To What Extent Will Intervention Be Needed During The Advent of Quantum Computing?

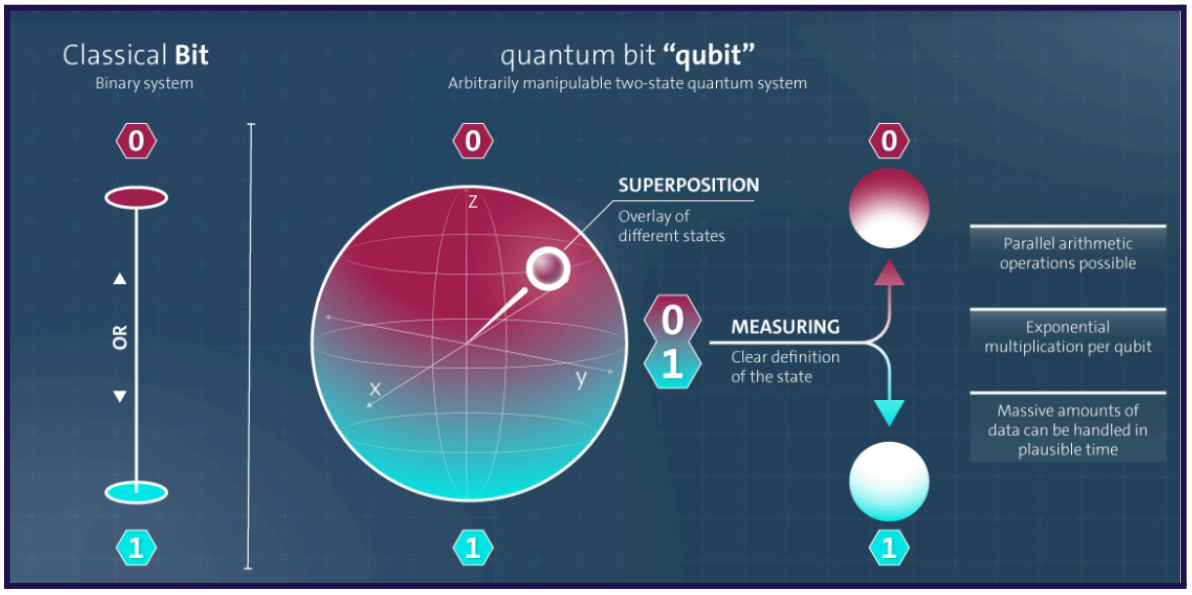
Sevin Fernando, Queen's College, Taunton

Preface

Quantum computing, developing at a time of technological uncertainty, is a precarious topic to consider. While there have been many claimed benefits, significant technical issues exist as obstacles to progress [1]. Nevertheless, as a novel technology experiencing strides in financing with technological giants paving the field, it is vital to consider potential intervention schemes.

The Potential of Quantum Computing

The essential difference between quantum computers and classical computers lies in their mechanism for data storage. According to McKinsey & Company, "while a classical computer has a bit, capable of representing a 0 or 1 distinctly, a quantum computer has a qubit, which can concurrently represent a combination of these values" [2]. In effect, numerous possibilities can be considered at the same time, leading to a potential acceleration of computing speed, which will be expanded on throughout the paper.



Bit and Qubit Comparison [3]

The Impact of Quantum Computing

The idea of acceleration is key to understanding how various sectors of society will be affected. We shall focus on its impact in Cybersecurity and Finance, discussing potential solutions and points of residual risk, thus identifying the precise nature of the real issues at hand.

Theoretical Societal Threats To Cybersecurity

The Weakening of Asymmetric Encryption

Encryption is the process of making data incomprehensible to an unauthorised third party using algorithms known as keys, thus being vital in the protection of sensitive data [4]. Asymmetric/public-key encryption, specifically, uses two linked keys in the cryptographic process [5], making it especially difficult for a hacker to reverse engineer [6]. However, the three common forms of asymmetric encryption (RSA, Diffie-Hellman, and ECC) are susceptible to Shor's algorithm utilisable by quantum computers [7]. Indeed, a 2017 Microsoft Research paper estimated that breaking a 256-bit ECC could be carried out with a 2330-qubit quantum computer [8], where 256-bit ECCs are an NIST-recommended standard today [9]. Furthermore, "Craig Gidney (Google) and Martin Ekera (KTH Royal Institute of Technology in Sweden) have claimed that a 2048-bit RSA encryption would be breakable in 8 hours with a noisy (any undesired source that changes the quantum system [10]) 20 million-qubit quantum computer" [11]. As reported by IBM, 2048-bit RSA is again a current "high-strength" standard [12]. Without intervention, this debilitation can make a large amount of data vulnerable.

Cryptographic Algorithm	Type	Purpose	Impact From Quantum Computer
AES-256	Symmetric key	Encryption	Secure
SHA-256, SHA-3	–	Hash functions	Secure
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Effect of Quantum Computers on Current Cryptographic Algorithms [6]

Firstly, the weakening of asymmetric encryption finds a specific point of security loss in digital signatures, which are used for identity confirmation [13]. This has the potential to extend widely. For example, SWIFT (The Society for Worldwide Interbank Financial Telecommunication) uses RSA-2048 to authenticate transactions [14], opening doors to mass theft. As financial systems are highly critical, underpinning living standards and order, maintaining the economic stability of a nation is highly motivated. Governments being the main access point to these vital public organisations and evidently having a large influence on civilian and corporate action, their intervention in implementing prevention schemes will be

significant. With public organisations, this can manifest as a general decisive haste, and with private organisations, legal imposition is a reasonable possibility considering the potency of the issue.

Furthermore, digital signatures are used in a process known as code-signing, involved in validating the integrity of software [15]. Without this validation, the spread of malware (malicious software) becomes a possibility posing a considerable threat to critical systems. In one case, the Natanz nuclear facility in Iran malfunctioned due to a worm, known as Stuxnet, as a direct result of a code-signing vulnerability [16]. Clearly, preventing damage to critical infrastructure is important to governments, and government intervention will exist in some form, perhaps by funding research in prevention schemes or strengthening the security of critical systems through government projects. With malware being widespread and systems often being interdependent, a large-scale implementation of quantum-secure methods is important. Through the aforementioned means, government intervention will be a key aspect of this ambitious solution.

Digital signatures are also used in the encryption of data-in-motion, relating particularly to communication. TLS (Transport Layer Security) is the most utilised protocol for confident communication and has applications in internet traffic, emails, and wireless transmission [17]. As it includes asymmetric algorithms as part of its structure [18], this weakening creates a susceptibility to man-in-the-middle attacks [19], allowing a hacker to change the messages between two devices [20] with the associated risk of data leaks. Focusing on communication, government intervention is deeply motivated in protecting the integrity of data. If, for example, sensitive national data or personal information is leaked, the nation may face a strategic loss related to sensitive developments, classified records, etc. Further, its trade relations may be soured, which can make it difficult for the nation to develop economically and maintain its peace, leading to a negative civilian response and drops in living standards. If asymmetric encryption collapses internationally, the effects are more complex as damages will be more evenly distributed amongst nations. With mass panic and severe damages to the international economy for the reasons previously mentioned, an anarchistic development is not an unreasonable assumption. As such, government intervention would ideally mean intervention coordinated between multiple governments. This is rather complicated, as not all international relations are perfectly conducive to cooperation, though an optimal, mutually beneficial solution calls for it. This may begin by spreading awareness of the issue, and continue with global summits involving a diverse array of parties held to discuss the details with subsequent implementation.

In effect, the collapse of asymmetric encryption prevents sensitive data transfer from occurring successfully. Though this is true on an individual level, the impact would perhaps be more pronounced in large, societally influential organisations such as governments and corporations where targeted attacks are more likely to occur.

Without cryptographic alternatives, data leaks could destabilise large portions of the market. For example, similar attacks on modern scales cost the health sector in the US more than $7.8B in 2021, also leading to suspended operations [21]. As such, online communication becomes too volatile a mode for common use. This may mean a reversion to physical methods of communication, but the practicality of this in a globalised world is questionable when considering the amount of data transferred at a given time. Attempts to refine our infrastructure to facilitate this may incur a large financial cost. Overall, the restructuring of the market and reduced economic opportunities can lead to a considerable reduction in the standard of living. From the perspective of a governing body, these notions alone provide major impetus for devising preparation schemes. From here, potential government intervention appears to at least be twofold. The transition to safe cryptographic alternatives could be mandated and facilitated for public critical infrastructure and, desirably, private organisations. Further, open research towards strong quantum-secure algorithms is vital, and inter-government incentivisation and funding can be useful in this regard, working simultaneously to reduce the privatisation of research data. The former point implies a high level of government intervention, especially if the route of strict legal mandates is taken, whereas the latter only moderately requires it, mainly as research can be incentivised through other means.

