial time [51], thus breaking public-key cryptography. However, to solve the factorization problem for large numbers that are believed to be cryptographically secure, a quantum computer has to reach a level of sufficient size and sophistication. This partially refers to the number of qubits, in which there are physical qubits that are noisy and error-prone, and logical qubits. There is a wide range of estimates on how many physical qubits would be needed to represent one logical qubit, but a reasonable number is 1.000 [52]. Throughout time, there have also been many different propositions on the amount of logical qubits needed to factor a 2.048-bit number, referring to RSA encryption. In 2003 [53], Beauregard estimated that it would require 2n+3 logical bits (4.099 logical qubits) to factor a n-bit number. In 2014 [54], Pavlidis and Gizopoulos proposed 9n+2 (18.434 logical qubits) and most recently, in 2021 [55], Gidney and Ekerå believed that it would require approximately 20.000 logical qubits. Today, the highest number of physical qubits that were achieved is 127 from IBM [56]. Meaning, there is still a long way before quantum computers will be able to break public-key cryptography. However, the level of growth should not be underestimated, as significant progress is occurring in this space [57]. Moore's Law states that the number of transistors in a microchip will double every two years, eluding towards exponential growth [58]. However, for quantum computers, Neven's Law seems to be gaining more attraction, as it predicts that quantum computing power will improve at a double exponential growth rate compared to conventional computing [59]. The estimates for the materialization of the quantum threat differ. However, WEF's latest report [60] argues that the timeline of 10 years, although uncertain, could arguably become even shorter due to the asymmetry of information and secrecy in regard to the (global) advancements in quantum computing by nations that aim to have a strategic advantage. To conclude, until now, only noisy-intermediate-scale-quantum operations have been performed, but once the necessary technological advances in this field have occurred, Shor's algorithm and its consequences will become reality [61].

Grover's algorithm, also referred to as the quantum search algorithm, searches through unsorted databases and reduces a brute-force search algorithm from $O(n)$ steps to $O(\sqrt{n})$ steps [62][63]. It is important to put this concept into context. A password passes through a cryptographic hash function that scrambles the data in a deterministic fashion. Meaning the same input always produces the same output, while adhering to the principles of the *"trapdoor"*. With classical computing, finding the original password would require checking all possibilities (brute-force). If the password has 8 characters, this results in $2^{64} = 1.8 * 10^{19}$ combinations. By utilizing Grover's algorithm, the password can be found in $\sqrt{2^{64}} = 4.3 * 10^{9}$ iterations. Assuming a rate of 1 billion checks p/s for both scenarios, it will respectively lead to password discovery in 585 years in comparison to a couple seconds [64]. Additionally, researchers have combined Grover's algorithm with the birthday paradox, resulting in $O(^{3}\sqrt{n})$ steps, thus further increases its efficiency to search through unsorted databases [65].

2.1.3. Introduction to Blockchain

Blockchain technology refers to a decentralized ledger that records and distributes all transactions across a peer-to-peer network. These transactions are contained in specific blocks in a particular chain in a network, and every time a new transaction appears on the blockchain, it is automatically recorded and added to every participant's ledger [66]. This database is managed by multiple participants and is referred to as the Distributed Ledger Technology. These ledgers can contain a variety of different types of data points, such as the attributes of a particular transaction, credentials, digital rights, intellectual property, identity (verification) or other pieces of relevant data and information [67]. As these transactions are recorded in a chronological manner, and each block in the network is validated through cryptographic hash functions (e.g. SHA-256), it forms an immutable chain that can neither be deleted nor modified [68]. It allows the users to record and share the common view of a particular system's past and current state across a distributed network, resulting in an immutable source of truth[69].

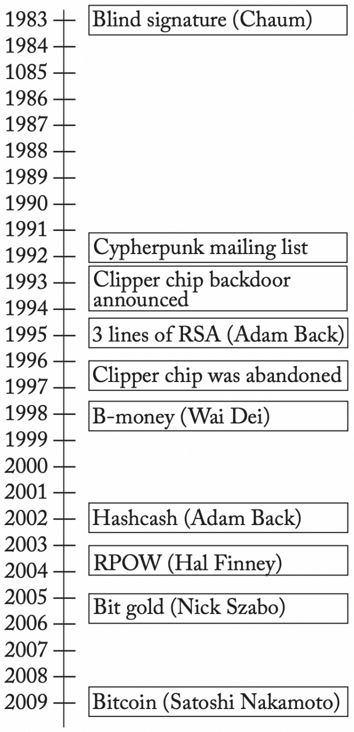


Figure 2.1: History of Cryptographic Currencies [1]

The creation of the underlying pieces of blockchain technology (BT) can be attributed to the cumulative efforts of many researchers over time, see Figure 2.1. More specifically, the concept of cryptographic currencies lies on the intersection of research between distributed systems and electronic cash systems [70]. However, Satoshi Nakamoto, whose real identity remains a mystery to this day, is widely recognized as the Founding Father of blockchain, after releasing the white paper *"Bitcoin: A peer-to-peer electronic cash system"* in 2008 [71], tying all the relevant research together, and conceptualizing the theory of distributed blockchains, whilst providing an infrastructure for secure, peer-to-peer transactions without the presence of a trusted third party. In less than one year after the publication, Bitcoin went from concept to reality when Nakamoto mined the first bitcoin block (the Genesis block), validating the concept of blockchain [72]. Despite the mysterious disappearance of Nakamoto after 2010, Bitcoin's trajectory continued to grow and by February, 2011, the value of one Bitcoin became equal to the U.S. dollar [73]. The focus was mostly on digital currency, however, in 2014, this focus started to shift slowly when Vitalik Buterin published a white paper [74] proposing a decentralized application platform and launched the Ethereum Foundation [75]. This moment can be recognized as a turning point for BT, as it discussed the technology's possibilities beyond digital currency usage through the introduction of smart contracts and provided developers with a platform to build decentralized applications (dApps) [76].

Throughout the years, researchers have established a wide range of use cases for blockchain; from financial and legal services to health care, manufacturing, supply chain, and many more [77]. Coupling this potential with the sheer amount of private and capital investments that are being made, the technology is expected to be adopted to a great extent and disrupt many (outdated) operations and industries [25].

2.1.4. Blockchain and the Quantum Threat

As discussed in section 2.1.2, quantum computing has introduced new security challenges. Consequently, this raises concerns on the level of security of blockchain. If there are no adequate measures in place to protect itself from CRQC's, blockchain will lose its data integrity and undergo significant asset theft.

Hash functions help to make blockchain (cryptographically) secure, and in order for a cryptographic hash function to be deemed secure, it needs to adhere to the "*trapdoor*" principle and be collision-resistant, in which the latter demands that it is 'difficult' to find two inputs that have the same hash value [68]. Grover's algorithm is a threat to cryptographic hashing, as it can search and find hash collisions in hash functions that are used in blockchains [78]. As a result, it can modify a signed data block on the blockchain and reduce the authenticity of the ledger entries. Furthermore, if "quantum mining" is utilized, it can accelerate the mining process in blockchains that make use of Proof-of-Work [79], undermining the computational effort with a quadratic speedup over a classical computer [80].

In order to obtain secure information exchanges between different parties, digital signatures are used to authenticate the transactions on the blockchain. For this process, blockchains can make use of Elliptic Curve Cryptography (ECC), which is a form of public-key cryptography with many discrete logarithm-based protocols, of which Elliptic Curve Digital Signature Algorithm (ECDSA) is used most frequently [81]. The security of ECDSA relies on the principle that one cannot solve the Elliptic Curve Discrete Logarithm Problem (ECDLP), which in turn relies on the assumption that there is no reasonably fast method in polynomial time to achieve this [82]. However, as discussed earlier in section 2.1.2, Shor's algorithm is capable of solving the discrete logarithm problem. Meaning, if a CRQC can successfully utilize Shor's algorithm, it can deduct the private key from the public key, resulting in significant asset theft. This has been analyzed by Deloitte for Bitcoin [2] and for Ethereum [3], see Figure 2.2 and 2.3. The results indicate that 25% of all Bitcoins are vulnerable to a quantum attack, whereas the number lies at 65% for Ethereum.

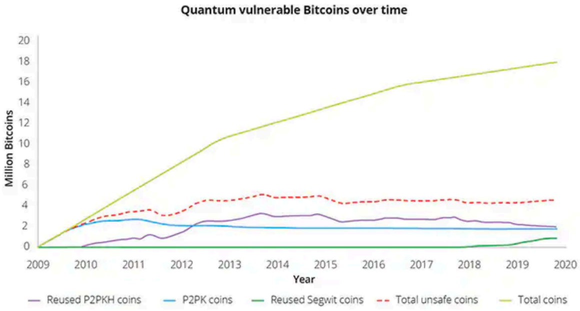


Figure 2.2: Distribution of Bitcoins that are stored in address that are vulnerable to quantum attacks [2]

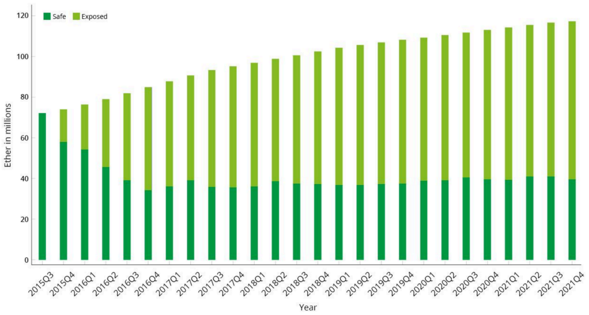


Figure 2.3: The number of Ether exposed (light green) and safe (dark green) to a quantum storage attack [3]

2.1.5. Preparations for Security in the Post Quantum Era

In December 2018, the National Quantum Initiative of the United States Congress was proposed as a law [83], aimed at accelerating quantum research and development for economic and national security. Accordingly, the National Security Memorandum of the White House [45], released on May 4th, 2022, stated how within one year of the date of this memorandum, and on an annual basis thereafter, the heads of all Federal Civilian Executive Branch Agencies should deliver an assessment [84] of their IT systems that remain vulnerable to the quantum threat. At the end of December 2022, US president Joe Biden enacted the legislation of the Quantum Computing Cybersecurity Preparedness Act [85], in which it is clearly outlined that *"a strategy for the migration of information technology of the Federal Government to post-quantum cryptography is needed* [86]. Similarly, the European Union Agency for Cybersecurity (ENISA) released two reports on Post-Quantum Cryptography [87] [88], in which they stated, in both the conclusion chapters: *"policymakers and system owners should make preparations"*.

According to an estimate of BCG, quantum applications for cryptography in terms of encryption and decryption has a value creation potential of anywhere between 20 to 40 billion USD [89], and "big tech" has already stepped foot in this sector. Microsoft has a dedicated Post-Quantum Cryptography team that works together with academia and industry [90], while Amazon has patented unique ways to bring quantum security to its cloud services and intel has filed the most overall patents related to post-quantum cryptography with the US patent office [91]. Nevertheless, a report by Capgemini [92] found that the assurance of a huge leap in security with quantum technologies would be the trigger for 30% of organizations to prioritize quantum cryptography, whereas more standardization of security protocols was found to be 58%. Meaning, standardization can be considered a strong driver for change.

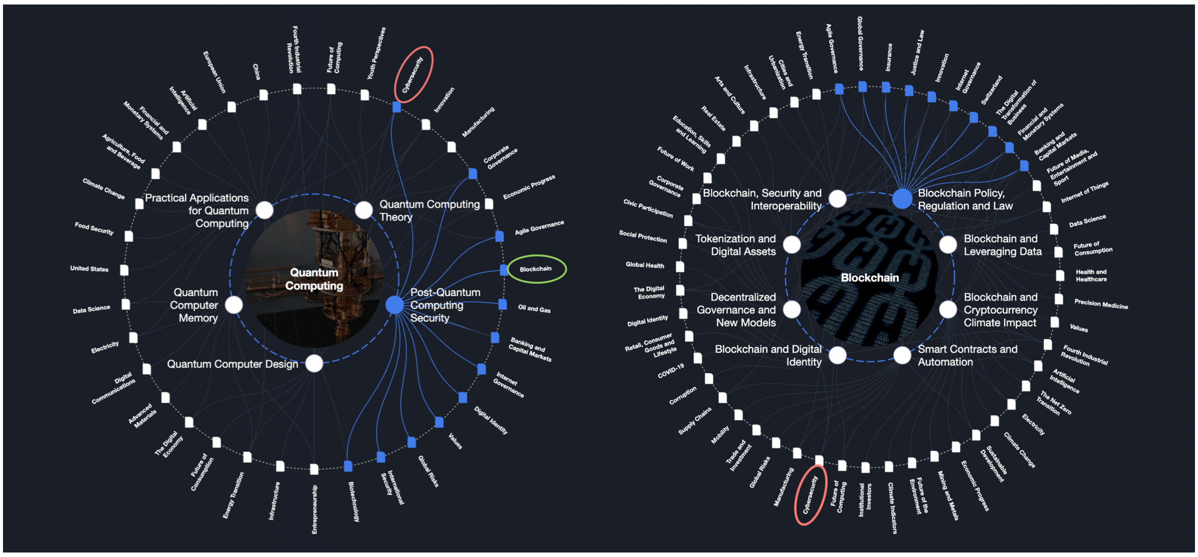


Figure 2.4: The Strategic Intelligence mapping of WEF for Quantum Computing (left) and Blockchain (right)

The WEF has developed and mapped out hundreds of global issues and their interdependencies in their *Strategic Intelligence* section [93]. In the map of *Quantum Computing*, *Post-Quantum Computing Security* has been directly tied to both *Blockchain* and *Cybersecurity*, but in the map of *Blockchain*, *Blockchain Policy, Regulation, and Law* is not (yet) tied to *Cybersecurity* (see Figure 2.4). This perfectly sums up the current state of affairs. There is awareness, relationships have been established, and simultaneously papers have been published by WEF that include discussions on the quantum threat of blockchain [60] [94], but it is not (yet) a part of (proposals for) policies and regulations. However, the same cannot be said about "regular" organizations in the non-BT domain. There, progress is occurring.

2.2. Research Analysis

2.2.1. Research Objective

Taking all of the aforementioned aspects into consideration, the following problem statement has been formulated:

The quantum threat is expected to change the (cryptographic) landscape of blockchain. However, little progress is occurring in the blockchain space and there are no policy recommendations that aid in accelerating the adoption of quantum-safe solutions for blockchain while discussing the most prominent technological and organizational barriers for implementation. Ultimately, there is no guidance (for policymakers) to protect the space.

Accordingly, the following research objective has been constructed for academic exploration in the dissertation:

The research objective is to design recommendations on how blockchain can transition towards a quantum-safe environment before the arrival of a CRQC by analyzing the most prominent technological and organizational mitigation strategies to overcome barriers for implementation, while discussing to what extent regulations and policies versus guidance and support will aid this transition.

It is important to note that it is relatively difficult to find a suitable organization that can provide policy recommendations on this topic for the blockchain space, as the topic itself is rarely (well) understood, let alone discussed. However, one organization does stand out. The WEF is working closely with industry experts and has released numerous publications on the quantum threat, and taking the global nature and reach of the WEF into consideration, they seem to be the right stakeholder for this report. Most recently, in September 2022, they published a white paper [60] that was focused on guiding organizations toward quantum safety. In this report, they devoted a very small piece to the consequences of the quantum threat on blockchain and noted the following: *"It is therefore imperative (for blockchain) to start preparing the transition as soon as possible.* This dissertation can be seen as a follow-up to this statement and provides the WEF with (policy) recommendations on how blockchain can successfully transition toward a quantum-safe environment and the possible means for accelerating this adoption. As of now, no such (policy) recommendations exist and the space is left to deal with this major threat on its own.

2.2.2. Research Questions

Consequently, the following main and sub-research question(s) have been composed to steer the research:

What type of regulations, policies, and guidelines should be made that can aid the blockchain space to transition towards a quantum-safe environment in time, both from within the blockchain community and from the outside (policy makers)?

1. *What are the technical solutions for achieving quantum safety for blockchain, and what are the technological implications and considerations when implementing these solutions?*
2. *How can one drive change in blockchain's decentralized governance mechanism and who are the most prominent stakeholders that should be leading the transition?*
3. *What is the current state of public market maturity surrounding the quantum threat in the blockchain domain?*
4. *What are the main considerations when designing policy recommendations for blockchain to transition toward a quantum-safe environment?*

2.2.3. Research Overview and Scope of Research

In order to provide an adequate policy recommendation that can aid the blockchain space to transition faster toward a quantum-safe environment, it is of great importance to understand the technical and organizational part. Accordingly, three categories have been designed to do so, and each is crucial for answering the subquestions.

- Technical - What does the quantum threat exactly mean for blockchain? What specific elements of this technology will it influence and what will be the corresponding consequences? What would be the most prominent mitigation strategies to tackle this threat, from a technical point-of-view, and what would be their implications if implemented for blockchain? What are some key technical factors that should be taken into consideration to have a successful transition toward a quantum-safe environment? This part answers sub-question 1
- Organizational - How can one drive change in an environment that is structured with a decentralized governance mechanism? Who are the most prominent stakeholders that can drive change? What is the current level of awareness, research, and adoption in the blockchain space in terms of quantum-safe solutions? This part answers sub-question 2 and 3.
- Recommendations - To what extent should the blockchain space be regulated with policies that accelerate the adoption of quantum-safe solutions, and what can such policies and regulations look like? What are the perceptions of industry experts on this topic? What type of guidance and support would be welcomed by the blockchain space and what are some key factors of success? This part answers sub-question 4.

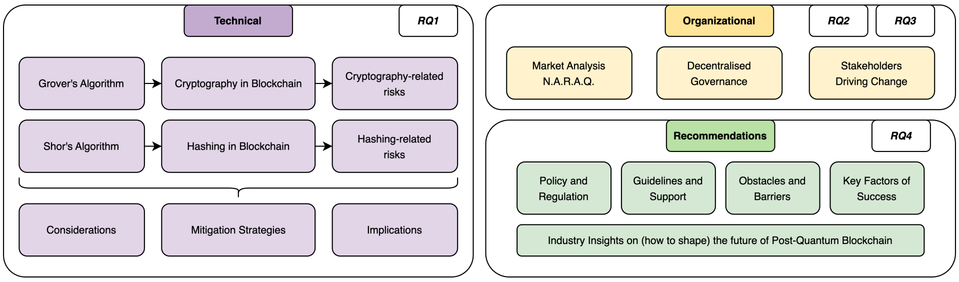


Figure 2.5: The elements that make up each sub-question of the research

This dissertation mostly focuses on public blockchains and does not discuss private (permissioned/permissionless) blockchains. This is due to the following reasons: (1) it is considered to be relatively easier for private blockchains to reach a consensus on upgrading the protocol due to their governance mechanism, (2) public blockchains will carry the "burden" of the technical tradeoffs of post-quantum cryptography more than private blockchains, due to the fact that public blockchain's networks are larger and rely more on speed, cost, and efficiency than private blockchains, i.e. R3 Corda or Hyperledger [95] [96] having a slower key generation speed is less important for their ecosystem than it is for Ethereum's.

This dissertation rests upon the assumption that the CRQC (1) will arrive in the future, otherwise there is no point for this research, and (2) will arrive around the year 2030, otherwise there is no reference point at which blockchain should become quantum-safe. The assumption of 2030 rests upon plotting the roadmap of IBM, which is one of the largest companies involved in developing scalable quantum computers, in terms of the expected number of qubits in relationship to Moore's Law [4], along with the results of a 2021 study that interviewed 47 quantum experts from academia and industry [70]. The (rough) estimate tends to point towards a CRQC arriving sometime between 2030 and 2040. As the quantum space is developing, more accurate predictions can be made, but as of now, the 2030 prediction will be adopted.

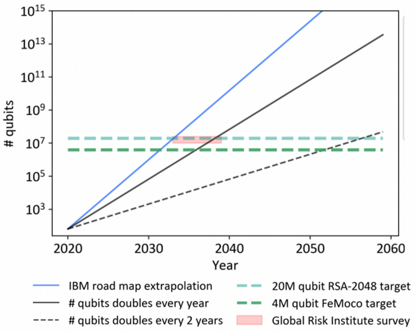


Figure 2.6: An estimate on the arrival of a CRQC [4]

3

Research Approach

This research aims to design a policy recommendation for blockchain that can aid the space to transition faster towards a quantum-safe environment. However, in order to do so, one must understand the technical aspect of the problem and solution, the governance element of the processes that are associated with implementing these types of protocol upgrades, the relevant stakeholders that are capable of driving change, and the (perceptions of blockchain experts surrounding) the topic of policies. Since this research requires a combination of many different approaches, both in terms of quantitative data exploration vs quantitative data, and primary and secondary data sources, it will make use of the mixed-methods approach. This section will provide an overview of the methodology that was adopted for this dissertation.

3.1. Research Methodology

There are three key research strategy decisions that have to be taken in order to select the right research approach [97]. Every decision slightly adjusts the focus of the research and offers a different academic approach of achieving the research objective in an efficient manner.

- Breadth vs Depth - Breadth encapsulates a large-scale approach that focuses on generalization of results. Depth focuses more on a small-scale approach that yields very specific knowledge that can be generalized to a lesser extent. This research aims to harmonize blockchain technology and cybersecurity in the context of the quantum threat. The researcher opts for breadth over depth, as nearly every single blockchain-related project has a unique approach to designing its protocol, and a policy recommendation needs to be given to the entire public blockchain space. However, for larger chains, they will be researched to a greater extent, to provide some level of depth understanding of how they function.
- Quantitative vs Qualitative - Quantitative knowledge would be required to compile the (literature) findings in tables and charts, and will consist of analyzing the respective variables in the form of numbers, but a greater emphasis will be on qualitative knowledge, as that is highly required to draw causal relations between pre- and post-quantum integration and the respective (potential) technological changes of blockchain's operations as a result of (partial) adoption, in which the latter refers to hybrid approaches.
- Empirical vs Desk - Empirical researchers gather first-hand data, while desk researchers aim to conduct extensive literature reviews and gather the most relevant and reliable data from other researchers, companies and organizations. The author opts to be a desk researcher in the earlier stages of the research, while also taking personal initiative by reaching out and setting up interviews with people (cyber and blockchain experts) to gain more insights into their thoughts on the upcoming opportunities, challenges and operations that are related to (policies for) transitioning towards post-quantum blockchain.

Taking this into consideration, the researcher will be making use of an exploratory research approach. It will investigate the existing theory on (post-quantum) cryptography and blockchain operations, and aim to investigate how they can successfully adopt this technology from a technological and organizational point of view. On top of this, interviews will be conducted with blockchain and cyber experts to better understand the perception surrounding the quantum threat and the reaction of this space towards possible policies that can aid the blockchain domain to transition faster towards a quantum-safe environment. It is of great importance to also draw up a research flow diagram that aims to illustrate how different methods, tools, and objectives relate to each sub-question of this research. In this diagram, green represents the deliverables/outcomes of each sub-research question (SRQ), blue the requirements/characteristics for the information and data sources, and yellow the respective data gathering and research methods.

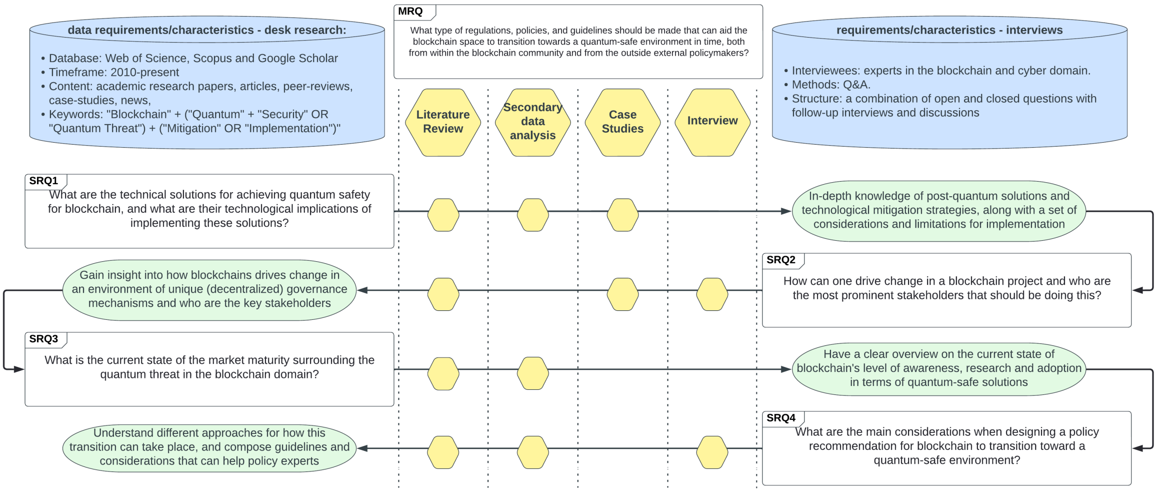

data requirements/characteristics - desk research:
• Database: Web of Science, Scopus and Google Scholar
• Timeframe: 2010-present
• Content: academic research papers, articles, peer-reviews, case-studies, news,
• Keywords: "Blockchain" + ("Quantum" + "Security" OR "Quantum Threat") + ("Mitigation" OR "Implementation")"
MRQ
What type of regulations, policies, and guidelines should be made that can aid the blockchain space to transition towards a quantum-safe environment in time, both from within the blockchain community and from the outside external policymakers?
requirements/characteristics - interviews
• Interviewees: experts in the blockchain and cyber domain.
• Methods: Q&A.
• Structure: a combination of open and closed questions with follow-up interviews and discussions
Literature Review
Secondary data analysis
Case Studies
Interview
SRQ1
What are the technical solutions for achieving quantum safety for blockchain, and what are their technological implications of implementing these solutions?
In-depth knowledge of post-quantum solutions and technological mitigation strategies, along with a set of considerations and limitations for implementation
SRQ2
How can one drive change in a blockchain project and who are the most prominent stakeholders that should be doing this?
Gain insight into how blockchains drives change in an environment of unique (decentralized) governance mechanisms and who are the key stakeholders
SRQ3
What is the current state of the market maturity surrounding the quantum threat in the blockchain domain?
Have a clear overview on the current state of blockchain's level of awareness, research and adoption in terms of quantum-safe solutions
SRQ4
What are the main considerations when designing a policy recommendation for blockchain to transition toward a quantum-safe environment?
Understand different approaches for how this transition can take place, and compose guidelines and considerations that can help policy experts

Figure 3.1: Research Flow Diagram

3.2. Interviews

3.2.1. Objective of Interview and Interviewee Profiles

The goal of the interview is to obtain valuable insights from people in the blockchain and cyber domain. In order to design an adequate policy recommendation, it is very important to listen to experts in these fields and integrate their considerations accordingly. These interviews are contributing to answering the last research question 4, and reflect back to subquestion 1, 2 and 3, and will be explained further in Chapter 6.

