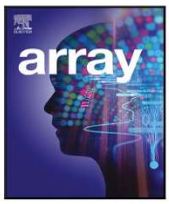
Array 15 (2022) 100225

Contents lists available at ScienceDirect

Array

journal homepage: www.elsevier.com/locate/array



Quantum advantage on proof of work

Dan A. Bard, Joseph J. Kearney, Carlos A. Perez-Delgado *

School of Computing, University of Kent, Canterbury, Kent CT2 7NF, United Kingdom

ARTICLE INFO

Keywords:
Quantum computing
Blockchain
Bitcoin
Proof of Work

ABSTRACT

Proof-of-Work (PoW) is a fundamental underlying technology behind most major blockchain cryptocurrencies. It has been previously pointed out that quantum devices provide a computational advantage in performing PoW in the context of Bitcoin. Here we make the case that this quantum advantage extends not only to all existing PoW mechanisms, but to any possible PoW as well. This has strong consequences regarding both quantum-based attacks on the integrity of the entirety of the blockchain, as well as more legitimate uses of quantum computation for the purpose of mining Bitcoin and other cryptocurrencies. For the first case, we estimate when these quantum attacks will become feasible, for various cryptocurrencies, and discuss the impact of such attacks. For the latter, we derive a precise formula to calculate the economic incentive for switching to quantum-based cryptocurrency miners. Using this formula, we analyze several test scenarios, and conclude that investing in quantum hardware for cryptocurrency mining has the potential to pay off immensely.

1. Introduction

Blockchain systems have become an integral part of modern financial society with their use reaching beyond the storage of value and cryptocurrencies into the wider financial market [1]. One of the core tenets of these systems is that decisions about what data is immutably written to the blockchain's ledger, and therefore what is made a permanent entry on the chain's state going forwards, is made by consensus between nodes connected to and storing the ledger's information.

Although, consensus can be achieved utilizing several different methods [2], Proof of Work (PoW) powered blockchains currently account for more than 90% of the current market share [3] and include some of the largest cryptocurrencies such as Bitcoin and Ethereum. These two blockchains alone account for a market cap of over US$1.6 trillion (approximate as of November 2021) [4]. This demonstrates that considerable financial assets are stored and maintained by blockchains, their transactions and therefore the underlying consensus algorithms.

In this paper we focus on the PoW mechanisms of blockchains. We show that quantum computers give a quadratic advantage in PoW efficiency; not just for all existing protocols but for any possible PoW protocol that relies on computational work being done.

Unlike many other cryptographic standards, blockchain systems intrinsically tie the protected asset (the ledger) with the encryption systems used. It has been previously shown that this makes blockchains particularly vulnerable to quantum attacks. The main concern is that replacing the cryptographic protocols that build a blockchain with 'post-quantum' ones is extremely more difficult than with more traditional cryptographic uses [5,6]. Several predicted timelines [7,8] pin the year 2035 as when we can expect quantum computers to reliably be able to break current mainstream cryptographic protocols such as RSA2048 and ECDSA. These two key facts make these concerns timely and pressing.

Within most blockchain technologies, PoW underpins the protocols' consensus algorithm and because the consensus algorithm determines which transactions and actions performed on the network are integrated into the chain. This gives a quantum actor a potentially much stronger ability to control the decision-making in the blockchain. From a cybersecurity perspective, when one actor (or group of actors) can reliably force all decisions in the blockchain, it is called a '51%' attack [9]. In the first part of this paper, we will describe how quantum actors can much more reliably, and with much fewer resources than any classical counterpart, perform '51%' attacks.

Signature schemes utilized by most major blockchains have been shown to be vulnerable to quantum attacks [5,6]. Fortunately, there are quantum-safe or *post-quantum* digital signature schemes [10–12]. These have even been adopted in some blockchains such as QRL [13] and Nexus [14]. On the other hand, there are no known post-quantum PoW systems. As we argue in Section 3, it is quite likely that there never will be a post-quantum PoW system.