The Risk of Harvest Now, Decrypt Later Attacks

Although we have discussed the vulnerability of data-in-motion, stored data is often protected using symmetric encryption, which has advantages in handling larger-sized files and in resource efficiency [22]. For example, the NIST approved AES to protect “sensitive, unclassified data” in 2001 [23], and “TOP SECRET data” in 2003 [24]. However, although sufficiently large AES (a symmetric encryption algorithm) is quantum-safe [25], other symmetric algorithms, such as 3DES (Triple Data Encryption Standard), are not necessarily so, in this case due to limited key lengths [26].

	DES	3DES	Blowfish	AES
Key length	56 bits	112 or 168 bits	448 bits	128, 192, or 256 bits
Block Size	64 bits	64 bits	64 bits	128bits
Developped in	1975	1978	1993	2000
Speed	Slow	Slow	Fast	Fast
Security	Not secure enough	Not secure enough	Secure enough	Excellent security
Structure	Feistel	Feistel	Feistel	Substitution Permutation
Time Required to Check All Possible Keys at 50 billion Keys per second	400 days	800 days	~3200 days	$5 \times 10^{21} days$

Contemporary Comparison Between Symmetric Encryption Algorithms [27]

At the same time, 3DES is an NIST-backed standard for government files through 2030 [28]. Although this may not seem like an issue, especially because quantum computing power is unlikely to be realised to significant attacking capacities by then (reasonable, albeit imperfect estimation) [29], there is a consequential concern due to "Harvest Now, Decrypt Later" attacks, in which attackers store encrypted versions of sensitive data waiting for the emergence of quantum computers for decryption [30]. In essence, data encrypted via a non-quantum-safe method now is susceptible to future leakage, which has manifold noticeable concerns. In fact, in a 2022 Deloitte poll of 400+ organisations, 50.2% considered it a threat to "sensitive, persistently valuable data" [31]. This stresses the importance of haste in implementing quantum-secure algorithms, so as to reduce this period of vulnerable data collection. Government intervention will likely play a large role in creating urgency, especially as they have legislative, mandating power that can be utilised here, the resources to support transition en masse, and the ability to manipulate critical network infrastructure, implying high-degree intervention.

Although AES functions as a replacement for 3DES (and DES), they maintain contemporary use in various internet protocols [32], with financial use cases in credit cards, for example [33]. Although predicting the extent of this threat is precarious due to the gradual shift away from 3DES, the algorithm and its precursor were prior NIST standards [34], evidently encrypting sensitive data in numerous fields. Therefore, the topic of interest becomes the longevity in their value. For example, in an individual/commercial context, data with long-term value can include banking details, hidden company USPs (Unique Selling Points), National Insurance numbers, etc. One can see how this creates possibilities for shifts in social/power dynamics, with access to said data potentially opening doors to blackmail (pressure by threatening to reveal private data [35]) and identity theft ("unauthorised use of a person's distinguishing information for illicit reasons" [36]). Government intervention is deeply motivated here in upholding ethical standards, maintaining public order, and ensuring national security. As 3DES is being phased out, the potential hazard is fairly minor, however governments should ensure critical infrastructure utilises AES and other quantum-secure symmetric algorithms. As communicated data can also be intercepted and stored, the aforementioned points of efficient implementation and incentivisation by governments is reapplied.

The Potential Political Impact

In a political context, using the US government as an example, the term of "classified status" in data generally has an upper limit of 25 years according to "Executive Order 13526" [37], though their utility can conceivably outlast this. For example, the VENOVA program operated from 1943-1980 decrypting past "Soviet telegrams" throughout the term [38]. According to "Stanford Senior Research Scholar" Herbert Lin, the hacking of foreign parties is conducive to poor

international relations [39]. When considering the spread of classified data such as “military operations, national system vulnerabilities, nuclear programs”, etc. (as per EO 13526), exacerbating these relations becomes a likelihood. Here, one should be cautious in extrapolating an outcome - hostile action is dependent upon various factors. (the usage of weapons of mass destruction, ally behaviour, global economic factors, etc.), but it does strengthen capacity, which is a complex problem in and of itself. Government intervention in ensuring the security of critical infrastructure (including government data centres) is practically required, especially as the alternative could mean political instability and a strategic loss for that nation as discussed earlier. Further, if politically sensitive, purposefully unpublicised data is leaked, whether that be in the form of immoral action or adverse plans, and this knowledge is spread amongst civilians, the gap allowing citizens to assume the morality of the nation will likely contract. If this image were to falter, this once again has anarchistic connotations. Though the social factor is difficult to predict, it is clear that governments collectively would not benefit, and their control over the storage of classified data means that their strong intervention in ensuring the implementation of suitably tested, rigorous encryption algorithms is important.

Significant Data Breaches Already Occur Globally [40]

Another potential extension of this idea is ‘internet sovereignty’ (the extensive territorial control of the web [41]), essentially dividing the internet. For example, the IT armies of Ukraine have performed successful DDoS attacks (overloading a host/network with traffic from multiple sources, preventing it from processing normal requests [42]) against the “Russian Kremlin, the Duma, and the state-owned media service Russia Today" [43]. This was likely a considerable factor towards the

recent move by Russia towards digital isolation, among other factors such as censorship [44]. Ultimately, this is speculative, but with the stressors of both individual and national security failures due to the malicious use of quantum computers, it becomes a justifiable viewpoint to hold. Government intervention by improving security standards to reduce the leakage of politically sensitive data is once again likely. If the nation is forced to largely scale back its network infrastructure and retreat into internet withdrawal, reverse globalisation will have a largely negative impact on its trade relations. Strong implementation schemes will be best handled if large-scale inter-government cooperation occurs.

A Clear Solution for Future Data

Fortunately, alternative asymmetric algorithms thought to be secure against quantum computers have been set by the NIST [45], which essentially cover the asymmetric use cases described above. Furthermore, Quantum Key Distribution (QKD), where "information of the private key is linked to the physical properties of particles displaying quantum behaviour" [46], is an alternative solution [47]. Because of its technical impracticalities (e.g. specialised hardware requirements), it may not be the "cheapest/most maintainable" choice [48], though it may potentially find a place in more sensitive, specialised areas such as government networks. Though these solutions have the potential to protect future data, past data and certain impracticalities which shall be discussed in the "Means of Government Intervention" section still enable significant points of residual risk. Nonetheless, controlled government intervention in ensuring suitability and a smooth mass implementation is key to reducing vulnerabilities.

Algorithm	Algorithm Family	Security Level
Classic McEliece	Code	5
Saber	Lattice	1, 3, 5
Crystals-Kyber	Lattice	1, 3, 5
NTRU-HRSS	Lattice	1
NTRU-HPS	Lattice	1, 3, 5
Crystals-Dilithium	Lattice	1, 2, 3
SIKE	Isogeny	1, 2, 3, 5
SPHINCS+	Hash	1, 3, 5

Adapted Table of Quantum-Secure Algorithms [7]

Theoretical Societal Threats To Finance

The Collapse of E-Commerce

According to the UNCTAD (United Nations Conference on Trade and Development), “worldwide e-commerce sales reached $25.6T in 2018 (30% of the global GDP)”, while showcasing an upwards trend indicating e-commerce growth [49]. In the case of weakened transaction security and the proliferation of financial crimes, online transactions can become too volatile to sustain. Subsequently, a major collapse in e-commerce is a likely consequence with a rather drastic impact on economies at large. As these consequences are difficult to handle after-the-fact, strong government prevention is highly incentivised once again.

To add, as per the OECD (Organisation for Economic Co-operation and Development), small businesses are 13% more likely to sell on “online platforms” than larger ones [50]. Considering their lower market shares [51], being forced to switch to physical stores and in part rebranding imaginably leads to a stronger challenge and a greater failure rate. Furthermore, the FSB (Federation of Small Businesses) reported that small- and medium-sized enterprises accounted for approximately 61% of UK employment in 2021 [52]. Overall, this lends itself not only to reduced entrepreneurship, but also major job losses and declining standards of living. Where unemployment has been linked to ill-health and a poorer quality of life [53] and economic recessions to greater rates of “depression, anxiety, and suicide” [54], this is very likely to have an exacerbating effect, such as that of the aggravating impact of the public response to the 2008 Financial crisis [55]. As stated, the social outcry of mass infrastructural failures and a loss of civilian trust in the ability of a government to maintain a stable economy and set of living standards is a primary motivator for government prevention to a great extent. In addition to what was stated in the cybersecurity section, this may involve close interaction with financial institutions as a means of both efficient implementation and reputation management.