A total of 30 people have been selected to be interviewed. The interviewees have been carefully selected based on their level of working experience and current positions at different organizations. From this group of people, 10 originate from the cyber/cryptography domain, and 20 from the blockchain domain. This has been purposefully done so, as the topic itself is a concern for people in the blockchain domain, but it is interesting to incorporate the views of people from the cyber domain. This way, one has a birds-eye overview of the topic itself, in which people from both cyber/cryptography and blockchain provide their specific input. Also, it is interesting to see on what topics their views align and vary.

3.2.2. Structure of Interview

The sessions were designed to be one hour long, and had the following format:

- First 15 minutes - Introduction of the interviewee; name, position at the company, current and past working experience, level of awareness surrounding the quantum threat, and level of understanding/proficiency on blockchain and cryptography (based on a scale from 0 to 5 with definitions for each level).
- 30 minutes - Approximately a dozen of questions were asked to the interviewees in a structured manner. They were closed questions, in the sense that they could pick the answer in the following manner:
  - Pick a, b, c or d in regards to ...
  - Would you agree or disagree with ... (yes or no)
  - Think of a number or percentage that is appropriate for ...
  - Rank the elements in terms of ... from low to high
- Last 15 minutes - A brief moment for open questions, i.e., what do you think would be key factors that could hinder blockchain to transition towards a quantum-safe environment?

3.2.3. Analysis of Interview (Results)

Every single session has been recorded and stored on TU Delft's OneDrive. Accordingly, a quantitative and qualitative approach to data harvesting emerged. These were as follows:

- Quantitative: during the interview, the answers to the structured questions were put in a large spreadsheet with filters. As a result, this file allows the author to easily find the averages of values/percentages, the most picked answers and can search for patterns according to an interviewee's level of working experience, domain, or understanding of cryptography (i.e., people with traits X, Y that know Z tend to lean more towards A, B, C).
- Qualitative: as every session was recorded, the author listened to each of them afterwards to take notes. These notes mostly focus on the last 15 minutes that relate to the open questions part, however, as interviewees tend to provide motivation for their answers to the structured questions, the first 45 minutes became relevant. On average, for each interviewee, half a page of notes emerged with their views/opinions on different topics.

Based on the results of the interviews, both quantitative and qualitative, interesting findings can emerge. These will be incorporated into the dissertation and provide a backbone for the policies and regulations that the author aims to design at the end.

3.2.4. Data processing and Ethics

For the interviewees, the Human Research Ethics Checklist was successfully completed and adopted. It has answered questions surrounding documentation, data quality, storage and backup processes, legal and ethical requirements, and codes of conduct. The results were only shared with the research team and the individuals have been anonymized accordingly. Additionally, a form of consent was sent to each interviewee, outlining the purpose of the study and their level of involvement in terms of data processing and anonymity.

4

Micro - A Technical Analysis on the Quantum Threat of Blockchain

This chapter aids to discuss the quantum threat of blockchain on a technical level, in which the first two sections will address Grover's algorithm and the last two sections will address Shor's algorithm. Through this analysis, the first subquestion of this research can be answered. It will provide insights into the specific areas within BT where the quantum threat could materialize and discuss the respective technical solutions to implement. Additionally, it will also touch upon the technical implications of implementing these solutions and the respective considerations that one has to make when adopting these mitigation strategies. For this chapter, the primary method used is literature analysis, followed closely by secondary data analysis and investigating case studies.

4.1. Grover's Algorithm and Blockchain's Operations

A hash function is a mathematical function that generates a fixed-length output number/value from a variable-length input, in which the output is referred to as the *hash value*, *hash digest* or simply, *hash* [98]. The fixed-length output is usually denoted in *bits*, but can vary depending on the specific hash function (64-bit, 128-bit, 256-bit, 512-bit, etc.). In the case of SHA-256, the hash function and mining algorithm of the Bitcoin protocol, it generates a hash of 256 bits, which is equivalent to 64 hexadecimal digits [99]. To be of viable use in blockchains, a hash function must meet the following criteria [100][101]:

- **Pre-Image Resistance** - The output that is generated by a cryptographic hash function cannot reveal any information about the input data and is partially related to the trapdoor principle.
- **Collision Resistance** - It should be computationally expensive and highly improbable to find two values that hash to the same digest.
- **Avalanche Effect** - A small change in the input should have a significant change in the output of the hash function.
- **Puzzle Friendliness** - Even if one were to know the first 200 bytes, one will not be able to deduce the next 56 bytes (in the case of SHA-256), relating to unpredictability.
- **Deterministic** - A hash function should always generate the same (hash) digest whenever the same input is provided.

In order for someone to find a hash collision in SHA-256 with traditional computing, it would require them to check 2^{256} combinations, which is a 78-digit number, making it an infeasible tasks. With the introduction of Grover's algorithm, the number of $O(n)$ steps reduces to $O(\sqrt{n})$ steps, resulting in 2^{128} combinations. However, with the introduction of the BHT algorithm [65], which uses Grover's algorithm and combines it with the birthday paradox, one could potentially further reduce the required steps to $O(\sqrt[3]{n})$ steps, resulting in 2^{85} combinations. Meaning, a hash function subjected to a potential quantum attack is only as secure as a hash function with one third as many bits subjected to an attack from classical computing. Accordingly, the following table has been constructed to provide an overview on the pre- and post-quantum security levels of the most prominent hash functions [102][103][8] that are used in blockchain:

Table 4.1: Security Levels of Algorithms used in Blockchain Pre- and Post-Quantum

Algorithm	**Pre-Q Security Level**	**Post-Q Security Level (=1/2 Digest Length)**	**Post-Q Security Level (=1/3 Digest Length)**
SHA-256	256 bits	128 bits	85 bits
Scrypt	256 bits	128 bits	85 bits
Keccak-256, Keccak-512	256/512 bits	128/256 bits	85/170 bits
RIPEMD160	160 bits	80 bits	53 bits

In a PoW-based blockchain, the immutability of transactions are enforced through hash functions, as each block in the chain stores the respective hash of the previous block [104]. The principal threat of Grover's algorithm is function inversion, allowing the generation of a pre-image from a given hash in a more efficient and accelerated manner. As a result, one could insert a modified block into the chain without disturbing the sequential consistency of the blocks and the integrity of the blockchain [105]. Additionally, in order for a malicious actor to double-spend Bitcoin, which refers to someone altering a blockchain network to spend the same digital token more than once [106], it needs to be able to validate the transactions on the network faster than the rest of the combined blockchain network. Below, a simple demonstration will be provided on how such an attack could take place for Bitcoin:

On average, a new block is mined every 10 minutes for Bitcoin [107]. As of the 7th of November, 2022, the hashrate of BTC was around 273,09 TH/s (273.097.232.383.000.000.000 H/s) [5], meaning, it performed $273 * 10^{18}$ hashes per second, which can be translated to $163 * 10^{21}$ hashes on average per 10 minutes. Therefore, a malicious actor must search a space of $163 * 10^{21}$ hash pre-images within 10 minutes if they wanted to double-spend BTC. A quantum computer would (theoretically) be able to perform this search with Grover's algorithm in $\sqrt{163 * 10^{21}} = 40 * 10^{10}$ time steps. Assuming, optimistically, a quantum machine performing 10^9 operations per second is ready for usage, this search will be performed in less than 7 minutes, thus, allowing the malicious actor to control the network's integrity. In cryptography, one can deduce the security parameter from the number in the exponent of the number of steps one would need to perform an attack [108]. In this case, on the 7th of November, 2022, the Bitcoin network offered approximately 2^{77} bits of security and fell short of the capabilities of a CRQC that can perform 10^9 operations per second, allowing for the hypothetical double-spending.

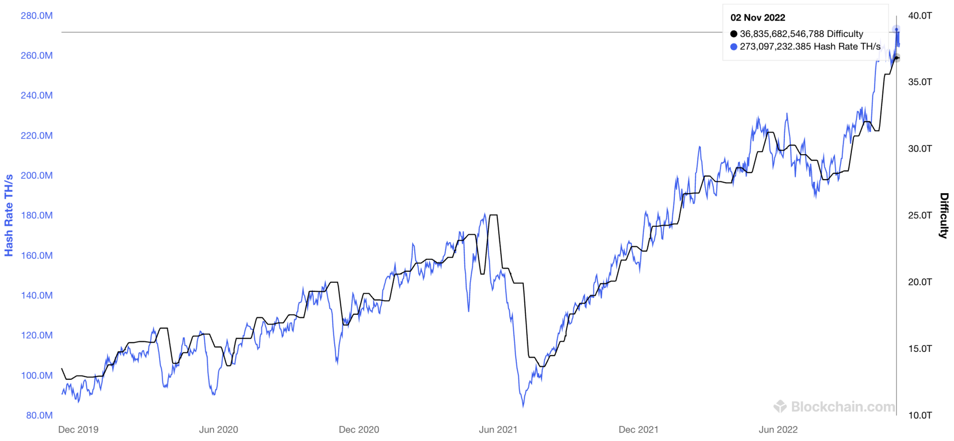


Figure 4.1: The Total Hash Rate in terahashes per second along with a relative measure of network difficulty [5]

The aim of the example above was to serve as a simple explanation of how a CRQC could potentially enable double-spending of BTC for contextual purposes. In reality, the required calculations are more demanding and complicated. It is also important to note that significant progress has to occur in the quantum space for this CRQC's computational power to become reality [109]. The optimistic estimate of a quantum computer's hash rate is around 13.8 GH/s [110], which is nearly 20.000 times less than today's highest achievable hash rate of 255 TH/s of the ASIC miners [111].

4.2. Mitigation Strategies for Grover's Algorithm for Blockchain

Considering the fact that blockchains are intended to provide an immutable permanent record, it is of great importance that the security levels for hash algorithms are of sufficient level for when a CRQC might arise. To recap, there are two ways Grover's algorithm can be used to attack the blockchain:

1. Search and find hash collisions to replace blocks of a chain without disturbing the sequential consistency of the blocks and the integrity of the blockchain.
2. Accelerate mining in PoW and generate additional blocks on the chain, potentially resulting in a recreation of the entire blockchain, since the longest chain is (generally) accepted to be true, allowing someone to rewrite history (51% attack).

In regard to point 1, it is understood that for a hash of length k bits, Grover's algorithm allows for a significant speedup by a factor of $2^{k/2}$, whereas some claim that this speedup could increase to $2^{k/3}$ [112]. Meaning, if a certain level of difficulty is required for blockchain's security, a quantum resistant standard should (in theory) require at least twice the hash length of the current required lengths of classical algorithms. Consequently, SHA-256 would only offer 85 bits of security against hash collisions, making it unsuitable for use in which security is based on hash collision resistance. Therefore, it would be recommended for blockchain to consider using hash algorithms with (at least) 384-bit digests [103]. In regard to point 2, the level of security is related to the computationally difficult process of signing a block by, for instance, finding a nonce in which the first m bits of the block's hash are zero's. Other smaller blockchain networks with less hashing power will be vulnerable sooner than the Bitcoin network. As for point 1, increasing the hash length k was a proposition. Here, one could also propose to increase the length m that is required for signing a block, however, that would make it also twice as hard for classical devices to sign a data block. This highlights the trade-off between system requirements and protecting the blockchain protocol against attacks from quantum devices [80].

Researchers have proposed to migrate to alternative forms of PoW that offer less of a quantum advantage. Momentum [113], a memory-hard PoW based on finding birthday collisions, will supposedly result in the running time of a quantum algorithm to be only two-thirds of the running time of a regular algorithm, instead of the quadratic advantage it could posses with the current state of PoW [110]. Similarly, Lattice-Based PoW [114] has been designed to tackle the quantum threat for PoW by reducing the quantum advantage. However, in both cases, they are not quantum-secure alternatives to hashing for PoW, as they ”only” reduce the level of advantage a quantum adversary might hold and not level the playing field. As PoW requires a mathematical problem that is hard solve, but easy to verify, quantum search algorithms will always provide advantage over classic ones and makes it very unlikely for a quantum-resistant PoW consensus mechanisms to be designed [6]. Taking this into account, one can state that quantum computers provide an *asymptotic efficiency increase* for PoW systems. So, does this mean that blockchains that utilize PoW now and in the future will be rendered obsolete once a CRQC arrives?

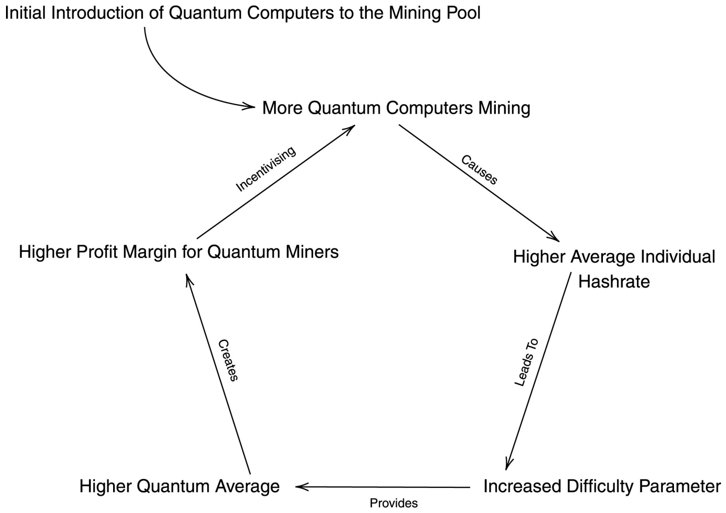

Initial Introduction of Quantum Computers to the Mining Pool
More Quantum Computers Mining
Causes
Higher Average Individual Hashrate
Leads To
Increased Difficulty Parameter
Provides
Higher Quantum Average
Creates
Higher Profit Margin for Quantum Miners
Incentivising

Figure 4.2: Self-propagating cycle of increasing quantum advantage on PoW networks [6]

So, a quantum computer attack would only successfully achieve its objective if a sizeable portion of cryptocurrency miners did not move to quantum hardware, protecting the network from a 51% attack. One might wonder how likely it is for this to happen. It has to be made clear that the quantum computers that the miners would utilize would not have to be more powerful than an entire network, but only more efficient than a single classical miner. These types of quantum computers will be available before the introduction of a CRQC that is capable of conducting a 51% attack, thus, researchers expect that quantum supremacy in cryptocurrency mining will be achieved sooner than a 51% attack [6]. This is further explained by a cascading vicious cycle for the introduction of quantum computers to a PoW based blockchain network, see Figure 6.2, in which it is discussed how quantum miners will increase the network's hash-rate, thus influencing its difficulty parameter, which in return should result in more quantum miners for a PoW-based blockchain, as it would be more profitable to do so. If the running costs of a quantum computer, along with the initial costs of setting it up is too high, some miners could also opt to make use of cloud-based quantum computing services [115], such as blind quantum computations, to use a cloud quantum server for mining in PoW [116]. Meaning, the network could potentially become secure to 51% attacks based on quantum advantage itself. The same researchers predict that over time the increased difficulty of PoW will render classical mining obsolete, and eventually, all mining will be quantum mining, resulting in a new equilibrium of PoW-mining tools.

Alternatively, PoW-based blockchains could move to other consensus mechanisms that do not require solving computationally intensive mathematical problems [117]. One recommendation could be Proof-of-Stake (PoS), as it does not provide a quantum adversary the computational advantage of conducting a 51% attack [118], as the objective of its consensus mechanisms is completely different. Meaning, it would reduce the risk of a 51% attack, as in order to add a new block in PoS, the attacker would have to own more than half of the cryptocurrency. However, during the asset creation mechanisms of PoS, the staking transaction itself is vulnerable to a quantum attack, putting the 'stakers' at risk of losing their assets by participation [119].

4.3. Shor's Algorithm and Blockchain's operations

Public and private keys are an integral part of cryptocurrencies. They are a part of public-key cryptography (PKC), which validates the authenticity of data using asymmetric encryption. In traditional computing, this technology is used to encrypt and decrypt messages, whereas for cryptocurrencies, it is used to encrypt and decrypt transactions. A public key can be used to receive cryptocurrencies and can be shared publicly. Each public key has its own unique private key, which provides the owner the ability to prove ownership and spend the funds that are associated with that public key [120]. A private key, which should never be shared with the public, can take many different forms [121]:

- 256 character long binary code
- 64 digit hexadecimal code
- QR code
- Mnemonic phrase, or seed phrase

There is one more element that is of great importance. In order to spend a cryptocurrency, one must prove ownership of the private key that is paired with the associated public key. However, this must be done without having to reveal the private key, otherwise it loses its purpose. This is where digital signatures come in play. In the original Bitcoin white paper [71], Satoshi Nakamoto defined a (cryptocurrency)coin as a *"chain of digital signatures"*. They are used to prove that someone knows the private key that is connected to the public key, without having them reveal the actual private key [122].

If someone wants to send Bitcoin, their wallet creates a transaction message that contains the number of Bitcoins that they wish to transfer and the recipient's address. This transaction message is then run through a hash function (Section 4.1) and produces an output, i.e. the (message) hash, which in turn is encrypted with that person's private key. Meaning, at the end of this process, the wallet has created two "items": (1) the transaction message, and (2) the digital signature, which is the encrypted hash of the transaction message. Because of this, every digital signature is unique and cannot be used for other transactions, as it is not only the private key that is used to create a digital signature, but also the hash of the transaction message. Now, when that person wants to initiate a Bitcoin transaction, their wallet will provide the Bitcoin network with the aforementioned two "items", along with their public key (address where the Bitcoins are stored). Accordingly, the nodes will take the transaction message and run it through the same hash function. As for the digital signature, they will use the public key to decrypt it, and since the private/public key pair are mathematically linked, one should be able to decrypt it with the public key. If both the hashes are an exact match, it provides proof that the owner of the funds wishes to send an X amount of Bitcoin to a specific address [7].

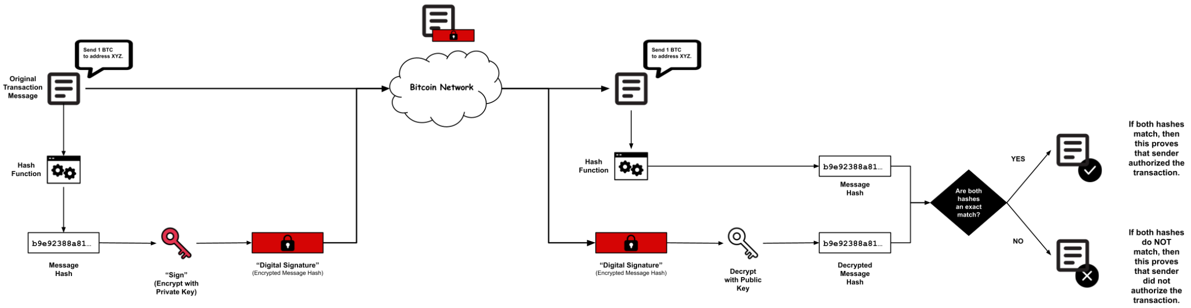

Send 1 BTC to address XYZ.
Original Transaction Message
Hash Function
b9e92388a81...
Message Hash
"Sign" (Encrypt with Private Key)
"Digital Signature" (Encrypted Message Hash)
Bitcoin Network
Send 1 BTC to address XYZ.
Hash Function
b9e92388a81...
Message Hash
"Digital Signature" (Encrypted Message Hash)
Decrypt with Public Key
b9e92388a81...
Decrypted Message Hash
Are both hashes an exact match?
YES
NO
If both hashes match, then this proves that sender authorized the transaction.
If both hashes do NOT match, then this proves that sender did not authorize the transaction.

Figure 4.3: How digital signatures are used to verify coin ownership [7]

Without digital signatures, anyone can write anything on the blockchain, e.g. claim to have send or received an X amount of cryptocurrencies. Therefore, in all blockchain networks, a transaction must be signed by the owner of a wallet before the blockchain can accept it. In short, a digital signature system allows someone to generate their own private/public key pair, in which the private key is used to generate digital signatures that prove that someone is the owner of the public key without having to reveal the associated private key [81]. The majority of cryptocurrencies make use of the ECDSA for their digital signature system [123]. For classical computers, breaking ECDSA is exponentially difficult to solve. However, as discussed in Section 2.1.4, the ECDLP is vulnerable to Shor's algorithm, as it can solve the problem in logarithmic time. There are also other digital signature systems used in cryptocurrencies (EdDSA, RSA, (EC-)Schnorr), but as they also rely on the factoring and discrete logarithm problem that Shor's algorithm can solve, they are all deemed as quantum vulnerable signing algorithms [124]. This means that the authenticity of the digital signature schemes can be compromised with a CRQC, as it will be able to efficiently compute the private key that is associated with the public key. Accordingly, the following threats could emerge in the form of storage and transit attacks [3] [125]:

- **Reused addresses** - by sending a transaction you reveal the public key that is associated with the address, allowing an attacker to receive your private key, take over the account and siphon all funds to another account.
- **Abandoned assets** - if the associated addresses were generated without hashing, public keys of older addresses would be exposed, putting the respective funds at risk prior to 2012 for Bitcoin.
- **In-flight transactions** - once a transaction is broadcasted to the network, an attacker could recover the private key during peak activity, i.e. congested networks, and sign another transaction to transfer the assets to another address before the original (legitimate) transaction is executed.
- **Transaction failure** - a signed transaction does not go through due to low fees or a script failure during verification, leaving the key vulnerable to attacks.
- **CoinJoin** - combining multiple payments into a single transaction to increase anonymity is also subject to revealing the public keys for malicious actors.

The aforementioned attacks and threats have devastating consequences for blockchain as a whole. It has the potential to render the technology completely useless if no adequate measures will be taken. Furthermore, it will also have disastrous implications from a financial point-of-view, as all the global investments that were ever made by retail and institutional investors will suddenly be close to zero when a CRQC breaks the underlying cryptography of blockchains and funnel all the funds.

4.4. Mitigation Strategies for Shor's Algorithm for Blockchain

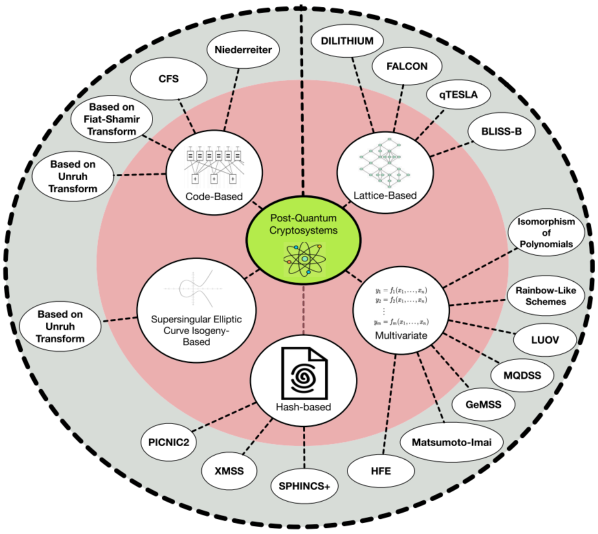

Niederreiter
DILITHIUM
CFS
FALCON
qTESLA
Based on Fiat-Shamir Transform
BLISS-B
Based on Unruh Transform
Code-Based
Lattice-Based
Post-Quantum Cryptosystems
Isomorphism of Polynomials
$y_1 = f_1(x_1, \ldots, x_n)$
$y_2 = f_2(x_1, \ldots, x_n)$
$y_m = f_m(x_1, \ldots, x_n)$
Rainbow-Like Schemes
Based on Unruh Transform
Supersingular Elliptic Curve Isogeny-Based
Multivariate
LUOV
MQDSS
Hash-based
GeMSS
PICNIC2
Matsumoto-Imai
XMSS
HFE
SPHINCS+

Figure 4.4: Post-quantum public-key cryptosystem taxonomy and main practical implementations [8]

There are a wide variety of different (types) of post-quantum cryptosystem. Figure 5.7 provides a great overview of the most prominent algorithms that could potentially be adopted to achieve quantum security [8]. One can conclude that post-quantum cryptography is much more than just one cryptography type and has many (competing) cryptosystems that each possess unique operations with distinguishable features. It is of great importance that the details of new algorithms and cryptosystems are public for analysis and thoroughly tested. This relates to one of Kerckhoffs's principles of modern cryptography, which states that a cryptography method must be secure even though its intricate details are known [126]. In terms of quantum-resistant cryptography, the area was considered to be relatively new with a great deal of uncertainty and no accepted standards. Accordingly, in 2017, the United States Congress enacted a federal law known as the American Innovation and Competitiveness Act (AICA) and tasked the National Institute of Standards and Technology (NIST) with researching and identifying quantum-resistant cryptography standards [127]. As the bill was originally introduced to Senate in June 2016, NIST went ahead and launched a formal call for proposals in December 2016 with a deadline for submissions on November 2017 [70]. There are also other organizations that have been looking into this, such as ETSI - a European Standards Organization (ESO), but their efforts are substantially less in this field, making NIST the global leader for (post-quantum) cryptographic standards [19]. The aforementioned program of NIST received 82 submissions, of which 69 satisfied the required conditions [18]. The second round selected 15 algorithms to proceed to the third round: nine Public-Key Encryption/KEMs and six digital signatures. In July 2022, NIST announced four candidate algorithms to be selected for post-quantum cryptography standardization, of which three were digital signatures [15] [16]:

Table 4.2: Overview of the digital signatures that were *3rd Round Finalists, **3rd Round Alternate Candidates and ultimately ***To Be Standardized [8] [15] [16]

Digital Signatures	Cryptosystem	3rd-R F*	3rd-R AC**	TBS***
CRYSTALS-DILITHIUM	Lattice-Based	X		X
FALCON	Lattice-Based	X		X
Rainbow	Multivariate-Based	X		
GeMSS	Multivariate-Based		X	
Picnic	Hash-Based		X	
SPHINCS+	Hash-Based		X	X

For contextual purposes it is worth discussing the different types of quantum-resistant cryptosystems to better understand their unique qualities. Generally speaking, there are five types of quantum-resistant cryptosystems, along with a sixth category that is referred to as *hybrid cryptosystems* (schemes that merge pre- and post-quantum cryptosystems) [8] [128] [129] [130]:

1. Code-Based Cryptosystems: the security is based on coding theory, i.e., the problem of decoding an erroneous codeword that has been produced through an unknown error-correcting code. McEliece's cryptosystem is a great example of this, providing fast encryption and decryption.