In the second part of this paper, we will consider a much less sinister, and much more profitable, use of quantum resources. Given the quadratic increase in PoW efficiency, one may consider using a quantum computer to *'mine'* Bitcoin or some other cryptocurrency (*mining* is the act of performing PoW in order to help the blockchain

* Corresponding author.
E-mail addresses: d.a.bard@kent.ac.uk (D.A. Bard), jjk30@kent.ac.uk (J.J. Kearney), c.perez@kent.ac.uk (C.A. Perez-Delgado).

https://doi.org/10.1016/j.array.2022.100225
Received 6 December 2021; Received in revised form 31 December 2021; Accepted 3 July 2022
Available online 6 July 2022

arrive at a consensus). Performing this task generally involves economic remuneration to the *'miner'*. A quantum cryptocurrency miner can potentially require fewer clock cycles, a lot less energy, and dissipate a lot less heat, in order to mine the same amount of cryptocurrency as a classical computer counterpart. Whether this makes the endeavour profitable, of course, will depend on both the initial cost, and operating costs of such a quantum device. We explore these questions in Section 4.

First, however, in the following section, we will discuss PoW as it is understood today, finishing with a formal definition of PoW that allows us to perform rigorous mathematical analysis. Then we derive, from first principles, the quantum advantage for PoW. In Section 3 we discuss how this advantage can be used in adversarial situations, *i.e.* in cyberattacks against a cryptocurrency. In Section 4 we switch to discussing the use of quantum advantage for non-adversarial purposes, *i.e.* mining a cryptocurrency. In this section – once again from first principles – we derive a set of equations that allow us to calculate the potential profit a cryptocurrency miner can expect when moving from (classical) ASIC-based miners, to quantum hardware. We then use these equations in a set of forecasts, using best available data. Finally, we conclude with a summary of results, and a discussion on the future outlook for PoW.

2. Proof of work

Consensus algorithms within blockchain technologies are critical to the running of the protocol and PoW is the most commonly utilized mechanism. It is used to ensure miners act honestly according to the rules of the blockchain protocol [15]. It was adapted as a mechanism for consensus across a blockchain by Satoshi Nakamoto [16,17]. PoW is widely used partly due to the utilization of Bitcoin's technologies and code base within a large amount of subsequent projects, but also because it is a highly secure mechanism for ensuring the good nature of mining nodes and because it lends itself well to distributed networks.

Blockchain consensus employs the concept of the longest chain. The longest chain is typically the valid chain that a majority of the network holds as the state of the blockchain. While a miner can create a malicious block and add it to the network trivially, it will not be accepted by a majority of the nodes, as other peers on the network will reject the block and choose an alternate proposed block, therefore, excluding the malicious block from the longest chain. If a malicious user controls a majority of the network's computational power, they could potentially overwhelm this consensus mechanism by adding blocks to the chain faster than the rest of the network can compete, meaning they consistently have the longest chain. This means that the user could gain overall control of what is included into each block. This is known as a '51%' attack and is the most damaging threat to a blockchain's integrity.

In PoW-based systems a user proposing a new block must perform a computationally intensive task. The successful completion of this task must be easily verified by other users on the network. Miners must expend a non-trivial amount of resources—usually computational *work* and its associated costs, such as electricity and heat. This incurs a sunk cost for the miner that will be lost if the block they present is malicious or malformed.

The Bitcoin PoW algorithm employs a NP-Complete problem where the goal is to create a hash digest based on a given input string [18]. This hash digest is required to be in a specific form. This form is dictated by a target value (some integer in the range $[0, 2^{256}]$) and Bitcoin miners must compute the hash digest that has an equal to or smaller value than the target. The target value is determined by the difficulty value of the blockchain network, which is altered depending on the computational power on the network as a whole as determined by the network's current *hash-rate* (leading to the final target value being in the range of $[0, (2^{256} - \text{difficulty})]$). Within Bitcoin, the difficulty value is changed according to the current computational power on the network once every 2016 blocks [15] in order to maintain a block time of approximately 10 min. While this example is taken from Bitcoin, this is applicable to any network which utilizes PoW.

The hash is calculated using the block header, which is constant for a specific block, and a nonce, which is changed repeatedly by the miner, to create different hash digests in the hope of finding a digest that fits the requirements for the block. As noted earlier, this problem is NP-Complete. The best known classical algorithms for solving PoW scale exponentially to the size of the difficulty (which in turn is bounded by the size of the hash itself).