The Devaluation of Cryptocurrencies

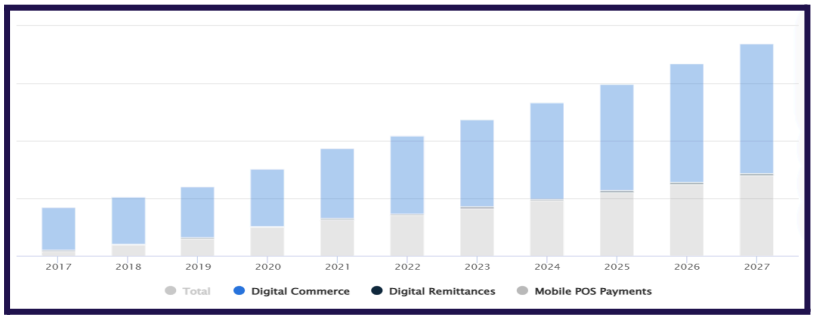
Furthermore, the shock to the system of cryptocurrencies resulting from the potential of unauthenticated transactions can be paralleled with prior major crises. For example, the 2018 hack of the “Coincheck Exchange” saw $530 million by value in NEM (a cryptocurrency) dishonestly obtained, leading to notable price volatility and substantial price plummets [56]. This showcases how reduced security can lead to lower investor confidence and spending, which may influence the larger market and those who own such assets. Furthermore, the security of CBDCs (Central Bank Digital Currencies), “digital, state-issued currencies not connected to physical items” [57], would be threatened. According to the Atlantic Council, 11 countries have

already had “full-scale launches” [58], making it an appreciable global issue. In the case of cryptocurrencies, government intervention may not be required to a great extent. Though their value to some individuals could lead to drops in living standards, these effects would be localised and have a chance of passing without catastrophic repercussions elsewhere. To note, this analysis is only a reflection of current conditions and may change with time. However, CBDCs with their direct link to national currency and potentially widespread use going forwards could invoke greater government intervention, taking the form of maximising robustness, making infrastructural changes if necessary, spreading awareness, etc. In fact, as CBDCs are novel, governments can develop them with quantum-secure algorithms in mind.

The Fundamental Issue of Practicality

In general, as the ownership of online currency becomes ambiguous, online transactions will be too insecure for use. Without sufficient protection, a reversion to solely using physical currency may become the only solution on a large scale. Granted, the finances of everyday individuals and small firms may not be targeted by hackers, but the idea that they can warrant some form of response by financial institutions and governments. Furthermore, their susceptibility to insider attacks, for example, should not be ignored.

According to a Statista report, “the yearly growth rate of the value of digital transactions is estimated to be 11.80% from 2023-2027” [59]. As transaction volumes increase, purely using non-digital means can be difficult to sustain, leading once again to issues in practicality and restructuring. Government intervention optimally exists in the same vein as discussed earlier - through strong prevention. Restructuring towards physical transactions or highly closed networks will not only be expensive with the changes in network infrastructure required, but their productivity will inevitably be poorer than what we currently have due to weaker communication and trade links. Economically, this will undo progress, likely leading to drops in GDP and potential infrastructural issues, motivating governments once again towards active prevention. With that said, further, more complex issues exist outside of cybersecurity, where quantum-secure algorithms are a reasonably reliable solution.



Recent and Forecasted Annual Transaction Value in Digital Segments [59]

The Potential Mechanisms of Dividea

IBM lists "Trading Optimization", "Targeting and Prediction", and "Risk Profiling" as the "three primary categories of financial use cases" [60]. As quantum computers likely will be costly due to their production and maintenance costs [61], it is probable that they will only be readily usable by large, wealthy organisations - especially those already involved in research and development. These organisations are likely to experience "increased returns through cost cutting, greater efficiency [62], improved analytical capabilities, a greater capacity to identify consumer behaviour/wants and maintain more effective marketing [63], a marked improvement in decision-making potential [64] through the speed-up of Monte Carlo simulations (often used in risk analysis)" [65], and a more competitive performance in saturated markets.

The extent of government intervention here is a complex, multifaceted topic, with both extremes of the argument being controversial. On the one hand, governments can avoid intervention entirely and enable dense wealth concentrations in the private sector. Despite the anti-competitive implications, there are real-world parallels in the form of existing major corporations that dominate their respective markets. Further, a conclusion stating that enabling dominant companies to flourish negates the efforts of small businesses, though partially coherent, has nuances that detract from its accuracy. Largely, this may be due to the sheer breadth of potential innovation leaving space for incoming talent and controlled government restrictions that manipulate the market intelligently. To add, these massive corporations and their hypercompetitive markets often breed scientific advancement and infrastructural progress, while providing job opportunities to the working population. Clearly, the advantages of a free market question the other extreme of complete restriction and a ban on the use of quantum computers entirely. Firstly, this is unrealistic as human curiosity and the desire to progress technologically is persistent, and healthy, free regimes will find difficulty in circumventing this especially in the long-term where access to quantum computers may become more theoretically feasible and extend beyond dense localities. Further, the attempt to restrict development may be viewed as a political shift, opening doors to resistance, though pressure is unlikely to come from everyday civilians considering the niche nature of the topic unless it is marketed in an unexpectedly far-reaching manner. However, considering purely the potential of quantum computers and their theoretical dangers, it would be advisable for governments to communicate openly and discuss whether strict restrictions should be imposed at this budding stage. At the very least, a level of control and understanding should be maintained by governing bodies, and this is most practically achieved by an open dialogue and technologically able staff, implying a high degree of intervention in either case. Overall, different mechanisms of divide can lead to different outcomes which we shall explore in this section.

- Divide In R&D: In effect, when a restricted portion of the market has access to high computational power, it is conceivable that this relays significant competitive advantages from a production standpoint, which can manifest in dominant market shares and trends towards monopolies. With research and development, we can see this effect when considering the use of supercomputers in the AI market. With AI-training, Google with its Cloud Tensor Processing Unit [66], Microsoft with its Azure-hosted model [67], and IBM with Vela [68], all examples of high-computational prowess, have aided their occupying significant market share in the AI market as listed in a Grand View Research report [69]. It is conceivable for quantum computers to emulate this behaviour, especially considering their further potential capacity for processing power [70]. From the perspective of realising innovation, this technological gap acts as a barrier for smaller firms, reducing the likelihood of startup success going forwards. Clearly, government intervention does not seek to completely equalise the size of all businesses, but rather prevent consumer oppression by monopolies and leave growth opportunities for aspiring entrepreneurs. The importance of research and data processing is not integral to the entire business world, so government intervention will likely be balanced and focused on certain sectors. Further, regarding the possibility of a ban on quantum computers, it is difficult to justify heavy restrictions on innovation unless the threat is clear (an international consensus that this technology is dangerous remains unlikely), so intervention will likely be after-the-fact and symptom-based.

- Stock Markets & Trading Dominance: Studies have already discussed the technical niche of quantum computers in financial markets [71][72][73]. In essence, this brings lower-risk trading speed [74] to a wealthy minority. A report by the Government Office for Science, London has considered this effect being financially harmful towards “slower, manual traders”. Furthermore, the report posits that at a certain point, “this speed advantage will nullify the effect of humans in trading systems” [75]. Though this is complex, a clear extrapolation of this idea is that a dense concentration of wealthy parties will have a disproportionate influence on the stock market. This idea can be seen in other sources. For example, a Time Magazine article suggests that “large institutional investors… can contribute to shifts in stock prices.” [76]. With high-frequency trading being associated with market volatility [77], this has largely negative economic implications and may change the demography of traders. The notion of private organisations having a significant influence on financial systems would be cautiously considered by governments as, in some manner, it can destabilise an otherwise clear hierarchy. However, trying to diminish this influence by reducing the quality of technology available to businesses can be seen as anti-capitalist, leading to a complex argument of a suitable political structure of a nation in changing times. These points should be made, as stated before,

in governmental discourse within international summits or similar media. To add, the true complexity of a stock market is beyond the scope of this essay and there remains the possibility of a healthy one despite the range of capacities in its participants. In general, balanced intervention in addressing problems as they arrive is likely.

- Lucrative Niche Market Capture: According to Forbes, a niche market is a "specialised market inside a larger one involving an unfulfilled customer base with specific wants" [78]. Currently, with smaller firms falling behind in performance and experiencing fewer growth windows [79], their success is becoming less likely. However, a clear strategy to combat this is through innovation in an untapped market. This First-Mover Advantage [80] has been shown to lead to early market share capture [81] placing the business in a more competitive position thereafter. Successful examples include Amazon ("first open-to-all, online bookstore" [82]), eBay ("first open online auction site" [83]), and Apple ("first successful touch-screen smartphone" [84]). The argument for this is especially true when considering that saturated markets show stagnant demand [85] and research considers that approximately 50% of small business failure can be attributed to a deficiency in innovative practices [86]. However, if quantum computers lead to a clearer picture of the trends in consumer behaviour (while R&D also improves innovation), the wealthy organisations owning them can better identify these untapped markets and subsequently fill them. Though this argument has nuances, especially as innovation can be argued to come from ingenuity as opposed to computation, analysis can still be a powerful tool. In this way, major small business success becomes less probable. As stated earlier with R&D divide, these nuances mean that balanced, after-the-fact government intervention focused on certain sectors is experimentally the safest way to determine policy. Governments can consider restricting quantum computer use until prices drop or developing shared quantum computing schemes as methods of stronger intervention, though these require further governmental discussion.