However, it also requires storing and performing the operations with large matrices that act as the public and private keys (between 100 kilobytes and several megabytes) [131] [132] [133].

2. Multivariate-Based Cryptosystems: the security is based on the complexity of the process of solving systems of multivariate equations (NP-hard or NP-complete). Due to the "guesswork" involved in the process, it has some limitations in terms of decryption speeds. The process also results in large public keys, with very small signatures. They require thousands of bytes per key, and further research is needed for better decryption speed and reduced key size [134] [135].
3. Lattice-Based Cryptosystems: the security is based on the difficulty of mathematical problems in the field of lattices, such as the Shortest Vector Problem, Closest Vector Problem, Shortest Integer Solution, or the Shortest Independent Vector Problem. It is considered to have reasonably efficient implementations and considerable simplicity with strong security proofs. They can be executed fast due to their computational simplicity, however, it does need to store and make use of large keys and ciphertext overheads [136] [137].
4. Hash-Based Cryptosystems: rather than the security being based on the hardness of a mathematical problem, it is based on the security of the underlying hash function, more specifically, its properties such as pre-image resistance and collision resistance (see Section 4.1). They have minimal implementation complexity, relatively small public/private key size and signatures generally do not tend to exceed 40 kilobytes [138] [139].
5. Supersingular Elliptic Curve Isogeny Cryptosystems: the security relies on the isogeny protocol for ordinary elliptic curves. They have promising key sizes, but they are not very efficient and produce very large signatures. In literature, there are also not that many existing ones due to their "poor" performances [140] [141].
6. Hybrid Cryptosystems: the security relies on merging pre- and post-quantum cryptosystems, but it does requires significant computational resources in order to handle two advanced security systems with large payloads. Additionally, there is also significant energy consumption. Here, there seems to be a trade-off between security, computational complexity and resource consumption [142] [143].

It is important to note that NIST is mostly interested in general-purpose digital signature schemes. Meaning, it does not have specific applications in mind when it comes to its process, such as blockchain. Therefore, additional analysis has to be conducted to determine to what extent the proposed candidate algorithms from Table 4.2 would be feasible for usage on the blockchain by discussing their technical features. However, before comparing these different algorithms, it is important to understand the 'security levels' of these cryptographic modules, ranging from 1 to 5 (see Table 4.3) [17]. In order for a cryptosystem to satisfy one of these levels, an attack must require computational resources that are comparable to or greater than the respective threshold. From Table 4.4 it becomes clear that the higher the level, the higher the security strength becomes. As NIST takes classical and quantum computing into account, it also measures quantum attacks that are restricted to a fixed running time or circuit depth, and refers to this parameter as $MAXDEPTH$, in which the value is 2^X logical gates [18].

Table 4.3: Security Levels of the (to be standardized) digital signature schemes [17]

Digital Signatures	**Security Level**				
	I	II	III	IV	V
CRYSTALS-DILITHIUM		x	x		x
FALCON	x				x
SPHINCS+	x		x		x

Before comparing the three finalists of the NIST standardization program, one final aspect needs to be discussed: parameters and performances. Generally speaking, the public key and signature lengths are the most important parameters for digital signatures in the blockchain context, as they will be stored in some capacity to verify the transactions [110]. Long public keys and signatures result in an increase in hashing time, which can sometimes be comparable to the time spent on signing or verifying a message. Therefore, small key sizes are preferred to reduce the storage required to store private and public keys [144] [145]. For the speed of the key pair generation, signature execution, and verification process,

Table 4.4: NIST requirements for each security level [18]

Level	Description	Search Type	Gate Counts
I	At least as hard to break as AES128	Exhaustive Key Search	$2^{170}/MAXDEPTH$ quantum gates or 2^{143} classical gates
II	At least as hard to break as SHA256	Collision Search	2^{146} classical gates
III	At least as hard to break as AES192	Exhaustive Key Search	$2^{233}/MAXDEPTH$ quantum gates or 2^{207} classical gates
IV	At least as hard to break as SHA384	Collision Search	2^{210} classical gates
V	At least as hard to break as AES256	Exhaustive Key Search	$2^{298}/MAXDEPTH$ quantum gates or 2^{272} classical gates

specialized hardware is used to obtain the cycle counts. These depict the speed of the cryptosystems (the more cycles, the slower the operations) [19].

Taking all of the aforementioned aspects into consideration, a table has been constructed that aims to aid in comparing the three finalists of the NIST standardization program. It is important to note that the performance characteristics of the signature schemes can vary by platform and implementation constraints. Therefore, the values should be taken as an indication only, however, it can provide great guidance for comparing the respective systems in terms of their strengths and weaknesses.

Table 4.5: Parameters and performances *128s-simple, **192s-simple, ***256s-simple [19]

Parameter set		Public Key (bytes)	Signature (bytes)	KeyGen (cycles)	Sign (cycles)	Verify (cycles)
CRYSTALS-DILITHIUM (lattice-based)	II	1 312	2 420	124 000	259 000	118 000
	III	1 952	3 293	256 000	429 000	179 000
	V	2 592	4 595	298 000	539 000	280 000
FALCON (lattice-based)	I	897	666	18 722 000	386 678	82 340
	V	1 793	1 280	63 135 000	789 564	168 498
SPHINCS+ (hash-based)	I*	32	7 856	144 000 000	1 100 000 00	1 190 000
	III**	48	16 224	206 000 000	1 910 000 00	1 650 000
	V***	64	29 792	136 000 000	1 650 000 000	2 560 000

As can be seen from the table above, each set of parameters that relate to the security levels has some level of trade-off between the complexity of the signing and verification process and the resulting size of the final signature. For simplification purposes, the performances of each algorithm have been compared to one another by looking at the lowest level of security. As a result, CRYSTALS-DILITHIUM came on top with the lowest clock cycles for key generation and signing, and relatively low levels for verifying. However, it does have the largest sizes for public keys and signatures among all three finalists. FALCON exhibited great levels of public key and signature size, with great clock cycles of signing and verifying, and can be deemed to be the most promising algorithm for blockchain usage. Out of all three, SPINCS+ has the shortest public key size but does not perform as efficiently as the others for the remaining parameters.

As FALCON's key and signature generation require more resources (gates and RAM) than CRYSTALS-DILITHIUM's and because it has a more complicated design of key and signature generation to ensure secure implementation, CRYSTALS-DILITHIUM was selected to be the primary signature algorithm to be recommended for general usage. FALCON is advised for usages that require smaller signature sizes. As SPHINCS+ relies on the security of the underlying hash function, the security assumption is independent of the ones on which CRYSTALS-DILITHIUM and FALCON are based, resulting in a useful fallback in case of an unforeseen cryptanalytic attack, making it a great backup option [17] [146].

There is one more important aspect that needs to be discussed: NIST’s aforementioned program that was aimed to select algorithms for post-quantum cryptography standardization had excluded one subfamily of hash-based signatures (HBS), namely stateful HBS. HBS schemes can be categorized as stateless and stateful schemes. Stateless HBS, (such as SPHINCS+) do not keep a record of the used key pairs, whereas stateful HBS records the information, which is referred to as the ”state”, after processing every signature [147]. As NIST’s competition was focused on general-purpose algorithms, it concluded that stateful HBS schemes would not be suitable for general usage as they require careful state management that can be difficult to assure [17]. However, for applications where state management would not pose any difficulties, NIST does consider stateful HBS useful [148] [149], in particular, XMSS and LMS (very similar PK and Sig. length) [150]. Stateful HBS schemes, such as XMSS, make use of one-time signature (OTS) schemes [151], whereas Stateless HBS, such as SPINCS+ make use of few-time signatures [152]. Accordingly, stateful HBS tends to result in smaller signatures and favorable performances in comparison to stateless HBS, but they do come at the following costs: signatures that belong to the same public key must be verified in chronological order, no preceding signature may be missing to verify a later signature, and for each missing signature, the corresponding one-time verification key should be added to a later signature. However, these ’requirements’ correspond to the verification method of blocks in a blockchain: chronological verification and transaction order, no intermediate blocks should be missing, and when transactions do not end up on the blockchain, the corresponding verification keys should be added to a later transaction [153]. Meaning, blockchain technology is one of the use cases where stateful HBS can be utilized. Therefore, XMSS should also be taken into consideration.

It is important to note that the PQC space is constantly developing. Most recently, in December 2022, NIST discussed a new algorithm [154] - Hawk (an optimized Falcon implementation) that offers smaller signature sizes and faster signature generation than Falcon [155]. Accordingly, a new table has been constructed that aims to compare the three finalists of NIST’s competitions with XMSS and Hawk512 to provide a more accurate representation of the current state of PQC’s [20] [21].

Table 4.6: Parameters and performances for signing a 59-byte message [20] [21]

Parameter set	**Public Key (bytes)**	**Signature (bytes)**	**Signature Generation (kilocycles)**	**Verification Speed (kilocycles)**
XMSS (stateful hash-based)	64	2 692	4 804	531
HAWK (lattice-based)	1 006	542	118	27
CRYSTALS-DILITHIUM II (lattice-based)	1 312	2 420	224	70
FALCON I (lattice-based)	897	652	459	23
SPHINCS+ I (stateless hash-based)	32	7 856	549 131	659

For blockchain, the most prominent variables are the public key and signature length (as they are stored on the blockchain for every transaction). The larger the size, the larger the transaction and the larger the computing resources that are required to run a (full) node (also, the lower the level of decentralization). Signature generation and verification speed are also very important as they could cause significant delays for a blockchain. The table above provides an overview of how these algorithms perform for these variables when signing a 59-byte message [20]. This is not the most accurate representation of how they would perform on the blockchain, as e.g., Bitcoin has a block size limit of 1MB [156], which is equivalent to 1.000.000 bytes, so the performances would be different. However, how these algorithms compare to one another in terms of ”relative” performance stays the same.

Different authors in the blockchain field have also proposed different types of modifications to current blockchains to mitigate the quantum threat, resulting in a variety of different papers. For example, for Ethereum, one set of researchers explored how one could modify the blockchain with the multivariate-based *Rainbow* cryptosystem [157], whereas others proposed a hybrid-post quantum digital signature scheme that includes *Crystals-Dilithium - Level 2* [158]. Although there was a significant increase in signing and verification time for both scenarios, both papers had successfully demonstrated the feasibility of these schemes. Similarly, for Bitcoin, researchers studied the possibilities of using the digital signature scheme TESLA# [159], XNYSS [160] and BPQS (a modified version of XMSS) [125]. This field is still developing and a great level of scientific discoveries have to be made before one develops and/or determines a set of clear candidates for blockchain adoption with relatively little to no drawbacks, but each paper that contributes to this field is bringing the community closer to this point.

Taking the aforementioned aspects into consideration, one can conclude that none of the current NIST candidates and modified versions of certain digital signature schemes constitute a perfect drop-in replacement for blockchain. The largeness of the key sizes is one of the greatest disadvantages of the current candidates for efficient implementation [128]. They also require larger computational resources with increased processing power, making the schemes less scalable and less practical to be implemented [147]. As of now, the identified post-quantum cryptosystems do not provide, at the same time, small key sizes with short signature/hash sizes, relatively fast execution times, low computational complexity, and low energy consumption [8]. Nevertheless, this is not the end, as NIST has recently issued a new Call for (PQC) Signatures with a submission deadline of June 1, 2023 [161]. The aim of this call is to diversify the signature portfolio with a focus on schemes that have short signatures and fast verification [162], which is great news for blockchain, as those variables are of great importance for its performance, and hence its adoption in the future.

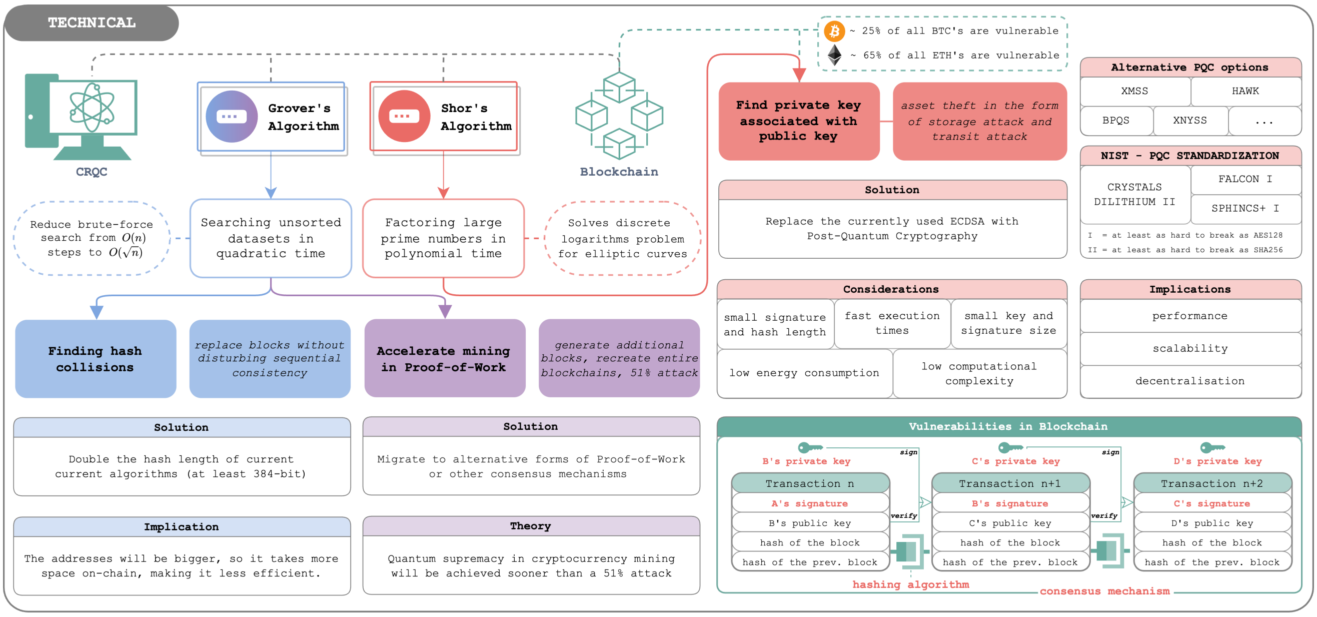

TECHNICAL
CRQC
Grover's Algorithm
Shor's Algorithm
Blockchain
~ 25% of all BTC's are vulnerable
~ 65% of all ETH's are vulnerable
Reduce brute-force search from $O(n)$ steps to $O(\sqrt{n})$
Searching unsorted datasets in quadratic time
Factoring large prime numbers in polynomial time
Solves discrete logarithms problem for elliptic curves
Find private key associated with public key
asset theft in the form of storage attack and transit attack
Solution
Replace the currently used ECDSA with Post-Quantum Cryptography
Alternative PQC options
XMSS
HAWK
BPQS
XNYSS
...
NIST - PQC STANDARDIZATION
CRYSTALS DILITHIUM II
FALCON I
SPHINCS+ I
I = at least as hard to break as AES128
II = at least as hard to break as SHA256
Finding hash collisions
replace blocks without disturbing sequential consistency
Accelerate mining in Proof-of-Work
generate additional blocks, recreate entire blockchains, 51% attack
Considerations
small signature and hash length
fast execution times
small key and signature size
low energy consumption
low computational complexity
Implications
performance
scalability
decentralisation
Solution
Double the hash length of current current algorithms (at least 384-bit)
Solution
Migrate to alternative forms of Proof-of-Work or other consensus mechanisms
Implication
The addresses will be bigger, so it takes more space on-chain, making it less efficient.
Theory
Quantum supremacy in cryptocurrency mining will be achieved sooner than a 51% attack
Vulnerabilities in Blockchain
B's private key
sign
C's private key
sign
D's private key
Transaction n
A's signature
B's public key
hash of the block
hash of the prev. block
verify
Transaction n+1
B's signature
C's public key
hash of the block
hash of the prev. block
verify
Transaction n+2
C's signature
D's public key
hash of the block
hash of the prev. block
hashing algorithm
consensus mechanism

Figure 4.5: Framework that focuses on the technical part of the quantum threat for blockchain

To conclude this chapter, a framework has been constructed to better understand the quantum threat for blockchain. The blue and purple part focuses on the two main threats that accrue from Grover's algorithm, whereas the red part focuses on Shor's algorithm. In the bottom right corner, a simplified visual representation can be found on how a blockchain transaction functions. It aims to highlight (in red) the main vulnerabilities of blockchain in terms of the quantum threat: the hashing algorithm, the cryptography that is related to signing and verifying a transaction, and the overarching consensus mechanism on which blockchains' function. This framework aids to provide people that are not familiar with the effects of the quantum threat on blockchain and possible mitigation strategies with a clear overview of all the relevant aspects, i.e., providing policymakers with a high-level understanding of the technical aspects, rather than keeping them in the dark or overwhelming them with technical details.

5

Meso - Blockchain Governance and Quantum Awareness

This chapter consists of two parts, in which the former will discuss the different ways in which change can be driven in blockchain's (decentralized) governance mechanism and ultimately lead to a list of the most prominent stakeholders, and the latter will analyze the current state of public market maturity surrounding the quantum threat in the blockchain domain. These two parts are required to answer subquestions 2 and 3 of this research. For both parts, the primary tool would be literature analysis, along with investigating case studies. The results of this chapter are crucial for the material that is used for drafting the interviews that will be conducted later in this research, as it highlights the most prominent stakeholders that can drive change, and the current level of quantum awareness in the market.

5.1. Blockchain's Governance and Implementing Change

Blockchain has been referred to by some as "the birth of decentralized governance" [163], but if its governance is decentralized, how does it function and how can one navigate through it accordingly? This section aims to provide a general overview of how blockchain's decentralized governance functions while providing examples on how a change would generally be implemented through the system.

Fundamentally, for blockchain, the source code underlines the software protocol and specifies the implementation and corresponding operations of the blockchain. It can be seen as the blueprint of how a blockchain functions. Its progress relies on a network of globally distributed developers who implement the respective code, and by doing so, distribute the power. Due to the decentralized nature of blockchain, its governance structure is different from conventional governance structures. A set of researchers [164] have defined blockchain governance as: "*the means of achieving the direction, control, and coordination of stakeholders within the context of a given blockchain project to which they jointly contribute*". The same researchers have also constructed a blockchain governance framework for analysis and comparison, which will be used in this dissertation as a reference point. Accordingly, they determined the following 'governance layers' to be prevalent in a blockchain organization:

- Off-chain community: encompasses the governance matters taking place in the real world with a focus on the wider community of a project.
- Off-chain development: encompasses the governance matters taking place in the real world with a focus on the software development process.
- On-chain protocol: encompasses the governance matters taking place on the blockchain through its underlying protocol.

For each of these layers, 5 dimensions of blockchain governance have been identified, and are as follows: (1) *Roles*: formal and informal roles, including responsibilities and to what extent they are held accountable for their actions, (2) *Incentives*: motivational factors for a role specified in the roles dimension, (3) *Membership*: the way participation and membership are managed for the available roles, (4) *Communication*: formal and informal ways of communication between the stakeholders, and (5) *Decision-making*: how decisions are made, monitored, and agreed upon on the three layers of governance. The aforementioned 5 dimensions and 3 governance layers are a great representation of blockchain governance. It underlines the general complexity of this environment, as there are individual stakeholders for each of the three governance layers, with each having varying answers to the 5 dimensions. Now, in order to understand how blockchain could potentially make a transition to a quantum-safe environment, it is of great importance to further investigate this by diving into the aspect of ”decision-making”. For this, the notion of upgradability will be examined, which, in the context of blockchain governance, refers to *the capability of being upgraded in functionality by adding or replacing blockchain components* [165].

However, before continuing down this path, a brief explanation has to be provided on soft and hard forks, and on the topic of nodes. A soft fork can be seen as a rule modification that is ”forward-compatible”, in which the ”old blockchain” can keep accepting new blocks. A hard fork is a ”backward-incompatible” upgrade, causing the primary blockchain network to split [166]. Hard forks require a stronger consensus of nodes and miners, as it often aims to make a change to the original protocol, whereas a soft fork only requires a small section of developers to want to add a small upgrade on a network level [167].

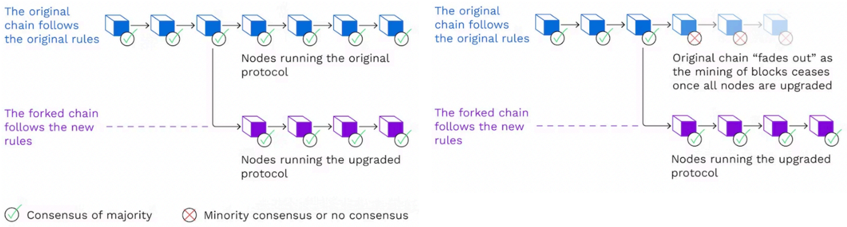

The original chain follows the original rules
Nodes running the original protocol
The forked chain follows the new rules
Nodes running the upgraded protocol
The original chain follows the original rules
Original chain “fades out” as the mining of blocks ceases once all nodes are upgraded
The forked chain follows the new rules
Nodes running the upgraded protocol
Consensus of majority
Minority consensus or no consensus

Figure 5.1: How do hard (left) and soft (right) forks work? [9]

Blockchain nodes are the respective electronic devices that are connected to the network and are the communication endpoints on which the users and/or applications interact. They can be seen as network stakeholders and keep track of the distributed ledger [168]. Depending on the type of node, the functionality and role within a particular blockchain ecosystem change. These are the most prominent types of blockchain nodes [124]:

1. Full nodes: maintaining all the transaction records, while being a part of the governing model in terms of voting.
   (a) Pruned Full nodes: these have a limit of how many blocks can be stored on them. When this limit is reached, old blocks are deleted in order to maintain only the essential metadata and sequence, and then proceed to add new blocks.
   (b) Archival Full nodes:
      i. Authority nodes: provide authorization to other nodes to join the network or can define access to a particular (data) channel for other nodes.
      ii. Miner nodes: are responsible for carrying out the mining process in PoW as a validation method.
      iii. Staking nodes: according to a pre-defined rule, such as time spent on the network of a PoS blockchain by staking, can validate the transactions.
      iv. Masternodes: do not have power to add new blocks, but can maintain the ledger and validate transactions
2. Light nodes: store and provide necessary data to accommodate daily activities.
3. Super nodes: specifically designed to resolve special tasks, like maintaining blockchain rules.
4. Lightning nodes: used to avoid the congestion that could lead to delayed transactions by creating a separate network on which users can push transactions to the main network.

Broadly speaking, according to their particular execution ways, governance models are either mostly off-chain or on-chain. Off-chain governance tends to be more centralized, run slower, and are conservative with gradual improvements [169]. Great examples here are Bitcoin [170] and Ethereum [171], which utilize the improvement proposal model. A Bitcoin Improvement Proposal (BIP) is the primary mechanism for proposing new features, collecting community input, and for documenting Bitcoin design decisions [172]. The BIPs are assigned a status (*draft, deferred, accepted, rejected, withdrawn, final, replaced,* and *active*) and based on their status, make progress. A "proposed" BIP can only change status to "active" if specific criteria "*reflecting real-world adoption has occurred"*. For a soft-fork BIP this requires a miner majority expressed by blockchain voting, e.g. by using BIP 0009 [173], a standard framework for soft forks to the Bitcoin protocol, in which, during a signaling period, 95% of blocks signal their support for the upgrade. This signal comes from the miners, and if this percentage is met (see the example on the right side for the acceptance of the SegWit soft fork in September 2017 [10]), the upgrade will be considered to be locked in. For a hard fork BIP, it requires adoption from the entire Bitcoin economy [174]. If not, a hard fork can occur, but will only take a (small) part of the Bitcoin community with it. As of January 2023, there are a total of 105 Bitcoin forks, of which 31 projects (30% of all Bitcoin forks) are considered to be historic and no longer operational [175].

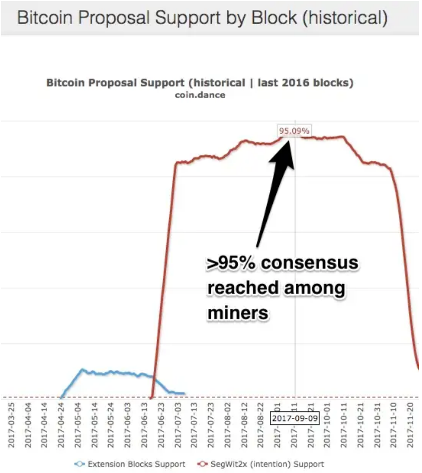


Figure 5.2: Mid September 2017, more than a 95% consensus was reached for Segwit soft fork [10]

For Bitcoin, anyone can submit a BIP, however, as the BIPs can be "censored" by the discretion of the editors, one could argue that they are in control. But, taking the 95% miners' confidence vote into consideration, one could point them out as the ones that are ultimately in control. However, the community (as a whole) can rally behind a different version of the project if a bad actor takes Bitcoin in a poor direction, giving the community control with its activity. Taking all of the aforementioned aspects into consideration, one can understand that the topic of control can be quite complicated. To illustrate this phenomenon further, a tripartite model has been added to showcase the power relationships between different stakeholders [11].