It is important to note that while hash-based PoW uses a NP-Complete problem, this does not necessarily have to be the case. It *must* be the case, however, that the miner expend a non-trivial amount of work, and that this expenditure can be verified by other users of the blockchain in a relatively trivial manner. In other words, let TC_V be the time complexity for verification and TC_S be the time complexity for the miner to solve the problem. Then, any PoW mechanism must guarantee that:

$$TC_V \ll TC_S. \tag{1}$$

Clearly, any NP-Complete problem will satisfy the equation above. More generally, however, any PoW algorithm must satisfy the following requirements:

Definition (*Proof of Work*)**.** A computational problem can be considered as a PoW problem if it satisfies the following two requirements

1. The computational complexity of the problem must satisfy Eq. (1),
2. The difficulty of the problem must be easily *tuneable* with a parameter.

Requirement 1 has been explained above. Requirement 2 is an important requirement for the continued health of the blockchain network over time. As the computational power of miners increases, this parameter needs to be re-tuned to keep PoW as a meaningful deterrent against rogue miners.

In the following section we will explore the quantum computational advantage in PoW as described here. We will then explore the cybersecurity threat of quantum attacks on blockchain networks. Finally, we will analyze the possibility, and possible profit, of using this quantum advantage for the more benign purpose of more efficient cryptocurrency mining.

3. Quantum advantage for PoW

When discussing quantum advantage for computational tasks, two main types of algorithms are most often cited. The first is the subgroup-finding algorithms based on Shor's seminal work [19]. These types of algorithm provide a exponential advantage on problems including factoring and discrete logarithm. Though this is only a relatively small set of problems, it covers a large area of the cryptographic landscape. The other type are the quantum search algorithms based on Grover's algorithm [20,21]. Whilst quantum search algorithms provide a more modest quadratic advantage over classical, their very broad applicability makes them extremely versatile, and central to our discussion.

The quantum search algorithm, as its name suggests, allows one to search *any* (including unsorted and unstructured) data-set S, of cardinality $N = |S|$ for certain items that fulfill some condition, or is an element of some subset $C \subseteq S$. This condition is specified, in the quantum algorithm, as a black box or oracle O that takes as input one register containing an element of $x \in S$, and an ancilla qubit, which is set to 1 if $x \in C$ and 0 otherwise. The importance of this algorithm is that it runs in *total time* $O(\sqrt{N})$, and makes $O(\sqrt{N})$ queries to O. This oracle can be, and in practical uses often is, replaced by a quantum circuit or subroutine program a that computes whether x satisfies the required condition, or is an element, of the subset C.

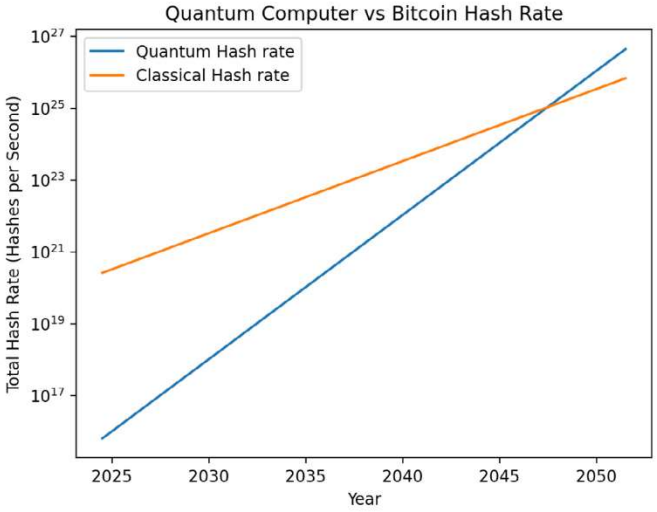


Fig. 1. Bitcoin network hash rate *vs.* single quantum computer. The graph shows the hash rate growth over time of the entirety of the Bitcoin network, compared to that of a *single* quantum computer. Future data-points are extrapolated from current hash-rates, and assumes growth-rates for both quantum and classical technologies in line with current Moore's Law trends. See the main text for further details.

In particular, one may consider a decision problem D that is NP-Complete. Let I be its input set, and $S \subseteq I$ the solution set. Given that the problem is in NP, there exists an efficient (polynomial-time) algorithm a that can compute, on input x, whether $x \in S$. This in turn implies that a quantum search algorithm can solve D in total time $O(\sqrt{N}) = O(\sqrt{2^n})$, where n is the input size in bits. Because D is NP-Hard, there is *no* (known) classical algorithm that can solve D in time substantially better than $O(2^n)$.