- Quantum Technology Patents: According to WIPO (World Intellectual Property Organization), a patent is "an exclusive right granted for an invention, which is a product or a process that provides, in general, a new way of doing something, or offers a new technical solution to a problem, allowing any unauthorised commercial use of patented products to be pursued legally" [87]. Though they serve to protect intellectual property, a 1994 survey of the "US manufacturing sector carried out by Carnegie Mellon" showcased patents being used mainly as barriers to competitors [88]. An example in technology can be found in Apple's blocking patents, which were cited to reject later patent applications by other parties, with "16,000 of these blocking patents leading to 147,000+ patent rejections in July 2023" [89], evidencing this barrier effect. From 2001 to 2021, the amount of accepted

patents in quantum technologies was 20,583 (albeit some being time-sensitive and publicly available) [90], which has significant implications. By using patents as a means of disabling parties from entering quantum computing production, patent owners have a major head start in innovation. In other words, they lack the inertia that other parties may suffer due to the extensive utilities they solely possess. Currently, an Oxford University Press article states that IBM, Northrop Grumman, and D-Wave have the biggest patent collection in quantum computing [91]. As developments continue in an early stage, there is still a sizable space for new entry, although the disadvantage may lean on smaller businesses and startups in the future. Governments can intervene to a great extent here due to their influence on patent provision. To allow space for startup involvement, ensuring that the majority of patents provided are made publicly usable, though decisive and strict against innovators, is possible. Rejecting these patents entirely exists in a similar vein, and harkens back to the idea of political structures. This should be done with caution and a degree of certainty as, once again, this has anti-capitalist, though justifiable, connotations.

- Wealth Divides Between Nations: Of the "top 18 quantum computing research institutes in 2022" according to the Quantum Insider (via Microsoft Academic data), 13 are located in the US, including the NIST [92], an "agency of the US Department of Commerce" [93]. Furthermore, "the US reportedly has 54.18% of patented inventions in quantum technologies (excluding cryptography), with China at 16.68% and Japan and Canada following" [94]. Concentrations of research and development in certain locations should be treated with caution. If the balanced government intervention discussed is implemented to reduce the negative economic impacts of quantum computing, its computational power can conceivably be an economic tool for countries. However, if these benefits are experienced solely by global superpowers, this has the potential to widen existing inequalities. This is especially true when reconsidering the concept of "inertia" in development. When developing countries have further existing infrastructural issues, focusing on closing this particular gap can become impractical allowing the challenge to grow with time. Extrapolating from here would have to be done with caution, especially as the upper limit of quantum computing power is unknown. If it grows to become a powerful commodity, technologically weak governments may become even less competitive, while other parties gain a strong negotiating power against them, for example. The inevitably strategic attitudes of governments make this issue challenging to resolve, and it is conceivable that the existence of this technological gap is partially desired by superpowers in maintaining control. Ideally, government intervention by these parties should involve extending support to a significant extent and intervention by weak governments should seek to maximise engagement with this technology.

Means of Government Intervention

Much of the complexity of the points of residual risk owes to their solutions requiring a compromise by conflicting parties. Furthermore, political factors can blur ethical lines and make finding an answer all the more challenging. In this section, we will consider each point of residual risk individually, such that we can explore their multiple angles and understand fundamentally the source of debate and complexity.

1. **Harvest Now, Decrypt Later Attacks Create Vulnerabilities in Stored/Transmitted Classified Information, Threatening Data Leaks:** With Harvest Now, Decrypt Later Attacks, previously intercepted data encrypted through quantum-insecure means is already threatened. As such, a swift, well-structured switch to quantum-safe algorithms encouraged by governments is a necessary part of the solution in preventing further damage. For example, the White House has already encouraged a “move to quantum encryption” with restructuring ongoing in US government agencies [95]. Organisations are incentivised to perform this restructuring themselves for their own security, though in national security cases, there is an argument that legal, government-backed impositions must be placed at least on privately-owned critical systems, such as hospitals and financial services, regarding their cryptography. For example, according to the FTC (Federal Trade Commission), the Gramm-Leach-Bliley Act “requires financial institutions to protect sensitive data” [96] showcasing precedent. With that said, the spreading of awareness and rooted education is equally an important step, such that parties know of the importance on both localised and wider scales of prevention. Regarding existing sensitive data, partial solutions may exist. For example, user banking details may be changed and users notified after a switch to quantum-safe algorithms, evidently backed through government legislation and decisiveness. In effect, the long-term value of older data can be purposefully reduced, further exemplified by credit card expiration dates. Though this is not universally applicable (e.g. hidden company USPs are fixed) and such drastic restructuring may be time-consuming and expensive, it may also be a working solution in a worse-case scenario for the economy. Clearly, a sizable degree of government intervention is required here.

2. **Uncertainties In The Advancement/Potential of Quantum Computing is Challenging to Prepare For, Making Early Preparation Unreliable:** The issue of the current unpredictability of quantum computing, as its development is predicated on a breakthrough in error correction [97], makes knowing how to prepare difficult. Furthermore, it being a relatively new field of study creates further potential for newfound discoveries. The problem is, by its nature, not completely solvable, and the only imaginable way to lessen

its negative impact from a governmental point of view is by further funding and encouraging research in the sectors of quantum computing and associated fields of study. In this way, further academic awareness is brought to the topic, which can help work towards an open ethos in quantum computing development. Fundamentally, breakthroughs in knowledge are required in this instance to forestall breakthroughs in cryptographic gaps, and this is a clear means to reduce this risk. The extent of government intervention in funding will vary based on expert analysis, though it will likely parallel the developmental progress of quantum computers.

3. **Longevity in Post-Quantum Cryptography Migration Creates Potential Vulnerabilities Within That Time Frame:** The core of this issue lies in practical difficulties and the novelty of PQC algorithms. As such, part of the solution is enacting a change in perception within the parties involved in the process. For example, governments spreading awareness of the urgency of migration, including global forums held regarding its necessity to foster public discussion. Furthermore, to address a lack of workforce capacity in implementing these algorithms, governments sufficiently restructuring higher education systems to teach their implementation becomes vital. While the human factor is being addressed, technical work should be done to facilitate a straightforward migration. For example, varied frameworks and platforms could be created through collaboration between involved parties to enable the fast implementation of PQC algorithms within individual organisations and in multiple types of systems, where governments can provide support via funding and appointing organisations as a means of hastening and control. Research could be done on the compatibility of quantum-secure algorithms with current hardware standards. Here, legal mandates on critical systems may be reconsidered. Forcing a sudden switch in their encryption is somewhat precarious and perhaps suboptimal. Though it would dissuade the inertia associated with large organisations in beginning the process, much of the reason this longevity exists is because migration has practical difficulties to be cautiously overcome. As such, governmental mandates should perhaps involve leniency by allowing suitable time spans or by referring to a general movement (not a strict one) towards wholly quantum-secure encryption standards. With that said, this is ultimately dependent on how governments choose to implement this policy. Furthermore, this may involve governmental organisations appointed to occasionally assess the transitional progress of certain bodies (e.g. critical systems), though wide-scale debate should specify the extent of these audits for privacy reasons.

4. **Our Limited Understanding of Modern PQC Algorithms Leaves Room for Threats:** This shares parallels with the issue of unknowns in the potential of quantum computing. As such, governments encouraging and funding the academic research of PQC algorithms still exists as a method to reduce theoretical uncertainty. At the same time, as PQC algorithms exist tangibly, a practical approach can be taken. For example, governments encouraging security testing programs of manifold types and scales can highlight issues not previously contemplated. This may be through incentivisation, increasing the scale of testing and simultaneously spreading awareness. Furthermore, research into the scaling of these algorithms - whether they begin to show unexpected weaknesses when implemented within a large body - may be used as an indicator of confidence during migration.