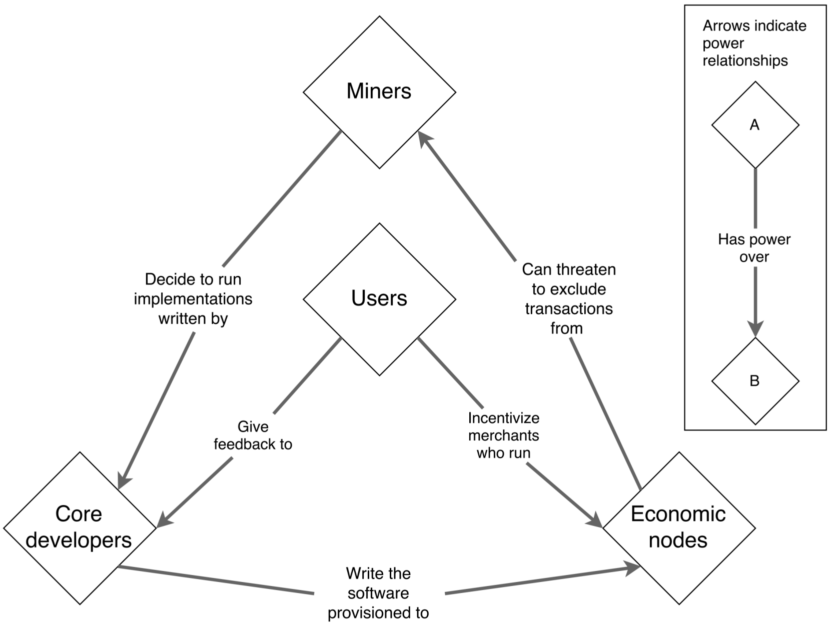

Miners
Users
Core developers
Economic nodes
Decide to run implementations written by
Can threaten to exclude transactions from
Give feedback to
Incentivize merchants who run
Write the software provisioned to
Arrows indicate power relationships
A
Has power over
B

Figure 5.3: A tripartite model depicting Bitcoin's internal power relationships [11]

A crucial point worth considering comes from Bitcoin's BIP GitHub page, stating: *"The BIP Author is responsible for building consensus within the community and documenting dissenting opinions"*, eluding to the fact that the BIP Author is the main person in charge that can potentially drive change by, not only submitting a proposal but also driving the other stakeholders to support it. Ethereum Improvement Proposal (EIP) [171] is based on the BIP and has a similar structure [176]. Meaning, there are different types of EIPs, including core EIPs for low-level protocol changes that affect consensus and require network upgrades. Anyone can propose an EIP and it also moves through similar stages (*draft, review, stagnant, living, last call, withdrawn* and *final)* [177]. These EIPs are debated and vetted by the Ethereum Editors (5 individuals), the Core Dev team, and the community's most active members. However, when it comes to core EIPs that require a hard fork, only the Core Dev Team can implement these changes and make them possible, making it a fairly centralized system to undergo change [178]. However, also very effective, as Ethereum has gone through many different hard forks over the years, in which the last one was referred to as Paris (The Merge) [179] and switched the PoW mining algorithm and associated consensus logic to PoS.

In regard to blockchains that utilize more on-chain models to govern change, they can be deemed to be a more "recent" concept. In this form, changes are possible without the need for hard forks. A consensus to change is typically achieved through voting on the protocol, in which the results are algorithmically managed and their corresponding (automatic) execution is built directly on the protocol [169]. Through doing so, it enables the creation and operation of DAOs (decentralized autonomous organizations) [180]. A great example of a blockchain organization that utilizes (a version) of this on-chain governance is Dfinity [181]. They have provided an integrated governance system in their Network Nervous System (NNS), allowing the community to vote on whether a particular protocol upgrade should be executed or not. Anyone and anyone that has staked their native ICP tokens can vote, and the voting power is based on the number of tokens they hold and the duration for which it is locked. Interestingly, one can also delegate their voting process to follow the votes of other (groups of) people. If the governance system is triggered for an upgrade, the protocol has built-in support for scheduling upgrades, and downloading and applying them without any human intervention [182].

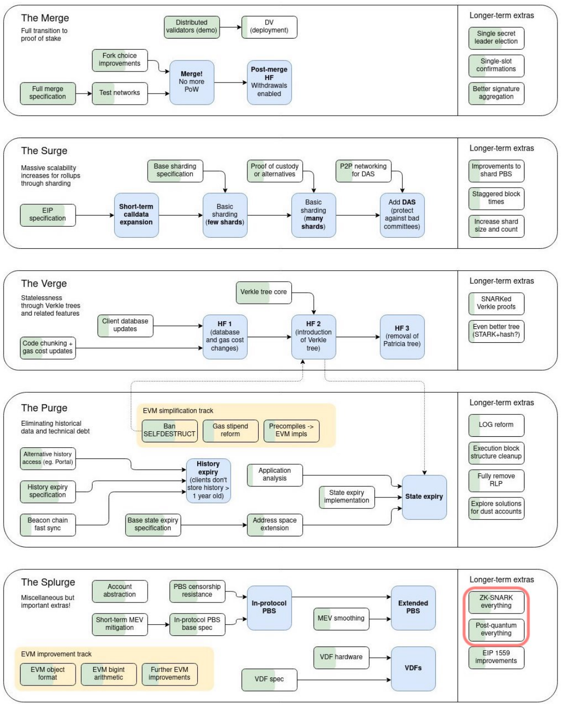

The Merge
Full transition to proof of stake
Distributed validators (demo)
DV (deployment)
Fork choice improvements
Full merge specification
Test networks
Merge! No more PoW
Post-merge HF Withdrawals enabled
Longer-term extras
Single secret leader election
Single-slot confirmations
Better signature aggregation
The Surge
Massive scalability increases for rollups through sharding
Base sharding specification
Proof of custody or alternatives
P2P networking for DAS
EIP specification
Short-term calldata expansion
Basic sharding (few shards)
Basic sharding (many shards)
Add DAS (protect against bad committees)
Longer-term extras
Improvements to shard PBS
Staggered block times
Increase shard size and count
The Verge
Statelessness through Verkle trees and related features
Verkle tree core
Client database updates
Code chunking + gas cost updates
HF 1 (database and gas cost changes)
HF 2 (introduction of Verkle tree)
HF 3 (removal of Patricia tree)
Longer-term extras
SNARKed Verkle proofs
Even better tree (STARK+hash?)
The Purge
Eliminating historical data and technical debt
EVM simplification track
Ban SELFDESTRUCT
Gas stipend reform
Precompiles -> EVM impls
Alternative history access (eg. Portal)
History expiry specification
Beacon chain fast sync
History expiry (clients don't store history > 1 year old)
Application analysis
State expiry implementation
Base state expiry specification
Address space extension
State expiry
Longer-term extras
LOG reform
Execution block structure cleanup
Fully remove RLP
Explore solutions for dust accounts
The Splurge
Miscellaneous but important extras!
Account abstraction
PBS censorship resistance
Short-term MEV mitigation
In-protocol PBS base spec
In-protocol PBS
MEV smoothing
Extended PBS
EVM improvement track
EVM object format
EVM bigint arithmetic
Further EVM improvements
VDF hardware
VDF spec
VDFs
Longer-term extras
ZK-SNARK everything
Post-quantum everything
EIP 1559 improvements

Figure 5.4: Old roadmap diagram of Ethereum [12]

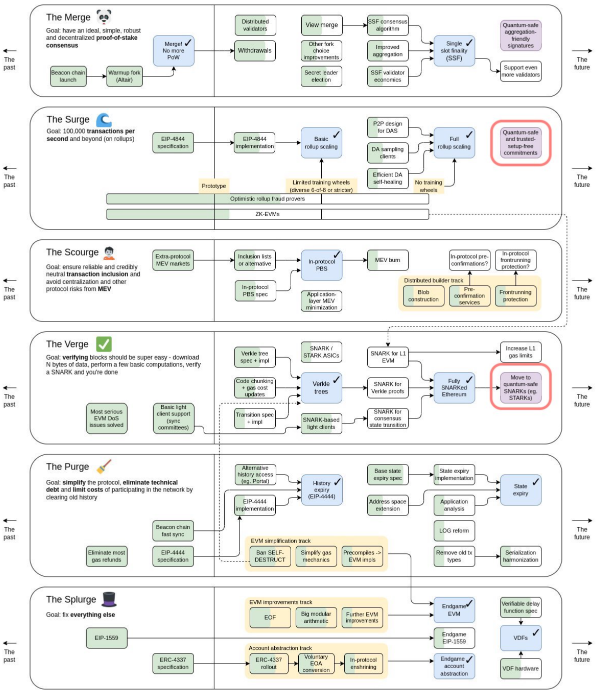

The Merge
Goal: have an ideal, simple, robust and decentralized proof-of-stake consensus
Beacon chain launch
Warmup fork (Altair)
Merge! ✓ No more PoW
Distributed validators
Withdrawals
View merge
Other fork choice improvements
Secret leader election
SSF consensus algorithm
Improved aggregation
SSF validator economics
Single ✓ slot finality (SSF)
Quantum-safe aggregation-friendly signatures
Support even more validators
The Surge
Goal: 100,000 transactions per second and beyond (on rollups)
EIP-4844 specification
EIP-4844 implementation
Basic rollup scaling ✓
P2P design for DAS
DA sampling clients
Efficient DA self-healing
Full rollup scaling ✓
Quantum-safe and trusted-setup-free commitments
Prototype
Limited training wheels (diverse 6-of-8 or stricter)
No training wheels
Optimistic rollup fraud provers
ZK-EVMs
The Scourge
Goal: ensure reliable and credibly neutral transaction inclusion and avoid centralization and other protocol risks from MEV
Extra-protocol MEV markets
Inclusion lists or alternative
In-protocol PBS spec
In-protocol PBS ✓
Application-layer MEV minimization
MEV burn
In-protocol pre-confirmations?
In-protocol frontrunning protection?
Distributed builder track
Blob construction
Pre-confirmation services
Frontrunning protection
The Verge
Goal: verifying blocks should be super easy - download N bytes of data, perform a few basic computations, verify a SNARK and you're done
Most serious EVM DoS issues solved
Basic light client support (sync committees)
Verkle tree spec + impl
Code chunking + gas cost updates
Transition spec + impl
SNARK / STARK ASICs
Verkle trees ✓
SNARK-based light clients
SNARK for L1 EVM
SNARK for Verkle proofs
SNARK for consensus state transition
Fully ✓ SNARKed Ethereum
Increase L1 gas limits
Move to quantum-safe SNARKs (eg. STARKs)
The Purge
Goal: simplify the protocol, eliminate technical debt and limit costs of participating in the network by clearing old history
Eliminate most gas refunds
Beacon chain fast sync
EIP-4444 specification
Alternative history access (eg. Portal)
EIP-4444 implementation
History ✓ expiry (EIP-4444)
EVM simplification track
Ban SELF-DESTRUCT
Simplify gas mechanics
Precompiles -> EVM impls
Base state expiry spec
Address space extension
State expiry implementation
Application analysis
LOG reform
Remove old tx types
Serialization harmonization
State ✓ expiry
The Splurge
Goal: fix everything else
EIP-1559
ERC-4337 specification
EVM improvements track
EOF
Big modular arithmetic
Further EVM improvements
Account abstraction track
ERC-4337 rollout
Voluntary EOA conversion
In-protocol enshrining
Endgame ✓ EVM
Endgame EIP-1559
Endgame ✓ account abstraction
Verifiable delay function spec
VDFs ✓
VDF hardware
The past
The future

Figure 5.5: New roadmap diagram of Ethereum [13]

What is important to note is that these blockchain organizations, depending on their type of governance and forward-thinking approach, have some type of schedule/roadmap for the future. In December 2021, Ethereum's co-founder Vitalik Buterin revealed a roadmap diagram for where the Ethereum protocol development will be heading [12]. This roadmap provided an overview of 5 Ethereum upgrades: Merge, Surge, Verge, Purge and Splurge. The 'final' upgrade, Splurge, encapsulates post-quantum blockchain security with the term *"post-quantum everything"*, but it was not (yet) known when this upgrade will exactly take place. Meaning, the topic of the quantum threat and its consequences were on Ethereum's radar, but there were no plans to mitigate this threat in the near future. However, almost one year later in November 2022, an updated version of this roadmap had been published [13]. This time, the term *"post-quantum everything"* has been changed and divided into two separate areas: (1) *"quantum-safe and trusted setup-free commitments"*, referring to researching a more ideal commitment that is quantum-safe, and (2) *"move to quantum-safe SNARKS (e.g. STARKS)"*, referring to implementing quantum-safe cryptography [183]. It is also important to note that (addressing) the quantum threat used to be on Splurge, which is considered to be an upgrade that focuses on *"everything else"* and has been referred to as the upgrade that incorporates *"miscellaneous but important extras"*.

This means that not only are some blockchain organizations aware of the quantum threat and possible solutions, but they are also preparing for the transition, and are adjusting their roadmap accordingly. However, as section 5 discovered, not every blockchain organization is this prepared, as there are varying degrees of quantum awareness, research and adoption. However, this does show a level of flexibility of blockchain organizations in terms of their planning. Meaning, (important) updates can be prioritized and taken more seriously over time.

Now, this last part aims to conclude this section by providing an overview on the most prominent stakeholders that are involved in the process of upgradability for off-chain and on-chain (governance) models. A research paper has conducted a systematic literature review with 37 primary studies and has composed a list of 18 stakeholders that are involved in blockchain governance [165]. However, one can deduce that there are less stakeholders present when a project is governing upgradability. Therefore, this list has been taken as a reference point, but adjusted accordingly to fit in the scope of this dissertation and the aforementioned elements. As a result, the following list of relevant stakeholders has emerged:

- Core Developers
- Project Foundation
- Community Figureheads
- Block validators
- Full node operators
- Token Holders or Investors

The choice of a blockchain community on whether they should implement a proposed policy upgrade can be seen as a coordination game, in which the governance rules can help the community members to select an equilibrium. This is partially due to the fact that blockchain platforms exhibit network effects, in which the amount of individuals on a chain determine its value. Meaning, a policy update highly depends on what the other individuals on the chain want. Researchers have conducted a strategic chain choice model [184], in which q denoted the fraction of the blockchain community that chose to transact on the upgraded chain. As a result, they have found that coordinating on a single chain is always a Nash equilibrium for the community (no fork). However, a hard fork can be a Nash equilibrium depending on the composition of the community and the specific upgrade that is being proposed. Meaning, if blockchain organizations want to successfully adopt quantum-safe solutions, it means that the respective stakeholders have to be convinced on the benefits of transitioning to a quantum-secure environment in order to increase q.

5.2. Blockchain's Maturity on Quantum Safety - N.A.R.A.Q.

In Chapter 4, the efforts of researchers in implementing post-quantum solutions for blockchain were briefly discussed. This part will expand upon this topic and see to what extent the blockchain community has progressed toward quantum safety in terms of adoption, research, and awareness.

In order to better understand the current landscape of developments within the blockchain community in terms of research and adoption of quantum-safe solutions, the N.A.R.A.Q. framework has been constructed. Each letter of this framework refers to a particular state of an organization in regard to the quantum threat. Taking this framework into consideration, an analysis has been conducted on the top 100 cryptocurrencies, based on their market cap as of January, 2022. Accordingly, each project was assigned a level of maturity from 0 to 3, in which the maturity levels were constructed based on overlapping patterns of projects, and related to the aforementioned N.A.R.A.Q. framework.

- Maturity Level 0 (**N**): there is no mention of the quantum threat, nor have there been discussions on (integrating) quantum-safe solutions, i.e., they are **not** aware
- Maturity Level 1 (**A**): the community is **aware** of the quantum threat, and discussions have taken place on (integrating) quantum-safe solutions.
- Maturity Level 2 (**R**): (academic) **research** has been conducted on quantum-safe solutions by and/or for this particular blockchain on (integrating) quantum-safe solutions.
- Maturity Level 3 (**A**): quantum-safe solutions have been **adopted**.
- Maturity Level 4 (**Q**): the blockchain can be deemed to be fully **quantum-secure**.

In order to conduct this analysis, the following (combination) of keywords were used on Google (Scholar):

(”name” OR ”ticker”) + (”quantum” OR ”post-quantum” OR ”pqc”) + (”blockchain”)

Accordingly, a variety of different sources emerged. These sources ranged from whitepapers, GitHub repositories, and published (academic) research all the way to project websites, Q&A videos, and community forums. The criteria for inclusion was the reliability level of the source, i.e., an (anonymous) comment replying to, or asking, whether project X was aware and/or had plans to adopt quantum-safe solutions was excluded from the analysis. After an extensive search period, all of the top 100 projects were analyzed and put in a spreadsheet. Upon completion, a second check occurred to make sure that the results were accurate for each project. Ultimately, a table has been constructed to showcase the results for each blockchain project and can be found in Appendix A.1, along with the respective sources.

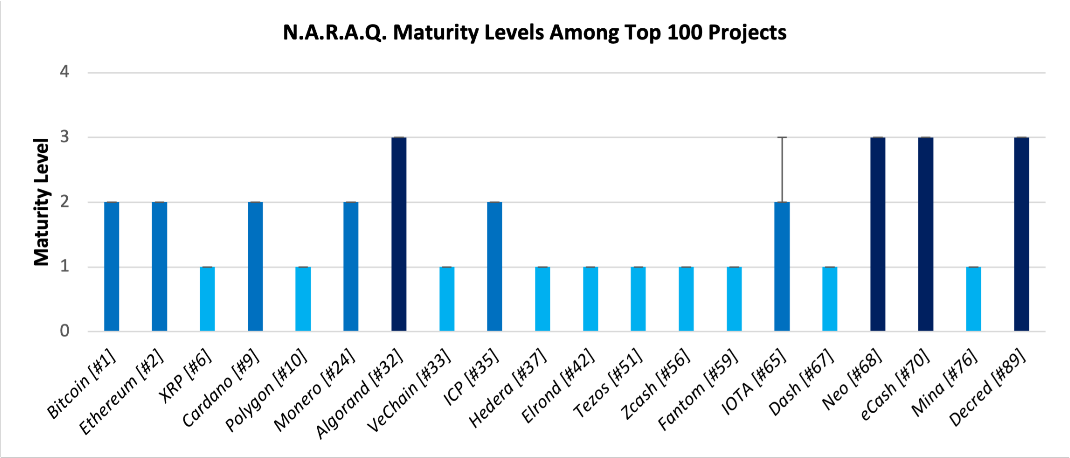


Figure 5.6: Projects that have a maturity level of 1 or higher in the top 100.

Based on this analysis, the following observations have emerged that are important to note:

- From the top 100 projects, 20 were identified with a maturity level of 1 or higher.
- There were 7 *"centralized"* and 5 *"decentralized"* exchanges on this list (i.e. Binance, Bitfinex... and Uniswap, PancakeSwap...) and all of them were identified to have a maturity level of 0.
- There were 10 *"stablecoins"* on this list (i.e. Tether, USD Coin...) and all of them were identified to have a maturity level of 0.
- There were 5 *"privacy coins"* on this list (i.e. Monero, Zcash...), and all of them were identified to have a maturity level of 1 or higher.

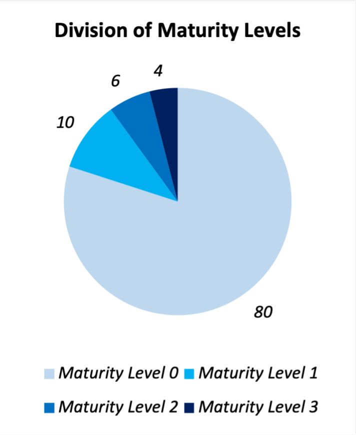


Figure 5.7: A pie chart depicting the division of maturity levels among top 100 projects

One should consider that these findings only relate to the perceived level of awareness and research from these organizations. Meaning, no interviews have been conducted with these blockchain platforms, so it is unknown what they are working on "behind the scene". This analysis only reflects their (portrayed) public "stance". However, generally speaking, taking the nature of blockchain's community and the projects' transparency into consideration, along with the fact that quantum-safe solutions can be a great 'selling point' to retail or institutional investors, it is unlikely that many of these blockchain projects are working on integrating quantum-safe solutions in secret. Side note, it might be the case that for some projects the developer team itself is less active in quantum solutions than (external) academic researchers that have conducted research (indirectly) 'for' them, e.g. Bitcoin. However, as this also constitutes knowledge that can be utilized to adopt quantum-safe solutions, they have also been taken into consideration for the aforementioned analysis.

Nevertheless, the analysis has shown that there is a 20% quantum awareness level among the top 100 projects, and 25% of this constitutes to *"privacy coins"*, which seems reasonable. Their main focus tends to be on ensuring great levels of privacy for their users with advanced levels of security [185], so it should not come as a (big) surprise that they are aware of (potential) future threats, such as quantum algorithms dedicated to breaking (blockchain's) cryptography.

Algorand, which has a maturity level of 4, seems to lead the effort of adopting quantum-safe solutions. John Woods, CTO at the Algorand Foundation, had originally stated that Falcon (see Section 4.4, will roll out across several applications of its blockchain in the future [186]. On the 7th of September 2022, the Algorand protocol upgraded to "State Proofs", an immutable chain of proofs that utilizes Falcon signatures to provide additional security to the network, while obtaining 5x faster performances (from 1200 to 6000 transactions per second (TPS)) [187] [188]. Furthermore, they have also stated that all PoS chains can implement State Proofs to improve their security [189].

eCash (2.0) proudly advertises itself as *"inalienably private and quantum-resistant to counterfeiting"*. During withdrawal transactions, it prepares a message that includes a quantum-secure hash of the spendable form of the respective coin being withdrawn [190] [191]. David Chaum, the inventor of eCash (2.0) and the creator of xx network, and his team have developed a quantum-secure consensus algorithm, known as xxBFT, to underpin all projects and operate under the standard Byzantine Fault Tolerant (BFT) assumption and utilizes WOTS+ signing keys [192]. NeoQS, developed by Neo, has built a cryptographic system that is 'resistant' to quantum computing called NeoQS [193]. It is a lattice-based cryptographic mechanism that relies on the underlying difficulty of quantum computers to solve the Shortest Vector Problem (SVP) and the Closest Vector Problem (CVP) (see Section 4.4), which are considered to be quantum-safe algorithms. Decred released v1.7, adding post-quantum security into its mixing services to provide protection and enhance privacy [194]. Outside the top 100 cryptocurrency projects, there are a small number of blockchains that (proudly) deem themselves to be quantum-secure. Quantum Resistant Ledger (QRL) utilizes XMSS with a one-time signature (OTS) scheme - Winternitz OTS and has quantum security built in from the genesis block [195]. Nexus (NXS) has actually integrated FALCON, and HyperCash (HC), originally known as Hcash, implemented post-quantum Ring Signature algorithms [196] [197]. However, they are not quite popular (yet). As of late December 2022, in terms of market cap, they are respectively ranked as #756, #845, and #943 [198].

An important aspect to note is that IOTA (MIOTA) was long (considered to be) quantum secure as they used Winternitz OTS. However, in April 2021, they relaunched IOTA 1.5, also referred to as Chrysalis, in which they moved away from post-quantum security and adopted the Ed25519 signature scheme for faster transactions and reduced transaction size, which came at the cost of not being quantum secure anymore [199]. This example perfectly underlies the dilemma of post-quantum cryptography in blockchain organizations, security vs performance, along with the (perceived) sense of urgency.

6

Macro - Transitioning Towards a Quantum-Safe Environment

This part discusses to what extent policies and regulations can help blockchain to transition toward a quantum-safe environment, and aids to answer subquestion 4. It will aid to answer subquestion 4 and partially touch upon subquestions 1, 2, and 3. For this section, the input of 30 interviewees (N=30) was used, of which 20 fall within the Blockchain domain and 10 within the Cyber domain. This distinction of domains has been created to highlight potential discrepancies between blockchain experts versus individuals that are (mostly) focused on cyber security with a focus on cryptography. The interviewees will be referred to as BD (Blockchain Domain) interviewees and CD (Cyber/Cryptography Domain) interviewees. It is important to note that the interviewees that were chosen from the CD have a great level of understanding of blockchain technology. A high-level overview of the profiles of the interviewees can be found in Appendix A.2, and the list of questions used in the interview in Appendix A.3.

The interviewees were told that they had to answer the questions based on the assumption that a CRQC will arrive around the year 2030 ±1 year. If no timeline was presented to them, it would have been very challenging to deduct reliable patterns, as the answers of interviewees would differ drastically based on their own (rough) estimate of when they believe the quantum threat will materialize.

This part will mostly focus on the results that accrue from the interview, but the associated findings and observations of these interview results will be integrated throughout the chapter.

6.1. The Quantum Threat

The interviewees were asked to discuss their levels of worry about the effects of the quantum threat materializing, i.e., not being able to implement the necessary solutions in time. This question was asked for (i) large organizations, institutions, and governments (non-BT domain) and for (ii) blockchain-related organizations and cryptocurrency projects (BT domain). They expressed their views as (0) not worried, (1) worried a little, (2) worried, and (3) very worried. The results are as follows:

- For the non-BT domain, 83% of all respondents stated that they were either ”worried” or ”very worried” of the threats of the quantum threat materializing. This number dropped to 43% for the BT domain. Only 13% of the respondents were more worried about the BT domain than the non-BT domain. For the non-BT domain, 17% of the respondent was ”worried a little”, whereas this number was 53% for the BT domain.

The reason for this was mostly attributed to the level of importance the interviewees assigned to traditional organizations versus the ones in the BT domain in terms of their impact, i.e., it would be more devastating for society if the entire banking industry and governmental agencies were exploited as a result of the quantum threat, then if a particular cryptocurrency project went under.

The next question was focused on the top 100 cryptocurrency projects as of January 2023, based on their market cap. They were asked what percentage of the top 100 they believed will be able to transition safely in time toward a quantum-safe environment. After they provided their answers, the focus shifted to the level of quantum awareness of the top 100 cryptocurrency projects being 20% (see Section 5.2). This question was two-fold: (1) do they think this percentage of 20% is low, sufficient, or high, and (2) would they have expected this percentage to be, lower, higher, or around this value? Lastly, this part was concluded by asking whether their perception has changed in terms of what percentage of the top 100 projects they expected to transition safely after knowing the current level of quantum awareness, i.e., have they become more or less optimistic about the blockchain space's future? Disclaimer: This question rests upon the assumption that all projects will be around and active by 2030. The results are as follows:

- Percentage of top 100 projects transitioning towards a quantum-safe environment in time - For the BD, the average and medians were 36% and 30%, respectively. For the CD, the average and medians were 57% and 60%, respectively, indicating a significant difference with the BD.
- Quantum awareness being 20% - For the BD, 50% found the level to be (too) low, whereas this percentage increased to 90% for the CD. In terms of what BD and CD expected, respectively 50% and 70%, expected the level of quantum awareness to be (significantly) higher.
- Perception shift on the percentage of top 100 projects transitioning towards a quantum-safe environment in time, after knowing the level of quantum awareness - For the BD, the average increased by 5%, whereas it decreased by 15% for the CD.

Meaning, initially, people outside of the BD were significantly more optimistic about BT's survival with respect to the upcoming quantum threat than people inside of the BD. However, as the level of quantum awareness was presented to them, this completely flipped. People from the CD became more surprised and alarmed than people inside the BD. Interestingly, they also became more pessimistic about blockchain's future, whereas the level of quantum awareness made people inside of the BD slightly more optimistic about BT's survival.