It should be now clear why the quantum search algorithm is of central importance to any discussion of quantum advantage for PoW. As discussed previously, most PoW systems today require the miner to find a SHA-x hash for a pre-determined string, that is under a certain value. This problem is NP-Complete. Hence, a quantum computer with a memory register large enough to run Grover's algorithm on the necessary hash size, would be able to gain a quadratic advantage over any classical device—including purpose-built ASICs.

To illustrate this, we can consider a toy example in which a classical brute-force search algorithm which runs in time precisely 2^n, and a quantum search one that runs in precisely time $\sqrt{2^n}$. On input size $n = 2$, the quantum algorithm is only twice as fast as the classical one. On input size $n = 256$ the quantum algorithm will run 3.4×10^{38} times faster. Compare this to ASIC chips that typically provide a speed-factor advantage of approximately 1×10^4.

We can also perform a more realistic analysis. Running a quantum search algorithm (assuming no error correction) on SHA-256 hashes requires roughly 512 qubits. Estimates by major quantum computer manufacturer predict such quantum computers will be available in 2023 [22]. At today's reported quantum computer clock-speeds [23] (barring any major improvements) we can thus expect the equivalent of 4×10^7 calculations performed per second which, using Grover's algorithm, leads to the equivalent of 1.6×10^{15} hashes computed per second (H/s).

Fig. 1 plots the Bitcoin network hash rate using the most current value of 130×10^{18} H/s [24] against a quantum computing technology that starts at 40 MHz [22], and both increasing over time at the same rate, as dictated by Moore's Law. This gives an estimated timeframe of approximately 27 years until a *single* quantum computer will be capable of completely out-mining the rest of the network, and hence be able to take over complete control of it (a successful 51% attack).

This prediction, however, is perhaps overly conservative for a couple of reasons. The first is that we consider the speed-increase in clock-rate for both quantum computers and classical computers to be the same. In reality, classical computers are known to be at the tail-end of Moore's Law's [25] logistic-curve rate-of-growth [26]. Meanwhile, we can expect quantum computers, which are in their infancy, to over-achieve this rate-of-growth [27].

Furthermore, this comparison has been made on the Bitcoin network, which has, by far, the largest hashing power of all blockchains [28]. Other comparatively smaller blockchain networks would be vulnerable far sooner than suggested here. For example, if network hash rates of blockchains such as Monero (1.28 Giga-Hashes per Second (GH/s)) [29] or Ethereum Classic (23.11 Tera-Hashes per Second (TH/s)) [30] do not improve in the coming years, we could expect them to be vulnerable to a quantum 51% attack as soon as there is a quantum computer with sufficient quantum memory, which is predicted to happen roughly in 2023 [22].

In short, not only do quantum computers provide an *asymptotic quadratic* efficiency increase for current PoW systems, they do so for any likely possible PoW system as well. Compare this to custom-built ASIC chips which also provide a speed increase in mining cryptocurrencies, but are however limited to constant-factor speed-increases. This results in a single quantum computer being able to launch devastating attacks on the cryptocurrency network, in the foreseeable future.

Of course, this *'single quantum computer'* attack would only work against a cryptocurrency network that is, at least for the most part, composed of classical miners. If a sizeable portion of a cryptocurrency's miners were to move to quantum hardware, this would protect the entire network from quantum 51% attacks. In the next section we explore legitimate uses of quantum technology for PoW-based cryptocurrency mining. As we shall see, there may also be definite profit motives for individual cryptocurrency miners to invest in and adopt quantum technologies.

4. The profitability of quantum cryptocurrency mining

In previous sections we studied the cybersecurity threat posed by quantum-led 51% attacks on blockchain networks. These attacks, while largely inevitable, are time-wise a bit far off—at least for the larger cryptocurrencies such as Bitcoin. The reason for this is that for a successful attack a quantum computer must have as much (or more) PoW computational power as the rest of the network combined.

Here, we will study the viability of using a quantum computer for the purpose of legitimately mining a cryptocurrency such as Bitcoin. In order to do *this* effectively and profitably, a quantum computer does not have to be more powerful than the whole network, it only needs to be more efficient (in terms of resource-cost per block approved by the network) than a single classical miner. Hence, we can expect quantum supremacy, in the field of cryptocurrency mining, to be achieved much sooner than the previously discussed dates given for 51% quantum attack viability.

We will first set out to derive a general equation that can be used to calculate the potential profitability of quantum-assisted cryptocurrency mining. We will then apply this equation to various credible scenarios, and give estimates of near-future profitability.