5. **Geographical Concentrations of Research Hubs Widens the Technological Gap Between Developed and Developing Countries:** This technological gap, seen by its persistent nature, is highly challenging to solve, involving the idea of eradicating inequalities between countries at all levels physical and psychological. This idea carries an uncertain optimism making it difficult to move forward. Nevertheless, it is worth discussing, especially with access to views held by educated professionals in the field. Theoretically, if a government strengthened its workforce, lined up its citizens' attitudes with future progress, and suddenly expanded and deepened its body of technology while building competitive research infrastructure with global cooperation, the problem would be soothed. This would have to occur through a great extent of initiative in the government as external legal influence would impose on the sovereignty of the nation, making recommendations complex to craft. Here, perhaps a method towards progress may be seen by governments organising global summits involving a range of countries of diverse economic situations regarding quantum computing and generally technological progress. In this way, though solutions would still not be immediately obvious, international governmental cooperation and communication can bring about positive change. A UN Chronicle article suggests that this issue is "not a result of a lack of political will and control in LDCs" (Least Developed Countries), though that is a complex claim. Nevertheless, it continues on to consider "insufficient investment in R&D, low educational participation, deficient progress-enabling policy, a lack of internet access (a limited access to broader knowledge), etc." as limiting factors [98]. The problems endured by LDCs in this aspect requires time to soothe, making slowing down the development of quantum computers after inter-government discourse the most direct answer. However, progress has an inevitability to it and legally halting the generation of ideas is impossible. Of course, government intervention can be made more potent through barriers to production, however that has a very low likelihood of working partially due

to the nature of its users and the strategic benefits potentially afforded to the nation itself.

6. **The Withholding/Privating of Information Related to Quantum Computers By Researching Parties Prevents the Open Discussion of Quantum Technology Development. This May Stifle Innovation and Can Be Used in an Anti-Competitive Manner, Furthering Divide:** This has flavours of the debate of the right to intellectual property. On the one hand, if a party has invested fiscal and mental resources towards making progress in the field, they are entitled to solely be rewarded for their efforts. On the other hand, considering a select few parties are capable of such investment, this withholding extrapolates to the benefits of this knowledge being highly concentrated. What makes this issue uniquely challenging is the potential power of quantum computing, which can create an incredibly competitive environment not only between organisations, but potentially nations. As such, governments calling for a completely open discussion by disabling this withholding from occurring is impractical, mainly because it is unlikely to be implemented. Nevertheless, it may be considered. Furthermore, for a government to know whether something is being withheld, there must be deep audits carried out on powerful organisations, which introduces the debate of privacy and government imposition. To add to that, these audits would have to be carried out by an authoritative government that fundamentally believes that privating information is dangerous, positing the question of whether one actually exists. Here, the extent of government intervention is likely great, though how it manifests is dependent upon the goals of that government, thus not being a question of ethical ideals.

7. **The Use of Patents to Prevent Quantum Technology Development by Upcoming Parties Can Disable Access to Upcoming Organisations in the Sector and Stifle Innovation:** This shares similarities with the utility of withholding information to gain a competitive advantage, where larger, more powerful organisations have a greater capacity for innovation, and thus are the largest restrictors of new entry. However, there are a few differences worth considering. For one, in many cases, knowledge can eventually be gained by external parties even if it is withheld. This is due to the idea that for knowledge on quantum technology to be useful, it must be implemented physically. From there, any deep level of observation by an external party, a simple audit of the quantum computer by an authority, or insights by media outlets can reveal this information to the public where it can be used thereafter, albeit at an uncompetitively late time. Patents however, are legally backed structures preventing the utilisation of known, important information, entailing that they more concretely facilitate this divide. On the other side of the coin, although the pursuit of knowledge and gaining of information cannot be legally blocked, quantum technology patents, being legal

structures, can be denied and regulated by governments meaning that this issue is more controllable. For example, a potential solution is governments not issuing patents for quantum technology/computers at all, thus allowing for a more open, accessible market sector, or in the same vein, ensuring quantum technology patents are available for 'licences of right', meaning that "though the innovations are patented, they can still be freely used by external parties" [99]. Here, though the extent of government intervention can vary, it is likely to be on the high end.

8. **A High Cost Barrier Enables Only Wealthy Organisations Benefiting From Quantum Computers, Reinforcing Wealth Divide and Monopolies, While Hindering the Growth of Startups Due to the Technological Gap:** As production processes improve over time, the price of quantum computers may drop naturally and become more accessible, thus nullifying the issue. However, by the nature of quantum technologies, whether significant improvements leading to reasonable prices can actually be achieved is an uncertainty. Furthermore, high initial prices may lead to temporary wealth divisions, perhaps with longer-lasting ramifications. Potentially, distributed open-access systems, where multiple people have access to sections of quantum computers hosted by a larger organisation for particular time slots may be a solution that governments can back through funding and further incentivisation. For example, the IBM Quantum Lab allows an individual to run their programs on quantum circuits freely via a cloud-based service [100]. Although this spreads quantum computing power, the capacity of these limited circuits would likely pale in comparison to the sole-serving quantum computers of industry leaders, thus still leaving the mechanism for wealth divide open. Government intervention, in its authoritative nature, will be required to close this, if closing this is necessary in the first place. Essentially, governments are unlikely to want to completely repress the self-improving actions of large corporations due to the advantages they confer, but would prefer if small companies had inroads to becoming large and if large companies did not become anti-competitive, suppressive monopolies (speaking generally). As such, the optimal extent of government intervention lies somewhere in between a total ban on quantum computers and complete inaction, and the exact point depends on various factors such as the government's political structure, how invasive quantum computers become in the future, etc., though it appears that the resulting extent of active government intervention should be fairly strong. Furthermore, if the interfaces between business users and quantum computers are mediated by self-servicing parties, such as anti-competitive monopolies, then significant data interception can occur potentially leading to bad faith practices. As such, open-source access to host quantum computers should be viewed with caution from the perspective of security. More drastic intervention, such as governments legally preventing the commercial use of quantum computers

until a certain accessibility threshold (e.g. a low-enough price) is reached may be considered. Granted, this would only be considerable if quantum computers existing at the time are sufficiently powerful to exert a monopolistic influence on the market that cannot be disregarded. Presuming this scenario, there still exists complexities regarding choosing which parties are allowed to use quantum computers. This selection in any case would have to be done by the nation's government as an overarching authority, entailing a high degree of intervention. For example, essential, infrastructure-focused fields such as medical research and cybersecurity using this technology may not lead to overly monopolistic consequences, while the benefits involved are significant, so they may be exempted. There are further complexities when considering defence as all countries would have to mutually agree to cease involving quantum technologies in their defence programs and act in good faith, which is a fragile requirement. To add, defining how quantum computers are being used in an anti-competitive manner in a way that can be legislated by a government and is sufficiently specific may be challenging. As an example, placing complete fault on a business for purchasing and benefiting from using a quantum computer is not an easily justifiable act. Nevertheless, exploring and discussing the effects of potential usage limits may be important going forward, and from these findings, government intervention is likely to be significant.

Conclusion

The question, "To What Extent Will Intervention Be Needed During the Advent of Quantum Computing?", remains complex. Optimistic assumptions about the distribution of quantum computers, their accessibility, their computational power, and their use cases have been made throughout this project, all leading to theoretical ethical issues with high levels of difficulty which may never come to be. Some extremely theoretical issues, such as the strong negotiating power possessed by private quantum-computer owning companies against technologically underdeveloped governments/authorities, the impeded growth of startups due to the rapid identification of niche markets by large quantum-computer owning firms, the usage of quantum computers to analyse data and consumer behaviour being an infringement of privacy and autonomy, and the dominating influence of quantum computers in the stock market conferring advantages on to monopolistic quantum-computer owning parties, have not been discussed because of this reason (and their scope), though they should at least be mentioned for completeness. With that said, from the discussed solutions and points of residual risk, an understanding of some of the potential underlying problems can be obtained.

Though much relies on the grassroots level, where implementation and real practices will occur, intervention will clearly be needed to steer organisations and parties in the correct direction - that is, to minimise disruption to current infrastructure. This form of intervention may partially be facilitated by governments through the opening of relevant educational avenues, for example, and may also arise naturally as interest grows in the field during a period of increasing demand. Legal intervention is also a common theme throughout this paper, though its implementation requires a more open discussion. On a national level, this aims partly to prevent security issues from damaging systems in the country, but can extend to anti-monopolistic legislation by governments to alleviate wealth inequalities. In such situations, the case for government intervention becomes stronger, though serious complexities arise when considering nations attempting to control this rampant progress. As quantum computers have the potential to become strategically valuable to nations and their economies, hindering their use partially weakens their position from the perspective of competitiveness. However, leaving it uncontrolled may open doors to the exacerbation of current issues. As such, the policy surrounding quantum computers must be crafted cautiously and be sufficiently strict, while enabling controlled mechanisms for growth, which will become a strategic challenge similar to the ongoing battle of legislating internet governance [101]. From an optimistic perspective, the greatest chance of society achieving a balanced relationship with quantum computing power may come with strong intergovernmental cooperation, especially as this weakens the incentive for high–level competition. As such, nations can focus on the localised issues that quantum computers may bring, such as growing technological/wealth divides, without needing to concern themselves with external competition compromising their progress. Despite such a scenario being unlikely, the importance of global discussion at the very least appears substantial.