6.2. Post-Quantum Cryptography

As discussed in Chapter 4.4, NIST launched a formal call for proposals, aimed at selecting post-quantum cryptographic standards. As a result, three digital signature schemes emerged. However, analysis in Chapter 4.4 has shown that none constitute a drop-in replacement for blockchain. This can be partially attributed to the fact that NIST's competition is focused on general-purpose algorithms, and does not take blockchain's specific technical trade-off considerations into account. Accordingly, the interviewees were asked whether they thought it would be great to have some level of ”external institutional technical support” that is more focused on blockchain's specific cryptographic needs, or whether this was a bad idea, i.e., ”blockchain does not need this support” or ”do not mix decentralized with centralized”. Additionally, the question was put forward on whether NIST, or a similar organization, should design an entirely new program for pqc signatures for blockchain or include it in its current program with a subdivision. Lastly, the interviewees were asked on what they generally expect blockchain organizations to do: (1) adopt the existing pqc signatures, (2) adjust the existing pqc signatures accordingly, (3) wait for new cryptosystems, or (4) design their own new cryptosystems. The results are as follows:

- 77% of interviewees had a positive outlook on the blockchain community receiving some level of external technical institutional support for transitioning towards a quantum-safe environment, of which 82% thought it would be a great idea to include BT into the current pqc program of NIST in a more direct manner. However, when asked whether they expected NIST to do such a thing before the year 2030, 78% did not expect this to happen.

- In terms of expectations on what the blockchain domain will generally do in terms of pqc signatures, a majority of 67% believed that they will adjust the existing pqc signatures accordingly, in which the remaining three options were roughly equally distributed over the remains.

People from the BD and CD have both deemed it to be beneficiary if NIST, or a similar organization, were to provide the blockchain space with some level of ”external institutional technical support” in terms of post-quantum cryptography by including blockchain's unique technical tradeoffs in their current program. However, not many expect this to become reality. In terms of what the blockchain space will do in terms of pqc signatures, it is expected that blockchain projects will generally opt for adjusting the existing pqc signatures accordingly to obtain more favorable parameters for their use cases. However, from the interviews it has become apparent that ”individual” project decisions will highly depend on a blockchain's (1) size, (2) character, (3) level of urgency, and (4) SME availability.

6.3. Stakeholders and Driving Change

This part aims to shed light on who people perceive to be the most and least prominent stakeholders to drive change in the blockchain space in terms of transitioning towards a quantum-safe environment. From a list of 7 stakeholders, the interviewees were asked to rank them based on who they believe **should** drive change and who they believe **will** drive change. This distinction was made to highlight any potential discrepancies in terms of the (perceived) level of influence a stakeholder should have, i.e., stakeholder X should drive the change, but in reality, stakeholder Y will drive it. 6 of the 7 stakeholders on this list emerged from the research that was conducted in Chapter 5, and are tied to the blockchain community itself. The 7th stakeholder has been determined to be the regulators/policy experts. Based on the ranking of the stakeholders, points were attributed to the stakeholders. The results are as follows:

- For 93% of the interviewees, there is a difference between who **should** and **will** drive change, showing a level of discrepancy between wanted and expected stakeholder influence on blockchain for transitioning towards a quantum-safe environment.
- For both the BD and CD interviewees, regardless of **should** and **will**, there seems to be a reoccurring pattern for the top three (denoted as light green) drivers for change to be core developers, project foundation, and community figureheads, with a strong emphasis on core developers.
- Based on the results of the BD and CD interviewees, either separate or combined, the top three stakeholders that are least **expected** to drive change are block validators, full node operators, and token holders/investors.
- In regard to the token holders/investors, the BD does not believe that they should be the ones driving the change, nor do they expect this to happen. The CD, on the other hand, does put more emphasis on these stakeholders.
- The biggest stakeholder that has moved places in terms of **should** versus **will** is the ”regulators/policy experts”, (denoted as yellow) as they moved from #7 to #4.

The three biggest stakeholders in terms of driving change for BT have been determined to be: Core Developers, Community Figureheads, and the Project Foundation. As a result, one can conclude that if one aims to achieve meaningful change to transition towards a quantum-safe environment, one should target these three stakeholders. Although token holders/investors have much on the line due to their capital investments, it is believed that they should not drive this change. A similar attitude can be observed for the ”infrastructure providers”, such as block validators and full node operators. Also, generally, people in the BD are less open to regulators and policy experts to lead the change than people in the CD. However, both domains do acknowledge that this stakeholder will play an important role in the future, right behind the top 3 aforementioned stakeholders.

Table 6.1: Ranking of the 7 most prominent stakeholders that can drive change in blockchain's governance structure in terms of interview results: should versus will (BD and CD)

Top 3 that should drive change (BD+CD)			Top 3 that will drive change (BD+CD)		
#1	Core Developers	*174*	**#1**	Core Developers	*172*
#2	Project Foundation	*153*	**#2**	Project Foundation	*154*
#3	Community Figureheads	*152*	**#3**	Community Figureheads	*153*
#4	Full Node Operators	*119*	**#4**	Regulators/Policy Experts	*132*
#5	Token Holders/Investors	*106*	**#5**	Token Holders/Investors	*101*
#6	Block Validators	*105*	**#6**	Full Node Operators	*96*
#7	Regulators/Policy Experts	*104*	**#7**	Block Validators	*95*
Top 3 that should drive change (BD)			Top 3 that will drive change (BD)		
#1	Core Developers	*114*	**#1**	Core Developers	*115*
#2	Project Foundation	*101*	**#2**	Project Foundation	*103*
#3	Community Figureheads	*95*	**#3**	Community Figureheads	*91*
#4	Full Node Operators	*83*	**#4**	Regulators/Policy Experts	*82*
#5	Block Validators	*75*	**#5**	Full Node Operators	*63*
#6	Token Holders/Investors	*69*	**#6**	Block Validators	*62*
#7	Regulators/Policy Experts	*61*	**#7**	Token Holders/Investors	*61*
Top 3 that should drive change (CD)			Top 3 that will drive change (CD)		
#1	Core Developers	*60*	**#1**	Community Figureheads	*62*
#2	Community Figureheads	*57*	**#2**	Core Developers	*57*
#3	Project Foundation	*52*	**#3**	Project Foundation	*51*
#4	Regulators/Policy Experts	*43*	**#4**	Regulators/Policy Experts	*49*
#5	Token Holders/Investors	*37*	**#5**	Token Holders/Investors	*40*
#6	Full Node Operators	*36*	**#6**	Full Node Operators	*33*
#7	Block Validators	*30*	**#7**	Block Validators	*33*

The white paper of the WEF on transitioning towards a quantum-secure economy identified four drivers of change, of which three can be translated for blockchain. As a result, the following three drivers of change for blockchain have emerged:

1. Stakeholders realizing that the quantum threat is approaching and genuinely wanting to protect the network's future - **protection**
2. The (anticipation of) policies and regulations that aim to accelerate the transition towards a quantum-safe environment for blockchain - **compliance**
3. Organizations wanting to differentiate themselves from competitors by (claiming that they are) becoming quantum-safe - **marketing**

The interviewees were asked whether they could rank these drivers for change from 1 to 3, once based on what they think it **should** look like, and once based on what they **expect** it to look like. The drivers of change were awarded points, in which #1 was awarded 3 points, #2 was awarded 2 points, and #3 was awarded 1 point. The higher the points, the greater the driver of change. Results are as follows:

- Across domains, the interviewees believe that the #1 driver of change should be **protection**, however, they expect **marketing** to be the leading driver of change.
- Across domains, people believe that **compliance** should be a higher driver than **marketing**.
- It is expected that **compliance** will play a higher role than **protection**.

Table 6.2: Ranking of the three drivers of change for blockchain to transition towards a quantum-safe environment based on the interview results: should versus expect (BD + CD)

	Should			*Expect*		
	Protection	**Compliance**	**Marketing**	**Protection**	**Compliance**	**Marketing**
BD+CD	90	50	40	54	59	69
BD	60	34	26	38	38	46
CD	30	16	14	16	21	23

Although the interviewees hoped that ”protection” would be the biggest driver of change, they do expect ”marketing” to be the leading driver. Also, due to a lack of regulation surrounding false advertising for BT’s, people prefer ”compliance” over ”marketing”, as they deemed it to be very problematic if organizations would (start to) make all sorts of (partially) false claims surrounding quantum safety.

6.4. Policies and Regulations

To better understand the perceptions of the interviewees on (indirectly) influencing and regulating the blockchain space, the question was asked: ”how welcoming are you of policies and regulations for blockchain and cryptocurrency projects?”. This question was asked to both domains for (1) **general** regulation of the BD, and (2) regulation aimed at accelerating the transition of the BD towards a **quantum-safe environment** in light of the upcoming future quantum threat.

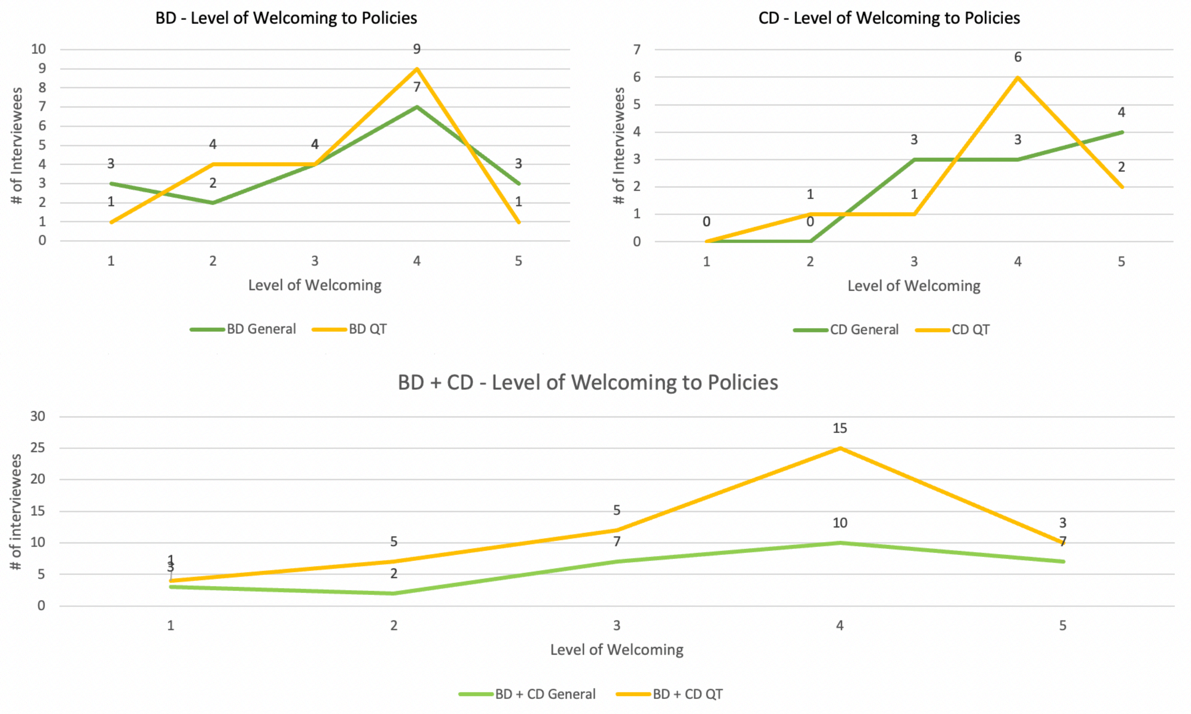


Figure 6.1: How welcoming are the interviewees from the BD and CD on (1) General, and (2) Quantum Threat (QT-related) policies and regulations? 1 = not welcoming at all, 3 = neutral, 5 = very welcoming

- For both domains, QT-related policies are generally welcomed. However, a turning point can be observed between points #4 and #5.
- The BD is slightly less welcoming of general and qt-related policies than the CD.

In general, people tend to be more welcoming of qt-related policies over general policies. However, there was a turning point observed between #4 and #5, as number 5 (very welcoming) was not picked very often. A pattern emerged that showcased how people were hesitant about a regulatory burden that was disguised as market protection with respect to the quantum threat. Meaning, generally, people are welcoming to policies that can aid the blockchain space to transition towards a quantum-safe environment, however, they are skeptical of the level of interference.

Taking this into account, the following proposition was put forward:

"There should be an external organization that audits a blockchain's level of security and provides a stamp of approval of it being quantum secure."

- More than 93% were welcoming of this idea and believed that it would benefit the BT space.
- When asked whether this external organization should be from the public or private sector, more than 76% believed that it should not be tied to a governmental organization, but should be part of the private sector, i.e., a (niche) IT-audit company.

The idea of an external organization auditing a blockchain's level of security and providing a stamp of approval of it being quantum secure is highly welcomed. A vast majority believe that this external organization should be tied to the private sector, and not the public sector.

Additionally, 5 policies were drafted to see where people draw the line in terms of regulating the space to aid in the transition process. These policies were designed with the following protected target group and associated operations in mind:

Table 6.3: Structure of the different groups and corresponding operations for each type of policy recommendation

	#1	#2	#3	#4	#5
Group	Institutions	Institutions	Users	Users	Developers
Operation	Using NQSBT	Investing in NQSBT	Using NQSBT	Investing in NQSBT	Developing NQSBT

1. *By 2030, companies and organizations will no longer be allowed to utilize BT in their operations if they have not been deemed to be quantum secure.*
2. *By 2030, hedge funds, VCs, and any type of institutional investment organizations will no longer be allowed to invest in BT if they have not been deemed to be quantum-secure.*
3. *By 2030, it will be illegal to use BT that has not been deemed to be quantum-secure.*
4. *By 2030, exchanges will no longer be allowed to facilitate the buying and selling of cryptocurrency projects that have not been deemed to be quantum-secure (in light of customer protection).*
5. *By 2030, it will be illegal to develop BT that has not been deemed to be quantum-secure.*

These policies were drafted in accordance with Table 6.3, to better understand to what extent the interviewees want regulations for which specific target group and associated operations.

The results of the respondents to these proposed policies are as follows:

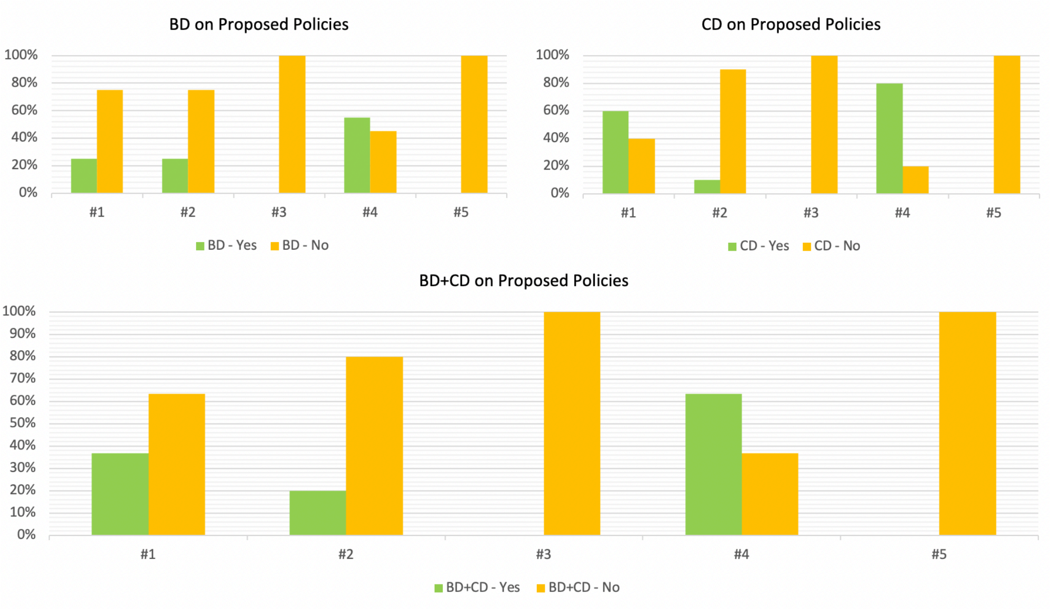


Figure 6.2: Respondent's answer (yes or no) on whether the policies #1, #2, #3, #4, and #5 should be implemented (left top BD, right top CD, bottom BC+CD).

Across domains, policies that aim to restrict the development and usage of NQSBT are not welcomed at all. The interviewees unanimously agreed that this would impede upon one's individual freedom to use whatever technology they want. A similar attitude was observed for the (experimental) freedom that should be provided to developers that want to develop an NQSBT or experiment with cryptography. For policies that aim to regulate the institutions in terms of adopting and investing in NQSBT have gathered mixed feelings, in which the majority opted out. However, a distinction was made for pension funds that risk the money of the citizens, as that should be investigated accordingly. Of all the proposed policies, the one that aimed to protect the retail investors by regulating centralized exchanges in terms of facilitating the buying and selling of NQSBT was welcomed the most.

This chapter has provided meaningful insights into the perceptions and views of interviewees from the BD and CD, where they overlapped, and where they differed. It has answered many questions on how they view the current and future state of the blockchain domain in light of the upcoming quantum threat and has provided valuable information that can aid in designing more accurate and industry-representable policy recommendations. The following chapter will build upon the knowledge that accrues from these findings.

7 Micro Meso Macro - Putting the Pieces Together

Each chapter has played a crucial part in answering the subquestions of this research, but only by putting them all together will the main research question be answered. Taking this into consideration, this chapter aims to provide an overview of different suggestions to implement, a discussion of to what extent the BD should be regulated and provided support for different use-cases and target groups, suggestions to different communities on efforts that can aid the transition, and a brief analysis on the most prominent barriers and obstacles of implementation. The chapter is concluded with a set of final remarks.

7.1. QSSA and N.A.R.A.Q.

From the analysis of the top three drivers of change for blockchain, "marketing" emerged to be the biggest expected driver for BT to transition towards a quantum-safe environment. According to the Federal Trade Commission (FTC), advertisements must be truthful, not misleading, and, when appropriate, backed by scientific evidence [200]. However, as of now, crypto companies can make many unbacked claims. Recently, the U.K. Advertising Standards Authority (ASA) threatened 50 crypto companies with targeted sanctions, as they were concerned with "problematic advertisement" [201]. Accordingly, HM Treasury, UK's department responsible for developing and executing public finance and economic policies [202], has unveiled its plans to crack down on misleading advertisements of cryptocurrencies by subjecting them to rules governed by the Financial Conduct Authority (FCA). It is expected that this will bring ads for crypto assets to the same high standards of financial promotions related to stocks and shares [203]. Putting this in relation to the quantum threat, it is of great importance to have some standard that verifies the claims of a blockchain organization that their protocol is (indeed) quantum-safe. As of now, there is no mention of (the suggestion for) this standard. Taking this into consideration, the Quantum-Secure Stamp of Approval (QSSA) is proposed by the author.

As of now, organizations in the BT domain can make all sorts of claims and there is no one that is investigating to what extent their claims are true and holding them legally accountable. It is problematic when an organization in the BT domain advertises to be quantum-secure, but in reality, they are not (entirely). As of now, this might not seem like a large issue, but once the quantum threat comes closer, it will become more apparent. Therefore, it is very important to have a trusted third-party providing the QSSA to organizations in the BT domain. However, there are a couple of considerations:

- Policy makers, together with cryptography experts and blockchain developers should together define all the necessary requirements for an organization for obtaining a QSSA.

- There must be clarity on what happens if someone were to claim that their protocol is quantum-secure, but have not (yet) obtained the QSSA.
- Define the boundaries on what is included and excluded from the QSSA in terms of peer-reviewed (theoretical) quantum safety, i.e., for post-quantum cryptography will it only include the recommendations of NIST and ETSI, or will it be (much) broader than this?
- Periodic assessments on the developments of BT in relation to the quantum threat, i.e., new (future) exploits appearing with innovative changes in the BD.
- According to the interviewees, a trusted third-party (IT) auditor from the private sector should be in charge of auditing a BT's security, according to 73% of the interviewees.

Part of this research was on discussing the current state of quantum awareness of BT by analyzing the top 100 cryptocurrency projects in terms of their maturity levels. This was done in accordance with the N.A.R.A.Q. framework that was created in Section 5.2. Results have shown that 20% of the top 100 projects were quantum aware and had a maturity level of 1 or higher. This number was considered to be (surprisingly) low by the interviewees and the majority also expected this number to be (significantly) higher. It is of great importance to increase the level of quantum awareness, but it is also important to know the current state of awareness, research, and adoption of quantum-safe solutions. Therefore, the N.A.R.A.Q. framework is proposed.

This framework will allow policymakers to have a better understanding of the current state of the market and will allow them to make informed decisions when designing policy recommendations, i.e., how does the N.A.R.A.Q. framework of 2027 compare to the one in 2023 and is this what we expected? Accordingly, they will have a reference point that can provide them support for discussing to what extent they should intervene and whether it should be in the form of policies and regulations or more on the guidance and support side. Additionally, organizations in the BD, users of this technology, and institutional/retail investors will also benefit from this, as it will provide them with a clear overview of which projects fall within which stage. This framework relates to QSSA, as only organizations that have reached maturity level 4 are awarded that. It is advised to conduct periodic assessments, one in half a year, on the developments of the market and release the results publicly.

There are many additional benefits and use cases, as Crypto exchanges, such as Binance and CoinBase [204, 205], and price-tracking websites, such as CoinMarketCap and CoinGecko [206, 207], can also integrate the results into their services to inform their users of this. If done properly, this framework can be a reference point on the current state of developments in the BD in terms of the quantum threat, guide policymakers into making more informed decisions, put indirect pressure on organizations in the BD to adopt quantum-safe solutions, and ultimately aid in the transition towards a quantum-safe environment.

7.2. Policies and Regulations versus Guidance and Support

From the interviews, it has become clear that the topic of regulating the blockchain space to aid in the transition toward a quantum-safe environment is a very complex and nuanced subject. This part will discuss to what extent policies and regulations should intervene with the BD and what this could look like. Accordingly, an overview has been provided of the most prominent areas of interest.

7.2.1. Investing in NQSBT

There is a substantial difference between the level of due diligence that a hedge fund, VC, and institutional investment makes before investing in a blockchain-related project in comparison to an average retail investor. Therefore, the following aspects must be taken into consideration for policy recommendations that are related to investments in NQSBT:

- It is a conscious risk when VCs are investing in NQSBT. Taking away this right will impede upon institutional freedom of investment. It will also have a counterproductive effect as if you reduce the money that VC's are investing in NQSBT, those projects will also have less money to use for transitioning towards a quantum-safe environment, making it more difficult for NQSBT to become quantum-safe, having a backwards effect on the goal.
- The interviewees' responses indicate that the tipping line is when institutions that are investing capital of the citizens, i.e., a pension fund. They should, at some point in time, not be allowed to invest in NQSBT. Canada's second-largest pension fund, CDPQ, invested over $110 million in the crypto lending firm Celsius, and another Canadian Pension Fund, the Ontario Teachers Pension Fund, invested more than 70$ million in FTX [208]. Unfortunately, both projects went bankrupt [209], and the investors lost all their money. This is something that can and should be prevented in light of the quantum threat and investing in NQSBT.
- Retail investors should be protected from losing their investments. For the EU, the European Securities and Markets Authority (ESMA) is tasked with promoting transparency, simplicity, and fairness for (traditional) consumer financial products and services [210]. As of now, the quantum threat and its consequences (for cryptocurrencies) have not (yet) been discussed by them or similar organizations. The following two methods can help to protect retail investors:
    1. Restrict access: centralized exchanges will no longer be allowed to facilitate the buying and selling of NQSBT. Whether a project classifies as a NQSBT or QSBT can be deduced from the QSSA that was proposed earlier.
    2. Raise awareness: allow the user to make an informed decision when investing in NQSBT. This can be done in two ways:
        (a) Showcase which projects are quantum-secure and which ones are not. This can be done by putting a (non)quantum-secure label or logo next to the project's name and/or ticker.
        (b) When a user wants to trade futures contracts on a centralized exchange, such as Binance, they have to answer a set of questions in the form of a quiz [211]. This assessment tests their level of knowledge on the topic itself and the associated risks. A similar quiz can be created for NQSBT, ensuring that the retail investor is aware of the quantum threat and its associated risks for NQSBT, and makes an informed decision when investing.

7.2.2. Companies and Institutions - BT domain versus non-BT domain

For organizations in the BT domain, the interviewees indicated that they should be free to decide which type of cryptography they adopt, regardless of whether it is quantum-secure or not. However, one can make a separate case for crypto custodians. They provide an infrastructure to store digital assets and can be seen as an intermediary between the owner of an asset and the respective exchange where the asset has been bought [212]. Depending on the country and region, there are different legislations surrounding the legal aspect of crypto custodians. According to the European Central Bank, there is currently no clear harmonized regulatory framework that governs crypto-asset activities and services [213]. Currently, it is mostly country-based, i.e., in Germany, certain crypto custodian activities are subjected to a banking license requirement [214], whereas other countries have more lenient legislation. For future iterations and new versions of regulations for crypto custodians, the QSSA should be considered an important element for the framework of crypto custodians.

For organizations in the non-BT domain, they should also be free to decide which type of technology they adopt for their services, regardless of whether they are quantum-secure or not. However, also here, a separate case can be made for organizations that have a (large) direct societal impact in the form of data management. A line needs to be drawn for organizations that adopt NQSBT to store and transmit sensitive user data. Depending on the legislation, which can range from medical records to Personal Identifiable Data (PID), organizations should be subjected to consequences if they are adopting NQSBT. However, this discussion goes beyond the scope of this research but should be taken into consideration for future policy recommendations.

7.2.3. NIST, ETSI and similar organizations

The blockchain domain can use the technical support of NIST, ETSI, and similar organizations for standardizing post-quantum cryptosystems that take blockchain's specific technical tradeoffs into consideration. Although many interviewees pointed out that this would be great to have, they made it clear that they do not think that NIST will be very preoccupied with whether or not blockchain will transition towards a quantum-safe environment. Whether all blockchain projects will adopt a standard that is provided by NIST really depends on the character of a particular chain, as some tend to be very anti-establishment. Regardless, their support, in the form of dedicating a section of their post-quantum cryptography program to the blockchain domain, will have a positive effect on the technological developments required to initiate a transition to efficient and effective quantum-safe solutions.

An additional suggestion is that there could be an intermediary organization, with a similar nature to NIST and ETSI, that solely focuses on post-quantum solutions for blockchain. However, it would be difficult to obtain funding for this new organization from a governmental perspective, as protecting blockchain is considered by many (interviewees) to not be very high on the governmental priority list of assets/technologies.