4.1. Profitability calculation

In this section we will be setting out an equation to calculate whether mining on a classical or a quantum entity is more profitable. The primary element to be considered when making this calculation is the income from any device mining blocks on a blockchain. This is based on the probability of mining a block during the time it takes for a new block to be generated. This exact value varies among blockchains with a new block being generated on average every 600 s within Bitcoin [31] and approximately every 15 s within Ethereum [32]. However, this value can be generalized, since the relation between

block generation and the probability of mining a specific block will be the same across all PoW based blockchains. This block time is controlled by the difficulty of a particular blockchain in relation to the hash size in bits defined by the blockchain's architecture [33]. This is changed periodically in order to maintain a consistent block time and so, across a larger timescale, the time taken to generate a new block can be averaged dependent on blockchain. Based on these values and the given hash rate of any considered classical miner, we can say that the probability of mining a block is defined as:

$$P_C = \frac{H_C t}{\frac{\eta D}{t}} \tag{2}$$

where P_C is the probability of mining a block from a classical device, H_C is the hash rate of the classical device, t is the block time, D is the difficulty of the blockchain network and η is the hash size.

The denominator of (2) is the calculation for the total network hash rate of any one network. This can then be simplified to:

$$P_C = \frac{H_C t^2}{\eta D}, \tag{3}$$

as derived from the hash rate of any one device divided by the total network hash rate [24]. As discussed in Sections 2 and 3, as blockchain technologies utilize NP-Hard problems for PoW and as D determines the complexity of said problems, D is the value where the quadratic increase in efficiency can be applied. Due to this advantage the probability of mining a block on any quantum device based on a given equivalent hash rate can then be defined as:

$$P_Q = \frac{H_Q t^2}{\eta \sqrt{D}} \tag{4}$$

where P_Q is the probability of mining a block from a quantum device and H_Q is the equivalent hash rate of that device.

These probabilities, when taken across any given operational timespan can then be used to calculate the overall income across said timespan for any given blockchain, taking into account a conversion into fiat currency, defined as a function f. As the exact conversion between cryptocurrencies and real world fiat currency can vary, this has been abstracted to a single function. The exact reward gained per block mined is another element which varies based on the cryptocurrency being considered and duration of the operating period. When performing the profitability calculations, this needs to be taken into careful consideration as, for some cryptocurrencies, the block reward can change across the lifespan of any particular cryptocurrency. For example, Bitcoin halves its block reward every 210,000 blocks, meaning that though it originally rewarded 50 bitcoins (BTC) per block mined [34], the current value is 6.25 BTC. The reward is expected to approach 0 by approximately 2140 [35].

Taking these elements into account, the total income over the given timespan can be calculated as the following for classical miners:

$$I_C = f\left(\frac{T}{t} \cdot P_C B\right), \tag{5}$$

where I_C is the income for a classical miner across the timespan T, and B is the block reward for the considered blockchain. The following holds for quantum miners:

$$I_Q = f\left(\frac{T}{t} \cdot P_Q B\right), \tag{6}$$

where I_Q is the income for a quantum miner across T.

Following this, we can bring in the initial cost of any particular device in order to calculate the point at which the given device becomes profitable whilst operating on the network across T. Once this value becomes greater than 0, it is then deemed to be profitable to run the miner on the blockchain network. As discussed in Section 2, miners are required to expend energy (in the form of computation) to ensure honesty between parties. This is considered here as the operational costs of any given device. From this, the profit returns for classical miners can be determined as:

$$R_C = I_C - (T \cdot O_C) - S_C, \tag{7}$$

where R_C is the profit, O_C is the operating costs and S_C is the setup costs for the classical device. The profit calculation for quantum miners is as follows:

$$R_Q = I_Q - (T \cdot O_Q) - S_Q, \tag{8}$$

where R_Q is the profit, O_Q is the operating costs and S_Q is the setup costs for the quantum device.

From these two equations, we can then calculate a profit ratio (G):

$$G = \frac{R_C}{R_Q}. \tag{9}$$

The above equation is particularly important: $G = 1$ is the inflection point at which quantum and classical technologies are equally feasible. Values of G less than 1 imply that the quantum miner in question is more profitable than a classical one, even after factoring in initial investment costs considered in the calculation.