Overall, to defend against the potential collapses and ethical missteps of high computational power, a substantial amount of intervention is likely to be required, to the point of at least a consideration of the merit of the technology in the first place. This challenge is both a task requiring international cooperation and communication and a balancing act between progress and limiting the growth of challenging issues. In practice, this is likely to vary with the changing attitudes of people and governments as the development of quantum computers unfolds.

Bibliography

[1]: Kulkarni, V. (2020, September 29). *The Inconvenient Truth About Quantum Computing*. The Wire. Retrieved June 1, 2023, from https://science.thewire.in/the-sciences/quantum-computing-qubits-error-correction-no-cloning-theorem/

[2]: (2023, May 1). *What is quantum computing?* McKinsey & Company. Retrieved June 1, 2023, from https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-quantum-computing

[3]: (2019, November 5). *Where is the Electron and How Many of Them?* Volkswagenag. Retrieved June 1, 2023, from https://www.volkswagenag.com/en/news/stories/2019/11/where-is-the-electron-and-how-many-of-them.html#

[4]: Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017, June). *An Introduction to Information Security*. NIST. Retrieved June 1, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

[5]: Simmons, G. J. (1979, December 1). *Symmetric and Asymmetric Encryption*. ACM. Retrieved June 1, 2023, from https://dl.acm.org/doi/epdf/10.1145/356789.356793

[6]: Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). *The Impact of Quantum Computing on Present Cryptography*. Arxiv. Retrieved June 1, 2023, from https://arxiv.org/pdf/1804.00200.pdf

[7]: Bavdekar, R., Chopde, E. J., Bhatia, A., Tiwari, K., Daniel, S. J., & A. (2022, February 6). *Post Quantum Cryptography: Techniques, Challenges, Standardization, and Directions for Future Research*. Arxiv. Retrieved June 1, 2023, from https://arxiv.org/pdf/2202.02826.pdf

[8]: Roetteler, M., Naehrig, M., Svore, K. M., & Lauter, K. (2017, October 31). *Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms*. Arxiv. Retrieved June 1, 2023, from https://arxiv.org/pdf/1706.06752.pdf

[9]: Kerry, C. F., & Gallagher, P. D. (2013, July 19). *Digital Signature Standard (DSS)*. NIST. Retrieved June 1, 2023, from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

[10]: Johnstun, S., & Huele, J. F. V. (2021, October 1). *Understanding and compensating for noise on IBM quantum computers*. American Journal of Physics. Retrieved June 1, 2023, from https://pubs.aip.org/aapt/ajp/article-abstract/89/10/935/859757/Understanding-and-compensating-for-noise-on-IBM?redirectedFrom=fulltext

[11]: Gidney, C., & Eker˚a, M. (2021, April 13). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Arxiv. Retrieved June 1, 2023, from https://arxiv.org/pdf/1905.09749.pdf

[12]: (2021, May 27). Size considerations for public and private keys. IBM. Retrieved June 1, 2023, from https://www.ibm.com/docs/en/zos/2.4.0?topic=certificates-size-considerations-public-private-keys

[13]: (2020, November 11). Preparing for Quantum-Safe Cryptography. NCSC. Retrieved June 1, 2023, from https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography#section_2

[14]: Tan, T. G., Szalachowski, P., & Zhou, J. (n.d.). *Challenges of Post-Quantum Digital Signing in Real-world Applications: A Survey*. IACR. Retrieved June 1, 2023, from https://eprint.iacr.org/2019/1374.pdf

[15]: Kozak, K., Kwon, B. J., Kim, D., & Dumitras, T. (2019, February 14). *Issued for Abuse: Measuring the Underground Trade in Code Signing Certificates*. Arxiv. Retrieved June 1, 2023, from https://arxiv.org/pdf/1803.02931.pdf
[16]: Singer, P. W. (2015). *Stuxnet and Its Hidden Lessons on the Ethics of Cyberweapons*. Case Western Reserve Journal of International Law. Retrieved June 1, 2023, from https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1009&context=jil
[17]: Bhargavan, K., Fournet, C., Kohlweiss, M., Pironti, A., & Strub, P. Y. (2013). *Implementing TLS with Verified Cryptographic Security*. IEEE-Security. Retrieved June 1, 2023, from https://www.ieee-security.org/TC/SP2013/papers/4977a445.pdf
[18]: Dowling, B., Fischlin, M., Günther, F., & Stebila, D. (2021, July 30). *A Cryptographic Analysis of the TLS 1.3 Handshake Protocol*. Springer. Retrieved June 1, 2023, from https://link.springer.com/article/10.1007/s00145-021-09384-1
[19]: Chang, Y. A., Chen, M. S., Wu, J. S., & Yang, B. Y. (n.d.). *Postquantum SSL/TLS for embedded systems*. Sinica. Retrieved June 1, 2023, from https://www.iis.sinica.edu.tw/papers/byyang/18988-F.pdf
[20]: Thankappan, M., Rifà-Pous, H., & Garrigues, C. (2022, December 30). *Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review*. Science Direct. Retrieved June 1, 2023, from https://www.sciencedirect.com/science/article/pii/S0957417422015093
[21]: Huang, K., Wang, X., Wei, W., & Madnick, S. (2023, May 4). *The Devastating Business Impacts of a Cyber Breach*. Harvard Business Review. Retrieved June 1, 2023, from https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach#:~:text=For%20example%2C%2060%25%20of%20organizations,to%2011.9%25%20after%20two%20years
[22]: Ahmed, A., & Naeem, M. (2022, March). *Analysis of Most Common Encryption Algorithms*. Research Gate. Retrieved June 1, 2023, from https://www.researchgate.net/publication/359686023_Analysis_of_Most_Common_Encryption_Algorithms
[23]: (2001, November 26). *Announcing the Advanced Encryption Standard (AES)*. NIST. Retrieved June 1, 2023, from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
[24]: (2003, June). *National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information*. NIST. Retrieved June 1, 2023, from https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/cnss15fs.pdf
[25]: Kirsch, Z. (2015, December 15). *Quantum Computing: The Risk to Existing Encryption Methods*. Tufts University. Retrieved June 1, 2023, from http://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf
[26]: Neha, K., & A. (n.d.). *Quantum Cryptography - The Future of Communication and Internet Security*. SciForum. Retrieved June 1, 2023, from https://sciforum.net/manuscripts/12637/manuscript.pdf
[27]: Sari, S. (2022, November 6). *DES vs 3DES vs Blowfish vs AES*. Baeldung. Retrieved June 1, 2023, from https://www.baeldung.com/cs/des-vs-3des-vs-blowfish-vs-aes
[28]: Barker, W. C., & Barker, E. (2012, January). *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*. NIST. Retrieved June 1, 2023, from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-67r1.pdf
[29]: Sevilla, J., & Riedel, C. J. (2020, December 9). *Forecasting timelines of quantum computing*. Arxiv. Retrieved June 1, 2023, from https://arxiv.org/pdf/2009.05045.pdf