According to one interviewee, which is a co-founder of a top 100 cryptocurrency project, a substantial part of the blockchain space is driven by ideology and not the technology itself. One example that they provided was how Bitcoin, and a substantial set of other cryptocurrency projects, had an anti-establishment attitude, and this topic seemed to be a reoccurring theme among different interviewees. Blockchain was born out of the deep mistrust of anything that was government-operated and endorsed since the Great Recession of 2008, and this also included government-endorsed cryptographic algorithms [215]. The distrust relies upon a belief that the NSA (and similar agencies) do not want to lose the ability to access different types of networks and communication channels [216], and when Snowden revealed documents in 2013 that outlined how the NSA had included backdoors in encryption algorithms to allow them privileged access [217], the distrust stuck. Many interviewees in the blockchain and cryptography domain pointed this level of distrust out. Although claiming that NIST will only standardize post-quantum solutions that are publicly unbreakable, but can be broken in secret by the NSA themselves can be deemed as an ungrounded conspiracy theory, it should be taken into consideration.

If external institutional technical support for blockchain to transition towards a quantum-safe environment can be deemed as a good thing, which the overwhelming majority of interviewees did, there should be efforts on building (more) trust with this community, as exclusion and separation will not help with rebuilding this trust. If the future is shaped together, the relevant actors must trust each other accordingly.

7.2.4. Blockchain Community and Stakeholders

The interviewees in this research do not expect that block validators, node operators, and users/investors will be the ones to drive change towards a quantum-safe environment, as they are only making use of the infrastructure by either using the technology or investing in it. It is the core developers, project foundations, and community figureheads that should be driving this change forward. Core developers are the core drivers behind this transition, as they will be the ones adjusting/designing and implementing the respective changes. Community figureheads are very influential people. People flock to these types of personalities when there is a disagreement or uncertainty, and typically, they are the ones that are responsible for discussing the topic openly, and most people make up their minds based on their views. They should be more open on this topic and lead the discussion. Project foundations should be leading the coordination of the transition and should provide clarity on the roadmap.

It is very important for these stakeholders to be more heavily involved in NIST's work. The program has been going on for nearly 5 years, and only now organizations in the non-BT domain are chipping with their views to shape the future of this program more in accordance with their needs. For the BT domain, this is missing. Voice your needs, be actively involved in the community, and participate in discussions more openly. Also, it would be very beneficiary if these three stakeholders from the largest chains would work together to lead the way. This can be done by hosting events and panels on this topic, cross-collaboration or jointly creating and funding a new organization that solely focuses on this threat and the associated technical solutions. The smaller chains do not have the SMEs and ”luxury” to investigate this manner, therefore, this burden lies on the larger chains to solve. As an example, the Payment Card Industry Data Security Standard (PCI DSS) refers to a set of security standards that date back to 2004. It was a joint effort of Visa, Mastercard, and American Express, among many others, to design a framework to secure credit/debit card transactions against data theft and fraud [218]. Although PCI SSC had no legal standing in terms of compliance, it was very beneficiary for a set of best practices existing and it helped the industry to grow together. Fostering this type of collaboration in the blockchain community in terms of quantum safety would be very beneficial for the entire domain.

The National Cybersecurity Center of Excellence (NCCoE), which is a part of NIST, is a collaborative hub where industry organizations, government agencies and academics come together to address cybersecurity challenges [219]. They have recently created a new project called ”Migration to Post-Quantum Cryptography”, as they aim to develop white papers, playbooks, demonstrations, and practical tools to help other organizations with implementing their conversions to pqc [220]. This consortium started with 12 partners, and has now grown to 18. Although this was not designed for blockchain specifically, it would have been great to have at least one member of the BD present. Perhaps a similar consortium can be set up for the BD.

7.3. Barriers and Obstacles

Having conducted an hour-long interview with 30 industry experts, ranging from blockchain project co-founders, CEOs, CTOs, and project leads to cybersecurity experts and (post-quantum) cryptography designers, the interviewees provided a variety of different inputs in terms of the barriers and obstacles that they see in front of the blockchain space to transition safely and in time towards a quantum-safe environment. This part will briefly discuss these barriers and obstacles.

7.3.1. Awareness and Understanding

There is a very low level of (public) quantum awareness in the BD. Drive more education in the market. This topic, and its devastating consequences, have been flying under the radar for a very long time. As the interviewees pointed out, the current level of publicly portrayed quantum awareness being 20% is very low, and considering that only 10% have published research on this manner and only 4% have adopted some level of quantum-safe solutions, there is a long way to go in terms of awareness. Therefore, find great mediums to spread the message to the target audience. The threat is also misunderstood or downplayed based partially due to its high-level complexity. Most of the time when the topic is discussed, it is on an advanced level. Make it understandable for an average policymaker and user/investor.

7.3.2. Timeline and Lead Time

Communicate the adjustments to existing policies and the arrival of future ones in advance, otherwise, you will put a lot of pressure on development teams to adopt quantum-safe solutions, and some might not be able to handle this appropriately in a short time frame. However, it is unsure when the quantum threat will actually materialize, making communicating in advance challenging. Therefore, it is highly recommended to keep a close eye on the developments of quantum computers and start (within a couple of years) designing predictive models on when the quantum threat could potentially materialize based on the technological developments in this field. This way, one can provide more clarity on the timeline, and organizations (in the BT domain) can prepare accordingly.

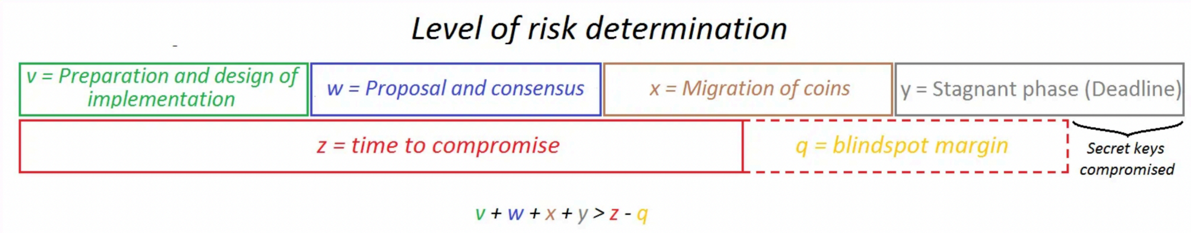

Level of risk determination
v = Preparation and design of implementation
w = Proposal and consensus
x = Migration of coins
y = Stagnant phase (Deadline)
z = time to compromise
q = blindspot margin
Secret keys compromised
v + w + x + y > z - q

Figure 7.1: Adjusted version of Mosca's theorem of risk determination for blockchain [14]

Timeline clarity goes hand in hand with lead time. The time associated with a successful transition toward a quantum-safe environment should not be underestimated. SMEs in this field have made it clear during this interview that the transition for most chains will be much more than a couple of months. Below, an adjusted version of Mosca's theorem of risk determination can be found that is relevant to blockchain's transition to quantum safety [14].

7.3.3. Consensus and Clear Transition Plan

Governance that is skewed towards profit maximization will postpone the transition as much as it can, and stakeholders need to be made more aware of the seriousness of the threat. Also, public permissionless blockchains tend to gravitate towards no change, i.e. when in doubt, do not change anything. Although, ultimately, it is expected that consensus will be reached on making, i.e., Bitcoin, quantum-resistant, the choice in method related to the type of signature, along with the method of implementation will result in varying opinions. Also, reaching consensus on the moment of implementation is another factor that needs to be taken into consideration. Therefore, there need to be best practices for blockchain organizations to effectively drive change in anti-change-oriented environments. These should include technical considerations. Quantum-safe solutions are not as good as regular solutions (yet). However, improvements are being made and future developments in cryptography could take blockchain unique technical tradeoffs (see Section4.2) into consideration. It should also include a roadmap for reaching a consensus with a designated buffer period for uncertainty.

7.3.4. Funding and Priority

Develop and/or invest in a set of think tanks that aim to help the blockchain space to transition toward a quantum-safe environment, or at the very least, engage in the conversation of required funding. Blockchain technology is reaching more parts of society and organizations, yet its level of quantum security is low on the priority list, especially in the eyes of governmental institutions. In order for this technology to survive on the long term, an institutional shift in priority needs to happen from ”performance” to ”cybersecurity” in light of the quantum threat. Policymakers should aim to reach out to the top three stakeholders of large chains, initiate discussions, and learn from one another how to drive change in this field as effectively and efficiently as possible.

7.4. Final Remarks and Considerations

Providing guidance to the blockchain community on the best practices of transitioning towards a quantum-safe environment is a must. It does not have to be binding, but at the very least, there should be a reference point for doing this. In the grand scheme of things, one should mostly focus on driving change for the larger chains, rather than focusing on the smaller ones. It also does not make sense, apart from a marketing perspective, for smaller chains to start the transition now if the larger ones remain stagnant. Need drives adoption, and if blockchain organizations do not see the need to transition, they will remain stagnant in their quantum-safe developments. The beauty of blockchain's ecosystem is that once something starts to work and people realize that it is a great alternative, it spreads like wildfire, leading people to adopt the ”winning strategy”. Larger chains should lead the example, and it is expected that smaller chains will follow, as quantum-safe solutions will ultimately become the status quo. Additionally, larger chains have the ”luxury” of being able to experiment around a variety of different post-quantum solutions, as they have the necessary resources (capital and talent) at their disposal and can ”afford” to (experiment with) start the transition (too) early. Whereas smaller chains are mostly focused on gaining attraction in the form of solving and addressing more short-term issues and goals (scalability, efficiency, interoperability, etc.).

Keep in mind that forcing (blockchain) organizations to transition too quickly can put pressure on the team and potentially lead to adopting bad standards. Therefore, raising the level of awareness as soon as possible, along with a great level of communication in terms of future policies and regulations is crucial. Communicate the new policies and upcoming changes to existing ones in terms of the quantum threat in advance. For large organizations and businesses that are not in the blockchain domain, they can afford to upgrade to post-quantum solutions ”too soon”, as it does not cost a business much to, e.g. upgrade to a heavier signature scheme, but for blockchain upgrading ”too soon” will cost them (comparably) more, as everyone in the network will pay a price for heavier signatures. This distinction between the cost of upgrading should be taken into consideration when looking at the space and discussing its (slow) developments.

Although BT has not yet reached full maturity with significantly high levels of adoption, it was discussed earlier how it is getting adopted by large organizations and how this is expected to increase. BT is no longer an isolated technology and is slowly mingling with other (sets of) technologies, operations, and services in a variety of different industries. Meaning, helping the BD to transition towards a quantum-safe environment will benefit more people than just the ones in the blockchain community. From a game theory and survival perspective, it is inevitable that all chains will adopt post-quantum solutions. The biggest concern is on timely switching in an efficient manner. As of now, many blockchains are either unaware of the problem or (at the very least) ignoring it, as they cannot solve it on their own and have no way of introducing meaningful change with post-quantum solutions without breaking the whole system apart. Therefore, they refuse to change something (now) and rather do nothing. It is expected that more centralized blockchains that have a clear mechanism in place to drive change will be more successful in transitioning towards a quantum-safe environment on the long term.

Also, it is important to note that one cannot distinguish where a digital signature came from. If a CRQC were to exist and be deployed to funnel funds of a user, it will look as though nothing out of the ordinary has happened. Only the person that owns the funds will know that he or she did not initiate this transaction. Therefore, it is very difficult to verify with 100% certainty that a CRQC has indeed stolen funds, unless numerous accounts have been exploited and the advancements of quantum computing elude towards the fact that quantum computers became capable of utilizing Grover's and Shor's algorithm. Another aspect that is (partially) related to this, is that there are many reasons for people to lie about their funds being stolen in the cryptocurrency space, in which the largest reason is tax-related. A user can have a (substantial) amount of money in cryptocurrency tokens and in order to prevent paying (future) taxes, they claim that their funds were stolen by a CRQC, but in reality, they themselves send the funds to a secondary wallet to launder money. These are some elements that have to be considered, as they could impede upon the legitimacy of claims.

8 Discussion

8.1. Conclusion

This MSC thesis aims to provide recommendations that can aid in blockchain's transition towards a quantum-safe environment. As of now, no such recommendations exist. There is no substance that can be used by policymakers to make an adequate decision on how to move forward. The thesis has covered a wide range of key areas and touched upon the Micro, Meso, and Macro elements. Thus, the main research question: "*What type of regulations, policies, and guidelines should be made that can aid the blockchain space to transition towards a quantum-safe environment in time, both from within the blockchain community and from the outside (policy makers)?*" has been answered.

The Micro part resulted in a technical framework, in which the threat of Grover's and Shor's algorithm was explained, the most prominent solutions discussed, along with their corresponding implications, and the necessary considerations in terms of compatibility and performance. Although the separate parts of the technical framework do not add to the existing body of knowledge, the framework and the corresponding text as a whole do. There is not a single paper that outlines the problem, solutions, considerations, consequences, and respective implications in one. All of the information is scattered around and written in a very complex and mathematical manner. If one were to be interested in this topic and was searching for an overview with all the relevant elements, on a micro (technical) level, this chapter has provided just that, as there is no (published) alternative (yet). Furthermore, there is also no overview of the current state of quantum awareness, research, and adoption levels of the cryptocurrency market. Not a single publication. The Meso chapter has filled this gap of knowledge. Furthermore, this chapter has provided an analysis of the different ways that one could potentially drive change in terms of (decentralized) blockchain governance and has selected 6 key stakeholders that can drive change. Lastly, the Macro chapter has provided numerous insights into what the industry experts think on this topic, and from this (in combination with the information gathered in the Micro and Meso part) a variety of different recommendations emerged, in which some were focused on regulations, whereas some were focused on the blockchain community itself and on providing guidance and support.

The research does not contribute to the technical conversation by means of designing a new, or improving upon an existing, post-quantum solution. However, it does provide policymakers with the necessary information to start the discussion and evaluates the current and future state of blockchain technology in light of the quantum threat, and propose recommendations that can aid in the transition. Ultimately, it is the blockchain organizations that have to drive this change, but now, research exists that can aid this domain in moving forward if policymakers wish to help blockchain with this transition.

8.2. Limitations

The timeline of 2030 was taken as an assumption for when the CRQC will emerge. This prediction can be too early or too late, and this uncertainty can influence the outcome of the recommendations, as it is unsure how much time is left. If the timeline were to be more clear, it would be easier to conduct a risk-management approach and change the recommendations into a timely implementation roadmap. Furthermore, an in-depth analysis of the top 100 cryptocurrency projects is missing in terms of the research that is being conducted behind the scenes.

The level of technological developments in this area, and the inability to foresee these future developments can also be attributed as a limitation of this research. As blockchain technology develops, so do the new areas in which the quantum threat could materialize. It could be the case that in the next years, many new applications surge, requiring a new set of quantum-safe solutions and potentially disregarding (parts of) the existing ones, along with the recommendations that were provided. Also, although 30 interviews can be considered to be sufficient to provide an in-depth analysis that can result in generalizable outcomes, a larger sample size would be a greater representation of the blockchain domain, and the results could be generalized to a greater extent.

8.3. Future Research

The following is a set of suggestions for further research (that builds upon this foundation):

A more extensive analysis of the N.A.R.A.Q. framework would be beneficial, in which maturity level 3 is further distinguished. Meaning, an organization has adopted quantum-safe solutions, but to what extent have those made the protocol quantum-safer? It would be great to have a clear overview of which part of the blockchain has been made quantum-safe, and the remaining parts that are not. Also, conducting a gap analysis on the current legislation surrounding blockchain and cryptocurrency would provide more clarity, along with legislation that focuses on cyber-security and analyzes how the future policies on the quantum threat can be positioned, i.e., will it be an extension of GDPR or another legislation, or build upon MiCA, or will it be an entirely new group on its own?

Another topic for further research could encapsulate a step-by-step guide on how one can conduct an IT audit in terms of quantum safety. How should one start this investigation, what are the necessary methods and tools for doing it effectively and what are some key considerations for this audit? It has ben a while since an updated version got published on the current state of exposed funds. Meaning, a 2023 overview of the total combined funds that are at risk, which are categorized based on project and vulnerability type, would help to put this threat more in a financial context. Lastly, technical suggestions on how a blockchain can deal with funds of lost/forgotten/idle wallets, i.e., the funds of Satoshi Nakamoto or someone who did not get the ”memo” of sending their funds to a quantum-safe wallet. Perhaps, building upon a side extension of the N.A.R.A.Q. framework by making a comparison with the top 100 companies in the S&P 500 to provide a better overview of to what extent the level of quantum awareness differs between the non-BT domain and BT-domain

Bibliography

[1] Aljosha Judmayer, Nicholas Stifter, Katharina Krombholz, and Edgar Weippl. History of cryptographic currencies. In *Blocks and Chains*, pages 15–18. Springer, 2017. URL https://link.springer.com/book/10.1007/978-3-031-02352-1.

[2] Itan Barmes and Bram Bosch. Quantum computers and the bitcoin blockchain. *Deloitte*, 2019. URL https://www2.deloitte.com/nl/nl/pages/innovatie/artikelen/quantum-computers-and-thebitcoin-blockchain.html.

[3] Itan Barmes and Bram Bosch. Quantum risk to the ethereum blockchain - a bump in the road or a brick wall?, January 2022. URL https://www2.deloitte.com/nl/nl/pages/risk/articles/quantum-risk-to-the-ethereum-blockchain.html.

[4] Quantum Amsterdam. A professional's guide to quantum technology, May 2022. URL https://www.quantum.amsterdam/part-5-when-can-we-expect-a-useful-quantum-computer-a-closer-look-at-timelines/.

[5] Total hash rate (th/s), November 2022. URL https://www.blockchain.com/explorer/charts/hash-rate.

[6] Dan A Bard, Joseph J Kearney, and Carlos A Perez-Delgado. Quantum advantage on proof of work. *Array*, 15:100225, 2022. URL https://www.sciencedirect.com/science/article/pii/S2590005622000650.

[7] How do digital signatures work?, August 2022. URL https://www.babypips.com/crypto/learn/how-do-digital-signatures-work.

[8] Tiago M Fernandez-Carames and Paula Fraga-Lamas. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE access*, 8: 21091–21116, 2020. URL https://ieeexplore.ieee.org/abstract/document/8967098.

[9] bitpanda. How do hard and soft forks work?, August 2017. URL https://www.bitpanda.com/academy/en/lessons/how-do-hard-and-soft-forks-work/.

[10] Galea Alex. Bitcoin development: who can change the core protocol?, March 2018. URL https://galea.medium.com/bitcoin-development-who-can-change-the-core-protocol-478b8ac5fe43.

[11] Nic Carter. A cross-sectional overview of cryptoasset governance and implications for investors, 2016. URL https://niccarter.info/wp-content/uploads/dissertation_UoE_1617.pdf.

[12] Buterin Vitalik. Happy birthday beacon chain!, December 2021. URL https://twitter.com/VitalikButerin/status/1466411377107558402/photo/1.

[13] Buterin Vitalik. Updated roadmap diagram!, November 2022. URL https://twitter.com/VitalikButerin/status/1588669782471368704?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1588669782471368704%7Ctwgr%5Efeee5af06c24b99f426afec7fb06d1e9139326fc%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fcointelegraph.com%2Fnews%2Fvitalik-reveals-a-new-phase-in-the-ethereum-roadmap-the-scourge.

[14] Walters Allen. An addition to the bitcoin wiki page on quantum computing, June 2019. URL https://medium.com/the-capital/an-addition-to-the-bitcoin-wiki-page-on-quantum-computing-and-moscas-theorem-of-risk-f2345e504bb4.

[15] Computer Security Resource Center. Pqc standardization process: Announcing four candidates to be standardized, plus fourth round candidates, July 2022. URL https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4.

[16] Computer Security Resource Center. Pqc standardization process: Third round candidate announcement, July 2020. URL https://csrc.nist.gov/News/2020/pqc-third-round-candidate-announcement.

[17] Alagic Gorjan, Apon Daniel, Cooper David, Dang Quynh, Dang Thinh, Kelsey John, Lichtinger Jacob, Liu Yi-Kai, Miller Carl, Moody Dustin, Peralta Rene, Perlner Ray, Robinson Angela, and Smith-Tone Daniel. Nist ir 8413 - status report on the third round of the nist post-quantum cryptography standardization process, July 2022. URL https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934458.

[18] Computer Security Resource Center. Security (evaluation criteria), November 2022. URL https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization/evaluation-criteria/security-(evaluation-criteria).

[19] ETSI. Etsi tr 103 616 cyber; quantum-safe signatures, September 2021. URL https://www.etsi.org/deliver/etsi_tr/103600_103699/103616/01.01.01_60/tr_103616v010101p.pdf.

[20] Duc Tri Nguyen and Kris Gaj. Fast falcon signature generation and verification using armv8 neon instructions. 2022. URL https://csrc.nist.gov/csrc/media/Presentations/2022/fast-falcon-signature-generation-and-verification/images-media/session6-nguyen-fast-falcon-signature-pqc2022.pdf.

[21] Nguyen Duc Tri and Gaj Kris. Fast falcon signature generation and verification using armv8 neon instruction, 2022. URL https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/papers/fast-falcon-signature-generation-and-verification-pqc2022.pdf.

[22] Aleksandra Kuzior and Mariya Sira. A bibliometric analysis of blockchain technology research using vosviewer. *Sustainability*, 14(13). URL https://www.mdpi.com/2071-1050/14/13/8206.

[23] Statista. Worldwide spending on blockchain solutions from 2017 to 2024, May 2022. URL https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/#:~:text=Global%20blockchain%20solutions%20spending%202017%2D2024&amp;text=Forecasts%20suggest%20that%20spending%20on,billion%20U.S.%20dollars%20by%202024.

[24] TripleA. Global crypto adoption, 2022. URL https://triple-a.io/crypto-ownership-data/.

[25] Gartner. Blockchain technology: What's ahead? be ready for the next phase of the blockchain revolution, March 2017. URL https://www.gartner.com/en/information-technology/insights/blockchain.

[26] Gartner. Blockchain today and tomorrow: A quick guide, March 2022. URL https://www.gartner.com/en/articles/what-is-blockchain.

[27] Vasileios Mavroeidis, Kamer Vishi, Mateusz D Zych, and Audun Jøsang. The impact of quantum computing on present cryptography. *arXiv preprint arXiv:1804.00200*, 2018. URL https://arxiv.org/abs/1804.00200.

[28] NIST. Nist announces first four quantum-resistant cryptographic algorithms, July 2022. URL https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms.

[29] David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen. Transitioning organizations to post-quantum cryptography. *Nature*, 605(7909):237–243, 2022. URL https://www.nature.com/articles/s41586-022-04623-2.

[30] WEF. Centre for the fourth industrial revolution, 2022. URL https://initiatives.weforum.org/c4ir.

[31] MIT Endicott House. The physics of computation conference, March 2018. URL https://mitendicotthouse.org/physics-computation-conference/.

[32] Feynman Richard P. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467–488, 1982. URL https://link.springer.com/article/10.1007/BF02650179.

[33] 40 years of quantum computing, January 2022. URL https://www.nature.com/articles/s42254-021-00410-6.

[34] Frank Arute, Kunal Arya, Ryan Babbush, Dave Bacon, Joseph C Bardin, Rami Barends, Rupak Biswas, Sergio Boixo, Fernando GSL Brandao, David A Buell, et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, 2019. URL https://www.nature.com/articles/s41586%20019%201666%205.

[35] Pednault Edwin, Gunnels John, Maslov Dmitri, and Gambetta Jay. Quantum computing: On “quantum supremacy”, October 2019. URL https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/.

[36] John Preskill. Quantum computing and the entanglement frontier. *arXiv preprint arXiv:1203.5813*, 2012. URL https://arxiv.org/abs/1203.5813.

[37] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An introduction to quantum computing.* 2006. URL http://mmrc.amss.cas.cn/tlb/201702/W020170224608149125645.pdf.

[38] Lars S Madsen, Fabian Laudenbach, Mohsen Falamarzi Askarani, Fabien Rortais, Trevor Vincent, Jacob FF Bulmer, Filippo M Miatto, Leonhard Neuhaus, Lukas G Helt, Matthew J Collins, et al. Quantum computational advantage with a programmable photonic processor. *Nature*, 606(7912):75–81, 2022. URL https://www.nature.com/articles/s41586-022-04725-x.

[39] Lavoie Jonathan and Vernon Zachary. Beating classical computers with borealis, June 2022. URL https://www.xanadu.ai/blog/beating-classical-computers-with-Borealis.

[40] The quantum decade: A playbook for achieving awareness, readiness, and advantage, June 2021. URL https://www.ibm.com/downloads/cas/J25G35OK.

[41] Bleu Azur Consulting. The big tech in quantum report: How google, microsoft, amazon, ibm, & intel are battling for the future of computing, May 2022. URL https://bleu-azur-consulting.eu/2022/05/28/.

[42] QURECA. Overview on quantum initiatives worldwide – update 2022, March 2022. URL https://qureca.com/overview-on-quantum-initiatives-worldwide-update-2022/.

[43] WEF. State of quantum computing: Building a quantum economy, September 2022. URL https://www3.weforum.org/docs/WEF_State_of_Quantum_Computing_2022.pdf.

[44] NSA. Nsa releases future quantum-resistant (qr) algorithm requirements for national security systems, September 2022. URL https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/.

[45] The White House. National security memorandum on promoting united states leadership in quantum computing while mitigating risks to vulnerable cryptographic systems, May 2022. URL https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

[46] QI. Knowledge base. what is a quantum algorithm?, July 2019. URL https://www.quantum-inspire.com/kbase/what-is-a-quantum-algorithm/.

[47] Ashley Montanaro. Quantum algorithms: an overview. *npj Quantum Information*, 2(1). URL https://www.nature.com/articles/npjqi201523.

[48] Katz Alexander, Williams Christopher, and Wang Tiffany. Public-key cryptography, June 2016. URL https://brilliant.org/wiki/public-key-cryptography/.

[49] Natalia Krzyworzeka. Asymmetric cryptography and trapdoor one-way functions. *Automatyka/Automatics*, 20(2), 2016. URL https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-2e4c1eed-f810-43c7-9936-8570fd67912f.

[50] Berkeley University of California. The science of encryption: prime numbers and mod n arithmetic, September 2002. URL https://math.berkeley.edu/~kpmann/encryption.pdf.

[51] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999. URL https://epubs.siam.org/doi/abs/10.1137/S0036144598347011.

[52] Austin G Fowler, Matteo Mariantoni, John M Martinis, and Andrew N Cleland. Surface codes: Towards practical large-scale quantum computation. *Physical Review A*, 86(3):032324, 2012. URL https://journals.aps.org/pra/abstract/10.1103/PhysRevA.86.032324.