Eq. (9) can be expanded, using the previous equations, to:

$$G = \frac{f\left(T \cdot \frac{H_C t}{\eta D} \cdot B\right) - (T \cdot O_C) - S_C}{f\left(T \cdot \frac{H_Q t}{\eta \sqrt{D}} \cdot B\right) - (T \cdot O_Q) - S_Q} \tag{10}$$

The above equation has many practical uses. For one, it allows one to *'plug in'* various known values, like research and development and other initial investments necessary to jump-start a quantum cryptocurrency mining operation, along with running costs for both classical and quantum mining, and decide whether the investment in quantum mining can pay off. It can also be used – as we do below – to estimate the timescales at which quantum cryptocurrency mining can become a profitable enterprise.

An important fact to emphasize is that Eq. (9) takes into account the introduction of further quantum computing machines onto the network. This is because difficulty is defined at the protocol level of a blockchain as a mechanism to ensure that the block time stays within certain bounds. For example the Bitcoin blockchain's difficulty operates so that over a period of time, if the block time exceeds or is less than 10 min, the difficulty of the PoW problem is corrected to bring the block time back in line with the pre-defined desirable time. This means that the introduction of quantum computers onto the network will in fact decrease the block time as they have a quadratic advantage over their classical peers. The Bitcoin protocol will thereby increase the difficulty of the PoW algorithm. This is then taken into account within our equation. Introduction of quantum computers into the mining ecosystem could potentially cause a dramatic increase in the difficulty. This means that the equation presented here will take into account new quantum computers mining the network as their inclusion will factor into difficulty.

The above is important for various reasons, but of particular import is the *first mover vs. second mover advantages.* Being a first mover, that is, being the first to enter a market (in this case with a quantum miner) has definite advantages and is of particular interest to entrepreneurs and investors. A common concern among potential investors is that of making a large investment, only to arrive *late* to a market, potentially ruining return-on-investment prospects. As we shall discuss in the last section of this paper, quantum mining has the peculiar property that the more quantum mining *'competitors'* one has, however, the more profitable it may become for one to do quantum mining.

4.2. Scenarios and forecasts

Using the equation derived earlier, we can analyze some possible near-future scenarios. The general goal will be to determine the profitability of quantum-based cryptocurrency mining. The cryptocurrency

which shall be used for this investigation will be Bitcoin as this is currently the blockchain with the highest comparative market value [4]. This shall be performed utilizing the denominator of Eq. (10) which can be formalized with the target as such:

$$f\left(T \cdot \frac{H_Q t}{\eta\sqrt{D}} \cdot B\right) - (T \cdot O_Q) - S_Q > 0 \tag{11}$$

Which, to summarize, represents the point at which the total possible profit made across the time period, T, is greater than 0. So, when true, it is profitable to mine Bitcoin on a quantum miner.

For our case-analysis scenario, let us consider using a cloud quantum computing service. IBM [36], amongst others, have announced for-profit cloud-based quantum computing services. This is a natural scenario to consider since most quantum computation in the near future is likely to involve cloud-based services [37,38]. This scenario has a composite advantage as well: it obviates the need for an initial investment, requiring instead only that the potential miner pay the rolling costs of renting quantum CPU time from the cloud provider. It will allow us, within this analysis, to set $S_Q = 0$.

Next, let us consider a time-frame. According to the roadmap set out by IBM, a quantum computer which can run a quantum search algorithm on Bitcoin's hashing function can be expected by roughly 2023 [22]. To be conservative, we consider 2025 to be an estimated 'year zero' in which a quantum computer can run a quantum search on hash-based PoW and so 01/01/2025 shall be used whenever a given date is required.

For our case scenario we are focusing on Bitcoin. This sets some further variables in our equation. These are $t = 600$ s, $\eta = 2^{32}$ [15,16] and $B = 3.125$ BTC [34,39]. As an additional part of the blockchain architecture, the difficulty is calculated and adjusted every 210,000 blocks in order for the block period to remain relatively constant. To provide a difficulty for this scenario, we plotted the historical difficulties and then the appropriate difficulty was extrapolated to our given date using polynomial curve of best fit. This provided a difficulty of $D = 4.2903 \times 10^{18}$. Though there are varying opinions of the future of Bitcoin difficulty [40], this matches the current trends.