[30]: Ott, D., Peikert, C., Hill, M., Drobnis, A. S., & Ramming, C. (2019, February 1). *Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility*. Arxiv. Retrieved June 1, 2023, from https://arxiv.org/ftp/arxiv/papers/1909/1909.07353.pdf
[31]: Pfaendler, S., & Graham, T. (2022, September 12). *Harvest Now, Decrypt Later Attacks Pose a Security Concern as Organizations Consider Implications of Quantum Computing*. Slideshare Deloitte. Retrieved June 1, 2023, from https://www.slideshare.net/DeloitteUS/harvest-now-decrypt-later-attacks-pose-a-security-concern-as-organizations-consider-implications-of-quantum-computing
[32]: Alanazi, H. O., Zaidan, B. B., Zaidan, A. A., Jalab, H. A., Shabbir, M., & Al-Nabhan, Y. (2010, March). *New Comparative Study Between DES, 3DES and AES within Nine Factors*. Arxiv. Retrieved June 1, 2023, from https://arxiv.org/ftp/arxiv/papers/1003/1003.4085.pdf
[33]: Dhanapal, R., & P, G. (2013). *RFID Detect Credit Card Skimmers using Neural Networks*. International Journal of Computer Science and Information Technologies. Retrieved June 1, 2023, from https://ijcsit.com/docs/Volume%204/Vol4Issue6/ijcsit2013040603.pdf
[34]: Barker, E., & Mouha, N. (2017, November). *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher Revision 2*. NIST. Retrieved June 1, 2023, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-67r2.pdf
[35]: Habsi, A., Butler, A., Percy, M., & Sezer, S. (2021). *Blackmail on social media: What do we know and what remains unknown?* Queen's University Belfast. Retrieved June 1, 2023, from https://pureadmin.qub.ac.uk/ws/portalfiles/portal/202125371/Accepted_Article.pdf
[36]: Burnes, D., DeLiema, M., & Langton, L. (2020, January 23). *Risk and protective factors of identity theft victimization in the United States*. National Library of Medicine. Retrieved June 1, 2023, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7013169/
[37]: (2009, December 29). *Executive Order 13526- Classified National Security Information*. Obama White House Archives. Retrieved June 1, 2023, from https://obamawhitehouse.archives.gov/the-press-office/executive-order-classified-national-security-information
[38]: (n.d.). *The Venova Story*. NSA. Retrieved June 1, 2023, from https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/coldwar/venona_story.pdf
[39]: Parker, C. B. (2016, August 11). *Cyberattack concerns real about U.S. Presidential election, Stanford scholar says*. Stanford. Retrieved June 1, 2023, from https://news.stanford.edu/2016/08/11/stanford-expert-cyberattack-worries-affect-elections/
[40]: (n.d.). *Data Breach Report - the world's biggest data breaches*. USwitch. Retrieved June 1, 2023, from https://www.uswitch.com/broadband/data-breaches-report/
[41]: Goldsmith, J. L. (2005). *The Internet and the Abiding Significance of Territorial Sovereignty*. Taylor Francis. Retrieved June 1, 2023, from https://www.taylorfrancis.com/chapters/edit/10.4324/9781315086392-8/internet-abiding-significance-territorial-sovereignty-jack-goldsmith
[42]: Cheng, J., Xu, R., Tang, X., Sheng, V. S., & Cai, C. (2018). *An Abnormal Network Flow Feature Sequence Prediction Approach for DDoS Attacks Detection in Big Data Environment*. Research Gate. Retrieved June 1, 2023, from https://www.researchgate.net/profile/Ruomeng-Xu-2/publication/350153694_An_Abnormal_Network_Flow_Feature_Sequence_Prediction_Approach_for_DDoS_Attacks_Detection_in_Big_Data_Environment/links/60537a0e299bf17367522830/An-Abnormal-Network-Flow-Feature-Sequence-Prediction-Approach-for-DDoS-Attacks-Detection-in-Big-Data-Environment.pdf

[43]: Milmo, D. (2022, March 18). *Amateur hackers warned against joining Ukraine's 'IT army'*. The Guardian. Retrieved June 1, 2023, from https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
[44]: Adee, S. (2019, May 15). *The global internet is disintegrating. What comes next?* BBC. Retrieved June 1, 2023, from https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next
[45]: (2022, July 5). *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*. NIST. Retrieved June 1, 2023, from https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms
[46]: Pillay, S. (n.d.). *The Implementation of Polarisation Encoded Quantum Key Distribution in Fibre*. Research Space. Retrieved June 1, 2023, from https://researchspace.ukzn.ac.za/bitstream/handle/10413/10719/Pillay_Sharmini_2012.pdf?isAllowed=y&sequence=1
[47]: Mosca, M., Stebila, D., & Ustaoglu, B. (2013). *Quantum Key Distribution in the Classical Authenticated Key Exchange Framework*. Springer. Retrieved June 1, 2023, from https://link.springer.com/chapter/10.1007/978-3-642-38616-9_9#:~:text=Quantum%20key%20distribution%20(QKD)%20can,QKD%20typically%20assume%20idealized%20authentication
[48]: (n.d.). *Quantum Key Distribution (QKD) and Quantum Cryptography (QC)*. NSA. Retrieved June 1, 2023, from https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
[49]: (2020, April 27). *Global e-Commerce hits $25.6 trillion – latest UNCTAD estimates*. UNCTAD. Retrieved June 1, 2023, from https://unctad.org/press-material/global-e-commerce-hits-256-trillion-latest-unctad-estimates
[50]: (2021, February 3). *SMEs in the online platform economy*. OECD-ILibrary. Retrieved June 1, 2023, from https://www.oecd-ilibrary.org/sites/1386638a-en/index.html?itemId=/content/component/1386638a-en#:~:text=E%2Dcommerce%20and%20online%20marketplaces,OECD%2C%202019%5B19%5D
[51]: (2022). *UK Small Business Overview Market Report 2022*. Mintel. Retrieved June 1, 2023, from https://store.mintel.com/report/uk-small-business-overview-market-report
[52]: (2022). *UK Small Business Statistics*. Federation of Small Businesses. Retrieved June 1, 2023, from https://www.fsb.org.uk/uk-small-business-statistics.html
[53]: Worach-Kardas , H., & Kostrzewski , S. (2013, May 17). *Quality of Life and Health State of Long – Term Unemployed in Older Production Age*. National Library of Medicine. Retrieved June 1, 2023, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4000620/
[54]: Guerra, O., & Eboreime , E. (2021, September). *The Impact of Economic Recessions on Depression, Anxiety, and Trauma-Related Disorders and Illness Outcomes—A Scoping Review*. National Library of Medicine. Retrieved June 1, 2023, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8464685/
[55]: Warsh, K. (2009, April 6). *The Panic of 2008*. Federal Reserve. Retrieved June 1, 2023, from https://www.federalreserve.gov/newsevents/speech/warsh20090406a.htm

[56]: Tsuchiya, Y., & Tsuchiya, N. (2021, November). *How cryptocurrency is laundered: Case study of Coincheck hacking incident*. Science Direct. Retrieved June 1, 2023, from https://www.sciencedirect.com/science/article/pii/S2665910721000724
[57]: (2023, February 7). *What is a CBDC?* Bank of England. Retrieved June 1, 2023, from https://www.bankofengland.co.uk/explainers/what-is-a-central-bank-digital-currency
[58]: Kumar, A., Brownstein, G., Lopez-Irizarry, R., & Vishwanath, A. (n.d.). *Central Bank Digital Currency Tracker*. Atlantic Council. Retrieved June 1, 2023, from https://www.atlanticcouncil.org/cbdctracker/
[59]: (2023, April). *Digital Payments - Worldwide*. Statista. Retrieved June 1, 2023, from https://www.statista.com/outlook/dmo/fintech/digital-payments/worldwide
[60]: Yndurain, E., Woerner, S., & Egger, D. J. (n.d.). *Exploring quantum computing use cases for financial services*. IBM. Retrieved June 1, 2023, from https://www.ibm.com/thought-leadership/institute-business-value/report/exploring-quantum-financial
[61]: Dargan, J. (2023, April 10). *What Is The Price of a Quantum Computer In 2023?* Quantum Insider. Retrieved June 1, 2023, from https://thequantuminsider.com/2023/04/10/price-of-a-quantum-computer/#:~:text=However%2C%20quantum%20computers%20are%20not,and%20extremely%20difficult%20to%20manufacture
[62]: Downey, L. (2022, May 25). *Optimization: Overview and Examples in Technical Analysis*. Investopedia. Retrieved June 1, 2023, from https://www.investopedia.com/terms/o/optimization.asp#:~:text=Optimization%20is%20the%20process%20of,assets%20with%20greater%20expected%20returns
[63]: (2022, April 12). *How to use predictive analytics in advertising*. IBM. Retrieved June 1, 2023, from https://www.ibm.com/watson-advertising/thought-leadership/how-to-use-predictive-analytics-in-advertising
[64]: Barone, A. (2020, September 23). *Risk Profile: Definition, Importance for Individuals & Companies*. Investopedia. Retrieved June 1, 2023, from https://www.investopedia.com/terms/r/risk-profile.asp
[65]: Woerner, S., & Egger, D. J. (2019, February 8). *Quantum risk analysis*. Nature. Retrieved June 1, 2023, from https://www.nature.com/articles/s41534-019-0130-6
[66]: Knight, W. (2017, May 17). *Google Reveals a Powerful New AI Chip and Supercomputer*. MIT Technology Review. Retrieved June 1, 2023, from https://www.technologyreview.com/2017/05/17/151656/google-reveals-a-powerful-new-ai-chip-and-supercomputer/
[67]: Langston, J. (2020, May 19). *Microsoft announces new supercomputer, lays out vision for future AI work*. Microsoft. Retrieved June 1, 2023, from https://news.microsoft.com/source/features/ai/openai-azure-supercomputer/
[68]: Smith-Goodson, P. (2023, February 23). *IBM Built A Giant AI Supercomputer In The Cloud To Train Its Massive AI Models*. Forbes. Retrieved June 1, 2023, from https://www.forbes.com/sites/moorinsights/2023/02/23/ibm-built-a-giant-ai-supercomputer-in-the-cloud-to-train-its-massive-ai-models/?sh=1d6e45234437
[69]: (n.d.). *Artificial Intelligence Market Size, Share & Trends Analysis Report By Solution, By Technology (Deep Learning, Machine Learning), By End-use, By Region, And Segment Forecasts, 2023 - 2030*. Grand View Research. Retrieved June 1, 2023, from https://www.grandviewresearch.com/industry-analysis/artificial-intelligence-ai-market