[53] Stephane Beauregard. Circuit for shor's algorithm using 2n+ 3 qubits. *arXiv preprint quant-ph/0205095*, 2002. URL https://arxiv.org/abs/quant-ph/0205095.

[54] Archimedes Pavlidis and Dimitris Gizopoulos. Fast quantum modular exponentiation architecture for shor's factorization algorithm. *arXiv preprint arXiv:1207.0511*, 2012. URL https://arxiv.org/abs/quant-ph/0205095.

[55] Craig Gidney and Martin Ekerå. How to factor 2048 bit rsa integers in 8 hours using 20 million noisy qubits. *Quantum*, 5:433, 2021. URL https://quantum-journal.org/papers/q-2021-04-15-433/.

[56] Jerry Chow, Oliver Dial, and Jay Gambetta. Ibm quantum breaks the 100-qubit processor barrier. *IBM Research Blog*, 2021. URL https://research.ibm.com/blog/127-qubit-quantum-processor-eagle.

[57] Bao Yan, Ziqi Tan, Shijie Wei, Haocong Jiang, Weilong Wang, Hong Wang, Lan Luo, Qianheng Duan, Yiting Liu, Wenhao Shi, et al. Factoring integers with sublinear resources on a superconducting quantum processor. *arXiv preprint arXiv:2212.12372*, 2022. URL https://arxiv.org/abs/2212.12372.

[58] Tardi Carla. What is moore's law and is it still true?, July 2022. URL https://www.investopedia.com/terms/m/mooreslaw.asp#:~:text=Key%20Takeaways,cost%20of%20computers%20is%20halved.&text=Another%20tenet%20of%20Moore's%20Law%20says,growth%20of%20microprocessors%20is%20exponential.

[59] Brown David. Moore's law vs. quantum computing: Is it comparing apples and oranges?, October 2021. URL https://www.electronicproducts.com/moores-law-vs-quantum-computing-is-it-comparing-apples-and-oranges/.

[60] WEF. Transitioning to a quantum-secure economy, September 2022. URL https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf.

[61] Jinyoung Ha, Jonghyun Lee, and Jun Heo. Resource analysis of quantum computing with noisy qubits for shor's factoring algorithms. *Quantum Information Processing*, 21(2):1–19, 2022. URL https://link.springer.com/article/10.1007/s11128-021-03398-1.

[62] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996. URL https://dl.acm.org/doi/pdf/10.1145/237814.237866.

[63] SJ Lomonaco. Grover's quantum search algorithm. In *Proceedings of Symposia in Applied Mathematics*, volume 58, pages 181–192, 2002. URL https://books.google.nl/bookshl=en&lr=&id=nIjHCQAAQBAJ&oi=fnd&pg=PA161&dq=SJ+Lomonaco.+Grover%E2%80%99s+quantum+search+algorithm.+In+Proceedings+of+Symposia+in+Applied+Math+ematics,+volume+58,+pages+181%E2%80%93192,+2002.&ots=KqK7ViRtK7&sig=Q_VYBEHWJ10aU0zwIG6cPPtPugw&redir_esc=y#v=onepage&q&f=false.

[64] Richard Preston. Applying grover's algorithm to hash functions: A software perspective. *arXiv preprint arXiv:2202.10982*, 2022. URL https://ieeexplore.ieee.org/abstract/document/10014648.

[65] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. In *Latin American Symposium on Theoretical Informatics*, pages 163–169. Springer, 1998. URL https://link.springer.com/chapter/10.1007/BFb0054319.

[66] Ghyan Shah, Sneha Padhiar, and Martin Parmar. Introduction to blockchain. 2018. URL https://www.researchgate.net/profile/Ghyan-Shah/publication/351365596_Introduction_to_Blockchain_is_a_stepping_guide_about_what_is_Blockchain_how_it_functi
links/60943a76299bf1ad8d816393/Introduction-to-Blockchain-is-a-stepping-guide-about-what-is-Blockchain-how-it-functions-and-a-basic-implementation-of-Blockchain-using-Python-This-will-give-you-a-basic-understanding-of-how-transac.pdf.

[67] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. Ieee, 2017. URL https://ieeexplore.ieee.org/abstract/document/8029379.

[68] Maoning Wang, Meijiao Duan, and Jianming Zhu. Research on the security criteria of hash functions in the blockchain. In *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, pages 47–55, 2018. URL https://dl.acm.org/doi/abs/10.1145/3205230.3205238.

[69] Xiaochen Zhang, Matias Aranguiz, Duoqi Xu, Xing Zhang, and Xinran Xu. Utilizing blockchain for better enforcement of green finance law and regulations. In *Transforming Climate Finance and Green Investment with Blockchains*, pages 289–301. Elsevier, 2018. URL https://www.sciencedirect.com/science/article/pii/B9780128144473000215.

[70] Mosca Michele and Piani Marco. 2021 quantum threat timeline report, January 2022. URL https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/.

[71] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, page 21260, 2008. URL https://assets.pubpub.org/d8wct41f/31611263538139.pdf.

[72] Phillips Daniel. The bitcoin genesis block: How it all started, February 2021. URL https://decrypt.co/56934/the-bitcoin-genesis-block-how-it-all-started.

[73] Nibley Brian. Bitcoin price history: 2009 - 2022, October 2022. URL https://www.sofi.com/learn/content/bitcoin-price-history/#:~:text=In%20February%20of%202011%2C%20BTC,starting%20price%20of%20about%20%240.30.

[74] Vitalik Buterin et al. A next-generation smart contract and decentralized application platform ethereum. white paper. *Ethereum Project White Paper*, 2014. URL https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[75] Vitalik Buterin. Launching the ether sale, July 2014. URL https://blog.ethereum.org/2014/07/22/launching-the-ether-sale.

[76] wackerow. Introduction to dapps, September 2022. URL https://ethereum.org/en/developers/docs/dapps/#:~:text=A%20smart%20contract%20is%20code,not%20an%20individual%20or%20company.

[77] Rahul Rao Vokerla, Bharanidharan Shanmugam, Sami Azam, Asif Karim, Friso De Boer, Mirjam Jonkman, and Fahad Faisal. An overview of blockchain applications and attacks. In *2019 international conference on vision towards emerging trends in communication and networking (ViTECoN)*, pages 1–6. IEEE, 2019. URL https://ieeexplore.ieee.org/abstract/document/8899450.

[78] Srikumar Maiyuren and Olsen James. Implications of quantum computation on blockchain, March 2022. URL https://mycelium.xyz/research/quantum-computation-implications-on-blockchain-technology.

[79] Thompson Charlie. Quantum computers pose a credible threat to the security of bitcoin, June 2018. URL https://medium.com/coinmonks/quantum-computers-pose-a-credible-threat-to-the-security-of-bitcoin-4b1dd65944ca.

[80] Brandon Rodenburg and Stephen P Pappas. Blockchain and quantum computing. Technical report, The MITRE Corporation, 2017. URL https://apps.dtic.mil/sti/citations/AD1125436.

[81] Shoup Victor. Threshold ecdsa: The key ingredient behind the internet computer's bitcoin and ethereum integrations, June 2022. URL https://medium.com/dfinity/threshold-ecdsa-the-key-ingredient-behind-the-internet-computers-bitcoin-and-ethereum-cf22649b98a1.

[82] Certicom Research. Certicom ecc challenge. URL https://www.certicom.com/content/dam/certicom/images/pdfs/challenge-2009.pdf.

[83] Senate. H.r.6227 - national quantum initiative act, December 2018. URL https://www.congress.gov/bill/115th-congress/house-bill/6227.

[84] Young Shalanda. Memorandum for the heads of executive departments and agencies, November 2022. URL https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf.

[85] Ducklin Paul. Us passes the quantum computing cybersecurity preparedness act – and why not?, December 2022. URL https://nakedsecurity.sophos.com/2022/12/29/us-passes-the-quantum-computing-cybersecurity-preparedness-act-and-why-not/.

[86] Senate. H.r.7535 - quantum computing cybersecurity preparedness act, April 2022. URL https://www.congress.gov/bill/117th-congress/house-bill/7535/text.

[87] ENISA. Post-quantum cryptography: Current state and quantum mitigation, May 2021. URL https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.

[88] ENISA. Post-quantum cryptography - integration study, October 2022. URL https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study.

[89] Bobier Jean-Francois, Langione Matt, Tao Edward, and Gourevitch Antoine. What happens when 'if' turns to 'when' in quantum computing?, July 2021. URL https://www.bcg.com/publications/2021/building-quantum-advantage.

[90] Microsoft. Cryptography in the era of quantum computers, March 2023. URL https://www.microsoft.com/en-us/research/project/post-quantum-cryptography/.

[91] CBINSIGHTS. The big tech in quantum report: How google, microsoft, amazon, ibm, & intel are battling for the future of computing, May 2022. URL https://bleu-azur-consulting.eu/2022/05/28/the-big-tech-in-quantum-report-how-google-microsoft-amazon-ibm-intelare-battling-for-the-future-of-computing/.

[92] Capgemini Research Institute. Quantum technologies: How to prepare your organization for a quantum advantage now, 2022 March. URL https://prod.ucwe.capgemini.com/wp-content/uploads/2022/03/Final-Web-Version-Quantum-Technologies-1.pdf.

[93] World Economic Forum. Strategic intelligence - transformation maps, Marc 2023. URL https://intelligence.weforum.org/.

[94] Barmes Itan, Kohn Isaac, and Soutar Colin. What does the dawn of quantum computing mean for blockchain?, April 2022. URL https://www.weforum.org/agenda/2022/04/could-quantum-computers-steal-the-bitcoins-straight-out-of-your-wallet/.

[95] R3 Corda. Digital finance is powered by corda, February 2023. URL https://r3.com/products/corda/.

[96] Hyperledger Foundation. Building better together, February 2023. URL https://www.hyperledger.org/.

[97] Piet Verschuren, Hans Doorewaard, and Michelle Mellion. *Designing a research project*, volume 2. Eleven International Publishing The Hague, 2010. URL https://www.scribd.com/document/371407174/Piet-Verschuren-Hans-Doorewaard-Designing-a-Research-Project-pdf.

[98] Horizen Academy. Hash functions, 2022. URL https://www.horizen.io/blockchain-academy/technology/advanced/hash-functions/#:~:text=Hash%20values%20are%20used%20for,property%20of%20being%20collision%2Dresistant.

[99] Techskill Brew. Hash functions in blockchain (part 3- blockchain series), December 2021. URL https://medium.com/techskill-brew/hash-functions-in-blockchain-part-3-blockchain-basics-c3a0286064b6.

[100] Bala Priya C. Cryptographic hash functions in blockchain (with bash & python code), April 2022. URL https://hackernoon.com/cryptographic-hash-functions-in-blockchain-with-bash-and-python-code.

[101] Kumar Dhairya. Role of hash functions in cryptocurrencies, June 2021. URL https://www.linkedin.com/pulse/role-hash-functions-cryptocurrencies-dhairya-kumar/.

[102] Alexandr Kuznetsov, Inna Oleshko, Vladyslav Tymchenko, Konstantin Lisitsky, Mariia Rodinko, and Andrii Kolhatin. Performance analysis of cryptographic hash functions suitable for use in blockchain. *International Journal of Computer Network & Information Security*, 13(2), 2021. URL https://mecs-press.net/ijcnis/ijcnis-v13-n2/IJCNIS-V13-N2-1.pdf.

[103] Maury Shenk. The quantum countdown: Quantum computing & the future of smart ledger encryption. *Quantum Computing & The Future Of Smart Ledger Encryption-Long Finance*, 2018. URL https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3675655.

[104] Evgeniy O Kiktenko, Nikolay O Pozhar, Maxim N Anufriev, Anton S Trushechkin, Ruslan R Yunusov, Yuri V Kurochkin, AI Lvovsky, and Aleksey K Fedorov. Quantum-secured blockchain. *Quantum Science and Technology*, 3(3):035004, 2018. URL https://iopscience.iop.org/article/10.1088/2058-9565/aabc6b/meta.

[105] Wei Cui, Tong Dou, and Shilu Yan. Threats and opportunities: Blockchain meets quantum computation. In *2020 39th Chinese control conference (CCC)*, pages 5822–5824. IEEE, 2020. URL https://ieeexplore.ieee.org/abstract/document/9189608.

[106] Ghassan O Karame, Elli Androulaki, Marc Roeschlin, Arthur Gervais, and Srdjan Čapkun. Misbehavior in bitcoin: A study of double-spending and accountability. *ACM Transactions on Information and System Security (TISSEC)*, 18(1):1–32, 2015. URL https://dl.acm.org/doi/abs/10.1145/2732196.

[107] Karl J O'Dwyer and David Malone. Bitcoin mining and its energy footprint. 2014. URL https://digital-library.theiet.org/content/conferences/10.1049/cp.2014.0699.

[108] Nohe Patrick. Re-hashed: The difference between sha-1, sha-2 and sha-256 hash algorithms, November 2018. URL https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/.

[109] Matthew Amy, Olivia Di Matteo, Vlad Gheorghiu, Michele Mosca, Alex Parent, and John Schanck. Estimating the cost of generic quantum pre-image attacks on sha-2 and sha-3. In *International Conference on Selected Areas in Cryptography*, pages 317–337. Springer, 2016. URL https://pdfs.semanticscholar.org/8915/cfdceeff825230684e0286e0199207e41ce2.pdf.

[110] 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. URL https://arxiv.org/abs/1710.10377.

[111] Miners profitability, November 2022. URL https://www.asicminervalue.com/.

[112] Akinori Hosoyamada, Yu Sasaki, Seiichiro Tani, and Keita Xagawa. Quantum algorithm for the multicollision problem. *Theoretical Computer Science*, 842:100–117, 2020. URL https://www.sciencedirect.com/science/article/abs/pii/S0304397520304187.

[113] Daniel Larimer. Momentum–a memory-hard proof-of-work via finding birthday collisions. Technical report, Tech. Rep., October 2014. URL http://www.hashcash.org/papers/momentum.pdf.

[114] Rouzbeh Behnia, Eamonn W Postlethwaite, Muslum Ozgur Ozmen, and Attila Altay Yavuz. Lattice-based proof-of-work for post-quantum blockchains. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, pages 310–318. Springer, 2021. URL https://link.springer.com/chapter/10.1007/978-3-030-93944-1_21.

[115] Dargan James. 13 companies offering quantum cloud computing software services, May 2022. URL https://thequantuminsider.com/2022/05/03/13-companies-offering-quantum-cloud-computing-services-in-2022/.

[116] Stefanie Barz, Elham Kashefi, Anne Broadbent, Joseph F Fitzsimons, Anton Zeilinger, and Philip Walther. Demonstration of blind quantum computing. *science*, 335(6066):303–308, 2012. URL https://www.science.org/doi/abs/10.1126/science.1214707.

[117] Lei Zhang, Andriy Miranskyy, Walid Rjaibi, Greg Stager, Michael Gray, and John Peck. Making existing software quantum safe: Lessons learned. *arXiv preprint arXiv:2110.08661*, 2021. URL https://arxiv.org/abs/2110.08661.

[118] Or Sattath. On the insecurity of quantum bitcoin mining. *International Journal of Information Security*, 19(3):291–302, 2020. URL https://link.springer.com/article/10.1007/s10207-020-00493-9.

[119] Amr M Khalifa, Ayman M Bahaa-Eldin, and Mohamed Aly Sobh. Quantum attacks and defenses for proof-of-stake. In *2019 14th International Conference on Computer Engineering and Systems (ICCES)*, pages 112–117. IEEE, 2019. URL https://ieeexplore.ieee.org/abstract/document/9068181.

[120] Moreland Kirsty. What are public keys and private keys?, October 2022. URL https://www.ledger.com/academy/blockchain/what-are-public-keys-and-private-keys.

[121] Staff Cryptopedia. What are public and private keys?, June 2022. URL https://www.gemini.com/cryptopedia/public-private-keys-cryptography#section-what-is-public-key-cryptography.

[122] Antony. How do digital signatures work on blockchains? (part 1), November 2021. URL https://hub.easycrypto.com/how-digital-signatures-work.

[123] Ethan Fast. Cryptography behind the top 100 cryptocurrencies, February 2021. URL http://ethanfast.com/top-crypto.html.

[124] Andrada-Teodora Ciulei, Marian-Codrin Crețu, and Emil Simion. Preparation for post-quantum era: a survey about blockchain schemes from a post-quantum perspective. *Cryptology ePrint Archive*, 2022. URL https://eprint.iacr.org/2022/026.

[125] Konstantinos Chalkias, James Brown, Mike Hearn, Tommy Lillehagen, Igor Nitto, and Thomas Schroeter. Blockchained post-quantum signatures. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pages 1196–1203. IEEE, 2018. URL https://ieeexplore.ieee.org/abstract/document/8726842.

[126] Rambus. A modern interpretation of kerckhoff, September 2020. URL https://www.rambus.com/blogs/a-modern-interpretation-of-kerckhoff/.

[127] 114th Congress. S.3084 - american innovation and competitiveness act, June 2017. URL https://www.congress.gov/bill/114th-congress/senate-bill/3084.

[128] Bakhtiyor Yokubov and Lu Gan. A performance comparison of post-quantum algorithms in blockchain. *The Journal of The British Blockchain Association*, 2022. URL https://jbba.scholasticahq.com/article/38508.pdf.

[129] S Brotsis, N Kolokotronis, and K Limniotis. Towards post-quantum blockchain platforms. 2022. URL https://www.nowpublishers.com/article/DownloadChapters?bookId=9781680838343&chapters=978-1-68083-835-0.ch7.

[130] Arman Rasoodl Faridi, Faraz Masood, Ali Haider Thabet Shamsan, Mohammad Luqman, and Monir Yahya Salmony. Blockchain in the quantum world. *arXiv preprint arXiv:2202.00224*, 2022. URL https://arxiv.org/abs/2202.00224.

[131] Robert J McEliece. A public-key cryptosystem based on algebraic. *Coding Thv*, 4244:114–116, 1978. URL https://ntrs.nasa.gov/api/citations/19780016269/downloads/19780016269.pdf#page=123.

[132] Elwyn Berlekamp, Robert McEliece, and Henk Van Tilborg. On the inherent intractability of certain coding problems (corresp.). *IEEE Transactions on Information Theory*, 24(3):384–386, 1978. URL https://ieeexplore.ieee.org/abstract/document/1055873.

[133] Shiyao Gao, Dong Zheng, Rui Guo, Chunming Jing, and Chencheng Hu. An anti-quantum e-voting protocol in blockchain with audit function. *IEEE Access*, 7:115304–115316, 2019. URL https://ieeexplore.ieee.org/abstract/document/8804187.

[134] Daniel J Bernstein. Introduction to post-quantum cryptography. In *Post-quantum cryptography*, pages 1–14. Springer, 2009. URL https://link.springer.com/chapter/10.1007/978-3-540-88702-7_1.

[135] Albrecht Petzoldt, Stanislav Bulygin, and Johannes Buchmann. Selecting parameters for the rainbow signature scheme-extended version. *Cryptology ePrint Archive*, 2010. URL https://eprint.iacr.org/2010/437.

[136] Johannes Blömer and Stefanie Naewe. Sampling methods for shortest vectors, closest vectors and successive minima. *Theoretical Computer Science*, 410(18):1648–1665, 2009. URL https://www.sciencedirect.com/science/article/pii/S0304397508009316.

[137] Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the twenty-ninth annual ACM symposium on Theory of computing*, pages 284–293, 1997. URL https://dl.acm.org/doi/pdf/10.1145/258533.258604.

[138] Sabah Suhail, Rasheed Hussain, Abid Khan, and Choong Seon Hong. On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions. *IEEE Internet of Things Journal*, 8(1):1–17, 2020. URL https://ieeexplore.ieee.org/abstract/document/9152977.

[139] Jiahui Chen, Wensheng Gan, Muchuang Hu, and Chien-Ming Chen. On the construction of a post-quantum blockchain for smart city. *Journal of information security and applications*, 58:102780, 2021. URL https://www.sciencedirect.com/science/article/abs/pii/S2214212621000284.

[140] Xi Sun, Haibo Tian, and Yumin Wang. Toward quantum-resistant strong designated verifier signature from isogenies. In *2012 Fourth International Conference on Intelligent Networking and Collaborative Systems*, pages 292–296. IEEE, 2012. URL https://ieeexplore.ieee.org/abstract/document/6337933.

[141] Steven D Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. *Journal of Cryptology*, 33(1):130–175, 2020. URL https://link.springer.com/article/10.1007/s00145-019-09316-0.

[142] Braithwaite Matt. Experimenting with post-quantum cryptography, July 2016. URL https://security.googleblog.com/2016/07/experimenting-with-post-quantum.html.

[143] Swati Kumari, Maninder Singh, Raman Singh, and Hitesh Tewari. A post-quantum lattice based lightweight authentication and code-based hybrid encryption scheme for iot devices. *Computer Networks*, 217:109327, 2022. URL https://www.sciencedirect.com/science/article/abs/pii/S138912862200367X.

[144] Amelia Holcomb, Geovandro Pereira, Bhargav Das, and Michele Mosca. Pqfabric: a permissioned blockchain secure from both classical and quantum attacks. In *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–9. IEEE, 2021. URL https://ieeexplore.ieee.org/abstract/document/9461070.

[145] Wazir Zada Khan, Qurat-ul-Ain Arshad, Mudassar Raza, and Muhammad Imran. Quantum cryptography a real threat to classical blockchain: Requirements and challenges. 2022. URL https://www.techrxiv.org/articles/preprint/Quantum_Cryptography_a_Real_Threat_to_Classical_Blockchain_Requirements_and_Challenges/21341817.

[146] Daniel J Bernstein, Andreas Hülsing, Stefan Kölbl, Ruben Niederhagen, Joost Rijneveld, and Peter Schwabe. The sphincs+ signature framework. In *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security*, pages 2129–2146, 2019. URL https://dl.acm.org/doi/abs/10.1145/3319535.3363229.

[147] Nivedita Dey, Mrityunjay Ghosh, and Amlan Chakrabarti. Quantum solutions to possible challenges of blockchain technology. In *Quantum and Blockchain for Modern Computing Systems: Vision and Advancements*, pages 249–282. Springer, 2022. URL https://link.springer.com/chapter/10.1007/978-3-031-04613-1_9.

[148] NIST. Stateful hash-based signatures hbs, October 2020. URL https://csrc.nist.gov/projects/stateful-hash-based-signatures.

[149] David A Cooper, Daniel C Apon, Quynh H Dang, Michael S Davidson, Morris J Dworkin, Carl A Miller, et al. Recommendation for stateful hash-based signature schemes. *NIST Special Publication*, 800:208, 2020. URL https://csrc.nist.rip/external/nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf.

[150] Panos Kampanakis and Scott Fluhrer. Lms vs xmss: Comparion of two hash-based signature standards. *Cryptology ePrint Archive*, 2017. URL https://eprint.iacr.org/2017/349.

[151] QRL. Ots key index, March 2018. URL https://docs.theqrl.org/developers/ots/.

[152] Bernstein Daniel, Hülsing Andreas, Kölbl Stefan, Niederhagen Ruben, Rijneveld Joost, and Schwabe Peter. The sphincs+ signature framework, November 2019. URL https://pure.tue.nl/ws/portalfiles/portal/143228945/p2129_bernstein.pdf.

[153] Breus Blaauwendraad, Zekeriya Erkin, Peter Schwabe, Oguzhan Ersoy, and Bart de Jong. *Postquantum Hash-based Signatures for Multi-chain Blockchain Technologies.* PhD thesis, Master Thesis, 2019. URL https://www.ru.nl/publish/pages/769526/z05_2019_thesis_breus_blaauwendraad_final.pdf.

[154] NIST. Fast falcon signature generation and verification using armv8 neon instructions, December 2022. URL https://csrc.nist.gov/Presentations/2022/fast-falcon-signature-generation-and-verification.

[155] Léo Ducas, Eamonn W Postlethwaite, Ludo N Pulles, and Wessel van Woerden. Hawk: Module lip makes lattice signatures fast, compact and simple. *Cryptology ePrint Archive*, September 2022. URL https://link.springer.com/chapter/10.1007/978-3-031-22972-5_3.

[156] Johannes Göbel and Anthony E Krzesinski. Increased block size and bitcoin blockchain dynamics. In *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*, pages 1–6. IEEE, 2017. URL https://ieeexplore.ieee.org/abstract/document/8215367.

[157] Ruping Shen, Hong Xiang, Xin Zhang, Bin Cai, and Tao Xiang. Application and implementation of multivariate public key cryptosystem in blockchain (short paper). In *International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pages 419–428. Springer, 2019. URL https://link.springer.com/chapter/10.1007/978-3-030-30146-0_29.

[158] Tonejc Jernej and Usher Nairi. A hybrid post-quantum digital signature scheme for the ethereum virtual machine, July 2022. URL https://ethresear.ch/t/a-hybrid-post-quantum-digital-signature-scheme-for-the-evm/13008.

[159] Meryem Cherkaoui Semmouni, Abderrahmane Nitaj, and Mostafa Belkasmi. Bitcoin security with post quantum cryptography. In *International Conference on Networked Systems*, pages 281–288. Springer, 2019. URL https://link.springer.com/chapter/10.1007/978-3-030-31277-0_19.

[160] Wouter van der Linde, Peter Schwabe, Andreas Hülsing, Yuval Yarom, and Lejla Batina. Post-quantum blockchain using one-time signature chains. *Radboud Univ., Nijmegen, The Netherlands, Tech. Rep*, 2018. URL https://www.ru.nl/publish/pages/769526/wouter_van_der_linde.pdf.

[161] NIST. Post-quantum cryptography: Digital signature schemes, August 2022. URL https://csrc.nist.gov/projects/pqc-dig-sig/standardization/call-for-proposals.

[162] NIST. Call for additional digital signature schemes for the post-quantum cryptography standardization process, 2022 August. URL https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf.

[163] Benito Arruñada and Luis Garicano. Blockchain: The birth of decentralized governance. *Pompeu Fabra University, Economics and Business Working Paper Series*, 1608, 2018. URL https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3160070.

[164] Rowan van Pelt, Slinger Jansen, Djuri Baars, and Sietse Overbeek. Defining blockchain governance: a framework for analysis and comparison. *Information Systems Management*, 38(1):21–41, 2021. URL https://www.tandfonline.com/doi/full/10.1080/10580530.2020.1720046.