[70]: King, B. M. (2018, May). *The Viability of Quantum Computing*. Missouri S&T. Retrieved June 1, 2023, from https://scholarsmine.mst.edu/cgi/viewcontent.cgi?article=1032&context=peer2peer
[71]: Racorean, O. (n.d.). *Decoding Stock Market Behavior with the Topological Quantum Computer*. Arxiv. Retrieved June 1, 2023, from https://arxiv.org/ftp/arxiv/papers/1406/1406.3531.pdf
[72]: Liu, G., & Ma, W. (2022, June). *A quantum artificial neural network for stock closing price prediction*. Science Direct. Retrieved June 1, 2023, from https://www.sciencedirect.com/science/article/abs/pii/S0020025522002821
[73]: Alaminos, D., Salas, M. B., & Fernandez-Gamez, M. A. (2022, June 27). *Forecasting Stock Market Crashes Via Real-Time Recession Probabilities: A Quantum Computing Approach*. World Scientific. Retrieved June 1, 2023, from https://www.worldscientific.com/doi/epdf/10.1142/S0218348X22401624
[74]: Jordan, S. P. (2017, March 24). *Quantum Computers May Have Higher 'Speed Limits' Than Thought*. NIST. Retrieved June 1, 2023, from https://www.nist.gov/news-events/news/2017/03/quantum-computers-may-have-higher-speed-limits-thought
[75]: Furse, C., Bond, P., Cliff, D., Goodhart, C., Houstoun, K., Linton, O., & Zigrand, J. (2012). *The Future of Computer Trading in Financial Markets An International Perspective*. Government Office for Science. Retrieved June 1, 2023, from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/289431/12-1086-future-of-computer-trading-in-financial-markets-report.pdf
[76]: Egan, J. (2023, March 29). *How Are Stock Prices Determined: The Factors that Affect Share Prices of Listed Companies*. Time. Retrieved June 1, 2023, from https://time.com/personal-finance/article/how-are-stock-prices-determined/
[77]: Caivano, V. (2015, March). *The impact of high-frequency trading on volatility: Evidence from the Italian market*. Consob. Retrieved June 1, 2023, from https://www.consob.it/o/PubblicazioniPortlet/DownloadFile?filename=/documenti/quaderni/qdf80.pdf
[78]: Markland, D. (2022, June 29). *5 Simple Steps To Find Your Niche Market*. Forbes. Retrieved June 1, 2023, from https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2022/06/29/5-simple-steps-to-find-your-niche-market/?sh=253c0a2115e4
[79]: Govindarajan, V., Lev, B., Srivastava, A., & Enache, L. (2019, August 16). *The Gap Between Large and Small Companies Is Growing. Why?* Harvard Business Review. Retrieved June 1, 2023, from https://hbr.org/2019/08/the-gap-between-large-and-small-companies-is-growing-why
[80]: Finkelstein, S. (n.d.). *First-Mover Advantage for Internet Startups: Myth or Reality?* Dartmouth. Retrieved June 1, 2023, from https://mba.tuck.dartmouth.edu/pages/faculty/syd.finkelstein/articles/First_Mover.pdf
[81]: Bloomenthal, A. (2022, July 27). *Early Majority Theory: Stages, Examples and Types*. Investopedia. Retrieved June 1, 2023, from https://www.investopedia.com/terms/e/early-majority.asp
[82]: Knecht, G. B. (1996, May 16). *Wall Street Whiz Finds Niche Selling Books on the Internet*. Wall Street Journal. Retrieved June 1, 2023, from https://www.wsj.com/articles/SB832204437381952500

[83]: Tarver, E. (2020, September 28). *First Mover: What It Means, Examples, and First Mover Advantages*. Investopedia. Retrieved June 1, 2023, from https://www.investopedia.com/terms/f/firstmover.asp
[84]: Woggon, M. (2022, July 20). *A Brief History Of Touchscreen Technology: From The IPhone To Multi-User Videowalls*. Forbes. Retrieved June 1, 2023, from https://www.forbes.com/sites/forbestechcouncil/2022/07/20/a-brief-history-of-touchscreen-technology-from-the-iphone-to-multi-user-videowalls/?sh=18dff20e422e
[85]: Hargrave, M. (2021, May 28). *Market Saturation*. Investopedia. Retrieved June 1, 2023, from https://www.investopedia.com/terms/m/marketsaturation.asp
[86]: Luamba, D., Blye, M. L. J., Williams, I. A., & Chagadama, J. (2021, November). *The Benefit of Innovation for Small Businesses*. Research Gate. Retrieved June 1, 2023, from https://www.researchgate.net/publication/356231944_The_Benefit_of_Innovation_for_Small_Businesses
[87]: (n.d.). *Patents*. World Intellectual Property Organization. Retrieved June 1, 2023, from https://www.wipo.int/patents/en/
[88]: Gubby, H. (2020, February 28). *Is the Patent System a Barrier to Inclusive Prosperity? The Biomedical Perspective*. Wiley Online Library. Retrieved June 1, 2023, from https://onlinelibrary.wiley.com/doi/epdf/10.1111/1758-5899.12730
[89]: (2023, May 16). *Apple Patents – Insights & Stats (Updated 2023)*. Insights by GreyB. Retrieved June 1, 2023, from https://insights.greyb.com/apple-patents/
[90]: Aboy, M., Minssen, T., & Kop, M. (2022, July 6). *Mapping the Patent Landscape of Quantum Technologies: Patenting Trends, Innovation and Policy Implications*. Springer. Retrieved June 1, 2023, from https://link.springer.com/article/10.1007/s40319-022-01209-3#:~:text=5.1%20Growth%20of%20Quantum%20Technology%20Patents&text=A%20total%20of%2020%2C583%20patents,over%20the%20last%2020%20years
[91]: Kop, M., Aboy, M., & Minssen, T. (2022, July 19). *Intellectual property in quantum computing and market power: A theoretical discussion and empirical analysis*. Oxford Journal of Intellectual Property Law & Practice. Retrieved June 1, 2023, from https://academic.oup.com/jiplp/article/17/8/613/6646536
[92]: Swayne, M. (2022, May 16). *Top 18 Institutions Leading Quantum Computing Research in 2022*. Quantum Insider. Retrieved June 1, 2023, from https://thequantuminsider.com/2022/05/16/quantum-research/
[93]: (n.d.). *National Institute of Standards and Technology Landing Page*. NIST. Retrieved June 1, 2023, from https://www.nist.gov/
[94]: Kyrlynn, D. (2022, November 8). *Top 10 Quantum Companies ranked according to their number of Quantum Patents*. Quantum Zeitgeist. Retrieved June 1, 2023, from https://quantumzeitgeist.com/top-10-quantum-companies-ranked-according-to-their-number-of-quantum-patents/
[95]: Burkitt-Gray, A. (2022, November 21). *White House tells agencies: Upgrade your security to quantum era*. Capacity Media. Retrieved June 1, 2023, from https://www.capacitymedia.com/article/2awyx1l2mrwyo9vgy4gsg/news/white-house-tells-agencies-upgrade-your-security-to-quantum-era
[96]: (n.d.). *Gramm-Leach-Bliley Act*. Federal Trade Commission. Retrieved June 1, 2023, from https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
[97]: Griffin, A. (2023, February 22). *Google announces major breakthrough that represents 'significant shift' in quantum computers*. Independent. Retrieved June 1, 2023, from

https://www.independent.co.uk/tech/google-quantum-computer-error-correction-latest-b2287412.html
[98]: ‘Utoikamanu, F. (2018, December). *Closing the Technology Gap in Least Developed Countries*. UN Chronicle. Retrieved June 1, 2023, from https://www.un.org/en/chronicle/article/closing-technology-gap-least-developed-countries
[99]: (n.d.). *Licenses of right*. Barker Brettell. Retrieved June 1, 2023, from https://www.euro-ip.com/content/uploads/2018/01/Licenses-of-Right.pdf
[100]: (n.d.). *Quantum Lab*. IBM. Retrieved June 1, 2023, from https://quantum-computing.ibm.com/lab/docs/iql/
[101]: Ben-Hassine, W. (n.d.). *Government Policy for the Internet Must Be Rights-Based and User-Centred*. UN Chronicle. Retrieved June 1, 2023, from https://www.un.org/en/chronicle/article/government-policy-internet-must-be-rights-based-and-user-centred