[165] Yue Liu, Qinghua Lu, Liming Zhu, Hye-Young Paik, and Mark Staples. A systematic literature review on blockchain governance. *Journal of Systems and Software*, page 111576, 2022. URL https://www.sciencedirect.com/science/article/abs/pii/S0164121222002527.

[166] Blockchain Council. Soft fork vs. hard fork: A detailed comparison, October 2022. URL https://www.blockchain-council.org/blockchain/soft-fork-vs-hard-fork/.

[167] Shardeum. Soft fork vs hard fork: What are the differences?, September 2022. URL https://shardeum.org/blog/hard-fork-vs-soft-fork/.

[168] Abrol Ayushi. What are blockchain nodes? detailed guide, December 2022. URL https://www.blockchain-council.org/blockchain/blockchain-nodes/#:~:text=Blockchain%20nodes%20are%20network%20stakeholders,network%20transactions%2C%20known%20as%20blocks.

[169] Taner Dursun and Burak Berk Üstündağ. A novel framework for policy based on-chain governance of blockchain networks. *Information Processing & Management*, 58(4):102556, 2021. URL https://www.sciencedirect.com/science/article/abs/pii/S0306457321000601.

[170] craigraw, January 2023. URL https://github.com/bitcoin/bips.

[171] protolambda. Update eip-4844: clarify datahash return value (, January 2023. URL https://github.com/ethereum/EIPs.

[172] jnewbery. bip-0002, May 2021. URL https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki.

[173] Bip 0009, January 2023. URL https://en.bitcoin.it/wiki/BIP_0009.

[174] van Wirdum Aaron. Why some changes to bitcoin require consensus: Bitcoin's 4 layers, February 2016. URL https://bitcoinmagazine.com/technical/why-some-changes-to-bitcoin-require-consensus-bitcoin-s-layers-1456512578.

[175] How many bitcoin forks are there?, January 2023. URL https://forkdrop.io/how-many-bitcoin-forks-are-there.

[176] Ethereum. Introduction to ethereum improvement proposals (eips), January 2023. URL https://ethereum.org/en/eips/.

[177] Becze Martin and Jameson Hudson. Eip-1: Eip purpose and guidelines, October 2015. URL https://eips.ethereum.org/EIPS/eip-1.

[178] Orenes-Lerma Linda. Ethereum improvement proposals: How they work and why they matter, December 2022. URL https://www.ledger.com/academy/topics/ethereum/ethereum-improvement-proposals-eip.

[179] Ethereum. The history of ethereum, January 2023. URL https://ethereum.org/en/history/.

[180] Aron Fischer and María-Cruz Valiente. Blockchain governance. *Internet Policy Review*, 10(2): 1–10, 2021. URL https://www.econstor.eu/handle/10419/235958.

[181] ICP. Blockchain protocol upgrade, November 2022. URL https://internetcomputer.org/how-it-works/upgrades/.

[182] DFINITY. Upgrading the internet computer protocol, December 2021. URL https://medium.com/dfinity/upgrading-the-internet-computer-protocol-45bf6424b268.

[183] domothy. Annotated ethereum roadmap, December 2022. URL https://notes.ethereum.org/@domothy/roadmap#The-Splurge.

[184] Cathy Barrera and Stephanie Hurder. Blockchain upgrade as a coordination game. *Available at SSRN 3192208*, 2018. URL https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3192208.

[185] Kurt M Alonso and Jordi Herrera Joancomartí. Monero-privacy in the blockchain. *Cryptology ePrint Archive*, 2018. URL https://eprint.iacr.org/2018/535.

[186] Woods John. Algorand: Pioneering falcon post-quantum technology on blockchain, Augustus 2022. URL https://www.algorand.foundation/news/pioneering-falcon-post-quantum-technology-on-blockchain.

[187] Grossman Noah. Algorand state proofs: Powering blockchain interoperability and post-quantum security, March 2022. URL https://www.algorand.com/resources/algorand-announcements/powering-blockchain-interoperability-and-post-quantum-security.

[188] Algorand. Algorand protocol upgrade introduces state proofs for trustless cross chain communication and 5x faster performance, September 2022. URL https://www.prnewswire.com/news-releases/algorand-protocol-upgrade-introduces-state-proofs-for-trustless-cross-chain-communication-and-5x-faster-performance-301619219.html.

[189] Wan Samuel. Algorand leads quantum-proof technology with development of falcon, August 2022. URL https://cryptoslate.com/algorand-leads-quantum-proof-technology-with-development-of-falcon/.

[190] Chaum David and Moser Thomas. ecash 2.0 - inalienably private and quantum-resistant to counterfeiting, 2022. URL https://chaum.com/wp-content/uploads/2022/11/eCash_2.0_9-7-22-.pdf.

[191] Hamacher Adriana. How david chaum went from inventing digital cash to pioneering digital privacy, April 2022. URL https://decrypt.co/95109/david-chaum-from-inventing-digital-cash-to-pioneering-digital-privacy.

[192] xx network. xx network white paper xx consensus, April 2021. URL https://xx.network/wp-content/uploads/2021/10/xx-consensus-whitepaper.pdf.

[193] NEO. Neo white paper, July 2017. URL https://docs.neo.org/v2/docs/en-us/basic/whitepaper.html#anti-quantum-cryptography-mechanism-neoqs.

[194] enero. Decred releases v1.7 with post quantum secure privacy and major subsidy split vote, 2022. URL https://decred.org/es/news/2022-01-24-decred-releases-1.7/.

[195] QRL. We are the quantum resistant ledger, December 2022. URL https://www.theqrl.org/.

[196] Nexus. Resource hub - quantum resistance, October 2019. URL https://nexus.io/ResourceHub/quantum-resistance.

[197] Hcash. Hypercash completed post-quantum linkable ring signature code development, February 2019. URL https://media-30378.medium.com/hypercash-completed-post-quantum-linkable-ring-signature-code-development-ae865476cd86.

[198] CoinMarketCap. Today's cryptocurrency prices by market cap, December 2022. URL https://coinmarketcap.com/.

[199] IOTA. Faq, 2022. URL https://wiki.iota.org/introduction/explanations/faq.

[200] FTC. Truth in advertising, August 2020. URL https://www.ftc.gov/news-events/topics/truth-advertising.

[201] Browne Ryan. Uk watchdog puts 50 crypto companies on notice over 'misleading' ads, March 2022. URL https://www.cnbc.com/2022/03/22/uk-watchdog-puts-50-crypto-firms-on-notice-over-misleading-ads.html.

[202] DevEx. Her majesty's treasury (hm treasury), May 2020. URL https://www.devex.com/organizations/her-majesty-s-treasury-hm-treasury-43922.

[203] Sweney Mark. Treasury plans crackdown on 'misleading' cryptocurrency ads, January 2022. URL https://www.theguardian.com/technology/2022/jan/18/treasury-plans-crackdown-on-misleading-cryptocurrency-ads.

[204] Binance. Buy, trade, and hold 350+ cryptocurrencies on binance, February 2023. URL https://www.binance.com/en.

[205] Coinbase. Jump start your crypto portfolio, February 2023. URL https://www.coinbase.com/.

[206] CoinMarketCap. Today's cryptocurrency prices by market cap, February 2023. URL https://coinmarketcap.com/.

[207] CoinGecko. Cryptocurrency prices by market cap, February 2023. URL https://www.coingecko.com/.

[208] Rajagopal Divya. Exclusive: Canada's biggest pension plan, cppi, ends crypto investment pursuit, December 2022. URL https://www.reuters.com/business/canadas-biggest-pension-plan-cppi-ends-crypto-investment-pursuit-sources-2022-12-07/.

[209] Olinga Luc. Ftx, luna, celsius, voyager: The year of crypto bankruptcies, 2022 December. URL https://www.thestreet.com/investing/cryptocurrency/ftx-luna-celsius-voyager-the-year-of-crypto-bankruptcies.

[210] European Securities and Markets Authority. Investment services, January 2023. URL https://www.esma.europa.eu/esmas-activities/investors-and-issuers/investment-services.

[211] O'Sullivan Ross. Binance futures: Why should you trade on binance futures?, 2022 February. URL https://everybithelps.io/binance-futures/.

[212] Who services who in crypto custody, October 2022. URL https://www.blockdata.tech/blog/general/who-services-who-in-crypto-custody.

[213] ECB. Licensing of crypto-asset activities, 2022 August. URL https://www.bankingsupervision.europa.eu/press/publications/newsletter/2022/html/ssm.nl220817_2.en.html.

[214] Andrade Laura. The legal side of crypto-assets custody, April 2020. URL https://micobo.com/the-legal-side-of-crypto-assets-custody/.

[215] Freund Andreas. Enterprise blockchains redux: How to be not-not nist compliant without breaking the bank, September 2022. URL https://entethalliance.org/enterprise-blockchains-redux-how-to-be-not-not-nist-compliant-without-breaking-the-bank/.

[216] West Darrell. A brief history of u.s. encryption policy, April 2016. URL https://www.brookings.edu/blog/techtank/2016/04/19/a-brief-history-of-u-s-encryption-policy/.

[217] Periroth Nicole, Larson Jeff, and Shane Scott. N.s.a. able to foil basic safeguards of privacy on web, September 2013. URL https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=2&_r=2.

[218] Pci dss certification. URL https://www.imperva.com/learn/data-security/pci-dss-certification/#:~:text=Governed%20by%20the%20Payment%20Card,against%20data%20theft%20and%20fraud.

[219] GQI. Nist announces collaborating vendors in the migration to post-quantum cryptography project, July 2022. URL https://quantumcomputingreport.com/nist-announces-collaborating-vendors-in-the-migration-to-post-quantum-cryptography-project/.

[220] National Cybersecurity Center of Excellence. Migration to post-quantum cryptography, February 2023. URL https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms.

[221] Iain Stewart, Daniel Ilie, Alexei Zamyatin, Sam Werner, MF Torshizi, and William J Knottenbelt. Committing to quantum resistance: a slow defence for bitcoin against a fast quantum computing attack. *Royal Society open science*, 5(6):180410, 2018. URL https://royalsocietypublishing.org/doi/full/10.1098/rsos.180410.

[222] TezosGovernance. Quantum resistance timeline, April 2021. URL https://forum.tezosagora.org/t/quantum-resistance-timeline/2950.

[223] IQT News. Ripple's cto says quantum computers will be a threat to bitcoin and xrp, July 2020. URL https://www.insidequantumtechnology.com/news-archive/ripples-cto-says-quantum-computers-will-be-a-threat-to-bitcoin-and-xrp/.

[224] Schwartz David, July 2022. URL https://twitter.com/JoelKatz/status/1552009213567635457.

[225] Zcash. Frequently asked questions. URL https://z.cash/support/faq/#quantum-computers.

[226] daira. Fully post-quantum zcash #805, March 2016. URL https://github.com/zcash/zcash/issues/805.

[227] jonmoss. Cardano foundation and z/yen explore threat of quantum computing to blockchain security, February 2018. URL https://forum.cardano.org/t/20-2-18-cardano-foundation-and-z-yen-explore-threat-of-quantum-computing-to-blockchain-security/8495.

[228] Hoskinson Charles. Surprise ama 04/13/2022, April 2022. URL https://www.youtube.com/watch?v=AejphsMjkPc.

[229] Cronja Andre. Quantum resistance, October 2018. URL https://github.com/Fantom-foundation/fantom-research/blob/master/quantum.md.

[230] ICO Analytics, November 2019. URL https://twitter.com/ico_analytics/status/1200854428628258816?lang=ca.

[231] Polygon Team. Polygon announces polygon miden - a stark-based, ethereum-compatible rollup, November 2021. URL https://polygon.technology/blog/polygon-announces-polygon-miden-a-stark-based-ethereum-compatible-rollup.

[232] Bakul B. Polygon's transition to zk-rollups & plonky2, 2022 January. URL https://www.mlq.ai/polygons-transition-to-zk-rollups-plonky2/.

[233] Nikhil Verma, Swati Kumari, and Pranavi Jain. Post quantum digital signature change in iota to reduce latency in internet of vehicles (iov) environments. In *2022 International Conference on IoT and Blockchain Technology (ICIBT)*, pages 1–6. IEEE, 2022. URL https://ieeexplore.ieee.org/abstract/document/9807757.

[234] IOTA R&D. Assuring authenticity in the tangle with signatures, February 2019. URL https://blog.iota.org/assuring-authenticity-in-the-tangle-with-signatures-791897d7b998/.

[235] DASH. The pow extinction event within 10 - 20 years, August 2021. URL https://www.dash.org/forum/threads/the-pow-extinction-event-within-10-20-years.51906/#post-227991.

[236] DASH. Quantum is here, should we be worried?, May 2018. URL https://www.dash.org/forum/threads/quantum-is-here-should-we-be-worried.30153/.

[237] igormcoelho. Proposal for quantum security (neoqs) #85, February 2019. URL https://github.com/neo-project/proposals/issues/85.

[238] Monero Insight. Identifying practical post-quantum strategies for monero, May 2020. URL https://ccs.getmonero.org/proposals/research-post-quantum-monero.html.

[239] Corbo Adam, Krawiec-Thayer Mitchell, and Goodell Brandon. Evaluating cryptocurrency security and privacy in a post-quantum world, September 2020. URL https://github.com/insight-decentralized-consensus-lab/post-quantum-monero/blob/master/writeups/technical_note.pdf.

[240] Post quantum security, January 2022. URL https://forums.minaprotocol.com/t/post-quantum-security/5214.

[241] MINA Foundation. Zk tech you should know — part 1: Snarks & starks, October 2021. URL https://minaprotocol.com/blog/zk-you-should-know-snarks-starks.

[242] VeChain Foundation. Vechain technical ama — software questions part 1, February 2018. URL https://vechainofficial.medium.com/vechain-technical-ama-software-questions-part-1-cb17c830e458.

[243] diegop. Long term r&d: Pq security (proposal), December 2021. URL https://forum.dfinity.org/t/long-term-r-d-pq-security-proposal/9395.

[244] Baird Leemon, Mukherjee Pratyay, and Sinha Rohit. Post quantum crypto, July 2022. URL https://hedera.com/blog/post-quantum-crypto.

[245] Hedera. Is hedera post-quantum secure?, January 2022. URL https://help.hedera.com/hc/en-us/articles/360000764318-Is-Hedera-post-quantum-secure-.

[246] Zerucha Tony. Decred announces system improvements, included quantum computing protection, in v1.7, January 2022. URL https://www.crowdfundinsider.com/2022/01/185890-decred-announces-system-improvements-included-quantum-computing-protection-in-v1-7/.

[247] Elrond. Frequently asked questions, November 2018. URL https://elrond.com/faq/.

[248] Xiaomo Liu, G Alan Wang, Aditya Johri, Mi Zhou, and Weiguo Fan. Harnessing global expertise: A comparative study of expertise profiling methods for online communities. *Information Systems Frontiers*, 16:715–727, 2014. URL https://link.springer.com/article/10.1007/s10796-012-9385-6.

A

Appendix

A.1. Quantum Awareness Among Top 100 Projects

Table A.1: An overview of the top 100 cryptocurrencies and their maturity levels in terms of quantum awareness, research and adoption

#	**Name**	**Ticker**	**Maturity Level**				**#**	**Name**	**Ticker**	**Maturity Level**			
			0	**1**	**2**	**3**				**0**	**1**	**2**	**3**
1	Bitcoin [110] [221]	BTC			X		51	Tezos [222]	XTZ		X		
2	Ethereum [158] [12]	ETH			X		52	KuCoin Token	KCS	X			
3	Tether	USDT	X				53	Axie Infinity	AXS	X			
4	USD Coin	USDC	X				54	Gemini Dollar	GUSD	X			
5	BNB	BNB	X				55	BitTorrent-New	BTT	X			
6	XRP [223] [224]	XRP		X			56	Zcash [225] [226]	ZEC		X		
7	Binance USD	BUSD	X				57	Trust Wallet Token	TWT	X			
8	Dogecoin	DOGE	X				58	The Sandbox	SAND	X			
9	Cardano* [227] [228]	ADA			X		59	Fantom [229] [230]	FTM		X		
10	Polygon [231] [232]	MATIC		X			60	Decentraland	MANA	X			
11	DAI	DAI	X				61	PancakeSwap	CAKE	X			
12	Litecoin	LTC	X				62	Maker	MKR	X			
13	TRON	TRX	X				63	PAX Gold	PAXG	X			
14	Polkadot	DOT	X				64	The Graph	GRT	X			
15	Shiba Inu	SHIB	X				65	IOTA** [233] [234]	MIOTA			X	
16	Uniswap	UNI	X				66	Klaytn	KLAY	X			
17	Solana	SOL	X				67	Dash [235] [236]	DASH		X		
18	Avalanche	AVAX	X				68	Neo [237] [193]	NEO				X
19	UNUS SED LEO	LEO	X				69	Aptos	APT	X			
20	Wrapped Bitcoin	WBTC	X				70	eCash [190] [192]	XEC				X
21	Chainlink	LINK	X				71	Fei USD	FEI	X			
22	Toincoin	TON	X				72	THORChain	RUNE	X			
23	Cosmos	ATOM	X				73	Nexo	NEXO	X			
24	Monero [238] [239]	XMR			X		74	Synthetix	SNX	X			

25	Ethereum Classic	ETC	X				75	GMX	GMX	X			
26	Stellar	XLM	X				76	Mina [240] [241]	MINA		X		
27	Bitcoin Cash	BCH	X				77	Osmosis	OSMO	X			
28	OKB	OKB	X				78	GateToken	GT	X			
29	Cronos	CRO	X				79	Lido DAO	LDO	X			
30	ApeCoin	APE	X				80	EthereumPoW***	ETHW			X	
31	Quant	QNT	X				81	XDC Network	XDC	X			
32	Algorand [187] [186]	ALGO				X	82	Neutrino USD	USDN	X			
33	VeChain [242]	VET		X			83	Frax Share	FXS	X			
34	Filecoin	FIL	X				84	1inch Network	1INCH	X			
35	Internet Computer [243]	ICP			X		85	Casper	CSPR	X			
36	NEAR Protocol	NEAR	X				86	Immutable X	IMX	X			
37	Hedera [244] [245]	HBAR		X			87	Stacks	STX	X			
38	EOS	EOS	X				88	Curve DAO Token	CRV	X			
39	Terra Classic	LUNC	X				89	Decred [194] [246]	DCR				X
40	Pax Dollar	USDP	X				90	Chain	XCN	X			
41	Bitcoin SV	BSV	X				91	NEM	XEM	X			
42	MultiversX (elrond) [247]	EGLD		X			92	Zilliqa	ZIL	X			
43	Huobi Token	HT	X				93	Loopring	LRC	X			
44	TrueUSD	TUSD	X				94	Basic Attention Token	BAT	X			
45	Aave	AAVE	X				95	Holo	HOT	X			
46	Theta Network	THETA	X				96	Enjin Coin	ENJ	X			
47	USDD	USDD	X				97	Balancer	BAL	X			
48	BitDAO	BIT	X				98	Convex Finance	CVX	X			
49	Flow	FLOW	X				99	Celo	CELO	X			
50	Chiliz	CHZ	X				100	Compound	COMP	X			

*Cardano's research on post-quantum cryptography has been done in collaboration with Z/Yen Group, they have sued Cardano Foundation and research has been taken offline, **IOTA is no longer quantum-secure, but (originally) conducted research on integrating quantum-safe solutions ***EthereumPoW has extensive research at their disposal, as the ”Merge” happened on September 2022 and research was (mostly) focused on PoW.

A.2. Profile Interviewees

Table A.2: Profile of Interviewees

	Domain	**Experience**	**Aware of QT**	**Blockchain**	**Cryptography**
B1	Blockchain	High	yes	5	5
B2	Blockchain	Very high	no	5	1
B3	Blockchain	Very high	yes	4	2
B4	Blockchain	Medium	yes	3	2
B5	Blockchain	Very high	yes	4	4
B6	Blockchain	Medium	yes	5	5
B7	Blockchain	Very high	yes	5	3
B8	Blockchain	Medium	yes	5	3
B9	Blockchain	Very high	yes	5	5
B10	Blockchain	Very high	yes	4	5
B11	Blockchain	Very high	yes	5	3
B12	Blockchain	Medium	yes	4	2
B13	Blockchain	Very high	yes	5	1
B14	Blockchain	Medium	yes	5	3
B15	Blockchain	High	yes	5	5
B16	Blockchain	Medium	yes	4	2
B17	Blockchain	Very high	yes	3	3
B18	Blockchain	Very high	yes	5	5
B19	Blockchain	High	yes	5	3
B20	Blockchain	High	yes	5	2
C1	Cyber/Cryptography	Medium	yes	2	4
C2	Cyber/Cryptography	High	yes	3	5
C3	Cyber/Cryptography	Very high	yes	3	4
C4	Cyber/Cryptography	Very high	yes	5	5
C5	Cyber/Cryptography	Very high	yes	4	5
C6	Cyber/Cryptography	High	yes	2	3
C7	Cyber/Cryptography	High	yes	3	5
C8	Cyber/Cryptography	Very high	yes	4	5
C9	Cyber/Cryptography	Medium	yes	2	3
C10	Cyber/Cryptography	High	yes	4	5

The level of Working Experience (WE) was denoted as: WE < 2 years: low, 2 years < WE < 5 years: medium, 5 years < WE < 10 years: high, 10 years > WE: very high

Although the interviewees were picked very carefully based on their level of expertise, a proficiency scale [248] was used for their level of understanding of BT and cryptography specifically.

- Novice (1) - Starts to learn the knowledge of the domain, asks questions on basic concepts
- Advanced beginner (2) - Knows basic concepts, but is not good at advanced knowledge in this domain
- Competent (3) - Has some advanced knowledge and can give relatively good answers
- Proficient (4) - Can answer most questions and knows some sub-topics of a domain very well
- Expert (5) - Knows core knowledge on a domain and always provides insightful answers

A.3. List of Questions for the Structured Part of the Interviews

1. Years of relevant working experience?
2. Which domain falls closer to your level of expertise?

   - Cryptography/Cyber
   - Blockchain

3. Were you aware of the quantum threat before you were approached by the interviewer?

   - Yes
   - No

4. Were you aware of the quantum threat on blockchain before you were approached by the interviewer?

   - Yes
   - No

5. Please indicate your level of blockchain expertise according to the provided proficiency scale (see A.2)
6. Please indicate your level of cryptography expertise according to the provided proficiency scale (see A.2)
7. How worried are you about the effects of the quantum threat materializing for large organizations, institutions, and governments (non-BT domain), i.e., them not being able to implement the necessary solutions in time?

   - Not worried
   - Worried a little
   - Worried
   - Very worried

8. How worried are you about the effects of the quantum threat materializing for blockchain (BT domain), i.e., them not being able to implement the necessary solutions in time?

   - Not worried
   - Worried a little
   - Worried
   - Very worried

9. Of the top 100 cryptocurrency projects, what percentage do you expect will transition safely in time towards a quantum-safe environment?
10. As of January 2023, there seems to be a 20% public “quantum awareness” among the top 100 cryptocurrencies. Do you think that number is…

    - Low
    - Sufficient
    - High

11. If you were asked to give a % on the level of public “quantum awareness” among the top 100 cryptocurrencies. Would this number be:

    - Lower
    - Around this value
    - Higher

12. Now, knowing the level of public QA, what percentage of the top 100 cryptocurrency projects do you expect will transition safely in time towards a quantum-safe environment?
13. Among these stakeholders, rank them based on who you believe should drive change:

    - Core Developers
    - Project Foundation

- Community Figureheads
- Block Validators
- Full node operators
- Token holders/Investors
- Regulators/Policy Experts

14. Among these stakeholders, rank them based on who you believe will drive change:
    - Core Developers
    - Project Foundation
    - Community Figureheads
    - Block Validators
    - Full node operators
    - Token holders/Investors
    - Regulators/Policy Experts
15. Do you believe that it would be great to have some level of "external institutional technical support" for blockchain that can aid in the process of transitioning towards a quantum-safe environment? Elaborate accordingly.
16. Would you want NIST, or a similar organization, to:
    - Create a separate new program for blockchain,
    - Include in its current pqc program
    - Other...
17. Do you expect this to happen?
    - Yes
    - No
18. Do you believe that blockchain projects will (generally):
    - Adopt the existing pqc signatures as they are
    - Adjust the existing pqc signatures accordingly
    - Wait for new pq cryptosystems
    - Design their own new pq cryptosystems
19. On a scale from 1 to 5, how welcoming are you of policies and regulations for blockchain and cryptocurrency projects? (0=not welcoming at all, 3=neutral, 5=very welcoming)
20. Do you think it would be a great idea if there were to be an external organization that "audits" a blockchain's level of security and provides a stamp of approval of it being "quantum secure"?
    - If yes, would you prefer this organization to be from the public or private sector?
21. Should we implement the following policies? Please elaborate on your answers:
    (a) *By 2030, companies and organizations will no longer be allowed to utilize BT in their operations if they have not been deemed to be quantum secure.*
    (b) *By 2030, hedge funds, VCs, and any type of institutional investment organizations will no longer be allowed to invest in BT if they have not been deemed to be quantum-secure.*
    (c) *By 2030, it will be illegal to use BT that has not been deemed to be quantum-secure.*
    (d) *By 2030, exchanges will no longer be allowed to facilitate the buying and selling of cryptocurrency projects that have not been deemed to be quantum-secure (in light of customer protection).*
    (e) *By 2030, it will be illegal to develop BT that has not been deemed to be quantum-secure.*
22. On a scale from 1 to 5, how welcoming are you of policies and regulations for blockchain and cryptocurrency projects that aim to accelerate the transition of blockchain towards a quantum-safe environment? (0=not welcoming at all, 3=neutral, 5=very welcoming)
23. Please rank the three drivers of change for blockchain-based on what it should look like according to you:

- Stakeholders realizing that the quantum threat is approaching and genuinely wanting to protect the network's future (protection)
- The (anticipation of) policies and regulations that aim to accelerate the transition towards a quantum-safe environment for blockchain (compliance)
- Organizations wanting to differentiate themselves from competitors by (claiming that they are) becoming quantum-safe (marketing)

24. Please rank the three drivers of change for blockchain-based on what you expect it to look like:

    - Stakeholders realizing that the quantum threat is approaching and genuinely wanting to protect the network's future (protection)
    - The (anticipation of) policies and regulations that aim to accelerate the transition towards a quantum-safe environment for blockchain (compliance)
    - Organizations wanting to differentiate themselves from competitors by (claiming that they are) becoming quantum-safe (marketing)