The value of Bitcoin has had a general increasing trend year-on-year, however due to the volatile nature of cryptocurrencies, no single prediction can be made. Therefore the values shown in Table 1 will account for various BTC to USD conversion rates including the current price (as of 17/12/2020 this was $23,536.12) [4], the average price over the last 12 months (taken as the average closing price from 01/01/2020 until 17/12/2020, $10,385.49), a predicted conservative price ($31,000) and a predicted high-end price ($100,000).

The final element of the equation to be assigned is the hash rate equivalent of the quantum computer. How the hashing power will increase as the development of quantum computers continues is not known. Thus, we consider two possibilities. In the first scenario, we take the clock-speed of (one of) Google's current quantum computers of $H_Q = 40$ MHz/s [23], and keep that value constant throughout time. In the second, more plausible, scenario we increase the quantum computer's clock-speed according to Moore's Law. After four doubling cycles, we arrive at a clock-speed of $H_Q = 640$ MHz/s.

Table 1 collects the calculations made for the various scenarios.

From these results, the best case scenario can be found when $H_Q = 640$ MHz/s and the market conversion result is $f = \$100,000$. In this case, as long as the operational cost of the quantum device (*i.e.* the quantum cloud CPU time charged by the provider) is below $O_Q = \$425,440.90$ a year, a quantum miner would still be able to turn a profit.

4.3. The effects of introducing quantum PoW technology

Finally, presented in Fig. 2 is a cascading *virtuous cycle* that will propagate upon the introduction of quantum computers to a PoW based blockchain network. This will happen as they become profitable when compared to classical alternatives, according to Eq. (10). Firstly, introducing quantum computers into a PoW based blockchain, as discussed, will consequently increase the hash-rate of the entire network, thereby shortening the average time it takes for the network to calculate a block. According to a blockchains protocol this will cause an increase in the PoW difficulty parameter in order to recalibrate the block-time to the prescribed value.

Increasing the difficulty parameter of PoW has been shown to solidify the quadratic advantage of quantum computers as miners. This advantage means that there will be greater incentive for investment into quantum mining technologies as the profit margin when compared with their classical counterparts will increase. This greater incentive will once again increase the number of quantum miners on the network, thereby decreasing the block-time and increasing the PoW difficulty in turn. This creates cycle within which quantum computing technologies will, eventually, completely replace classical miners, as the later cease to be cost-effective.

This cascading effect also has a security benefit for the network itself. As soon as the majority (roughly) of the miners are quantum, the network itself become impervious to 51% attacks based on quantum advantage *alone*. It would still be technically possible to mount such an attack, but such an attack would only succeed by using *other* methods such as miner-collusion, rather than by merely leveraging quantum advantage.

Over time the increased difficulty parameter of PoW will lead to classical miners being made obsolete. The increase in difficulty will cause the PoW problem to become exponentially harder for both classical and quantum devices. However, the impact to classical miners is quadratically worse, over time, than the impact to quantum miners. Eventually, this will lead to all quantum miners being more cost-effective than classical miners (regardless of their initial setup costs).

Table 1
This table shows the income generated by a quantum Bitcoin miner, over the period of a year in USD in relation to a specified quantum computer clock speed (first column) and a fiat currency conversion (second column). In the third column O_Q is calculated with $I_Q = 1$ (USD).

H_Q (MHz/s)	f (USD)	O_Q
40	23,536.12	6258.27
40	10,385.49	2761.51
40	31,000.00	8242.92
40	100,000.00	26,590.06
640	23,536.12	100,132.28
640	10,385.49	44,184.12
640	31,000.00	131,886.68
640	100,000.00	425,440.90

5. Discussion

Quantum computation gives a definite advantage over classical computation for the purpose of calculating PoW for blockchains. As we have seen, in Section 3, this quantum advantage can be used by an adversarial party, in order to attempt what are called 51% attacks, on the cryptocurrency. The possibility of these types of attacks is, however, in the reasonably distant future.

On the other hand, it is very unlikely that there ever will be a quantum-secure – or *post-quantum* – alternative to hashing for the purposes of PoW. Not only is hashing-based PoW susceptible to quantum advantage, but so are other well-known PoW systems such as Zcash's use of the Birthday Paradox-based computational problem [41].

Our security analysis is mathematically consistent with the previous analysis of Bitcoin quantum security by Cojocaru et al. [42]. The authors there conclude that Bitcoin can be made safe against quantum adversaries, but only by assuming strong bounds on the computational power of these quantum adversaries—never a safe assumption.

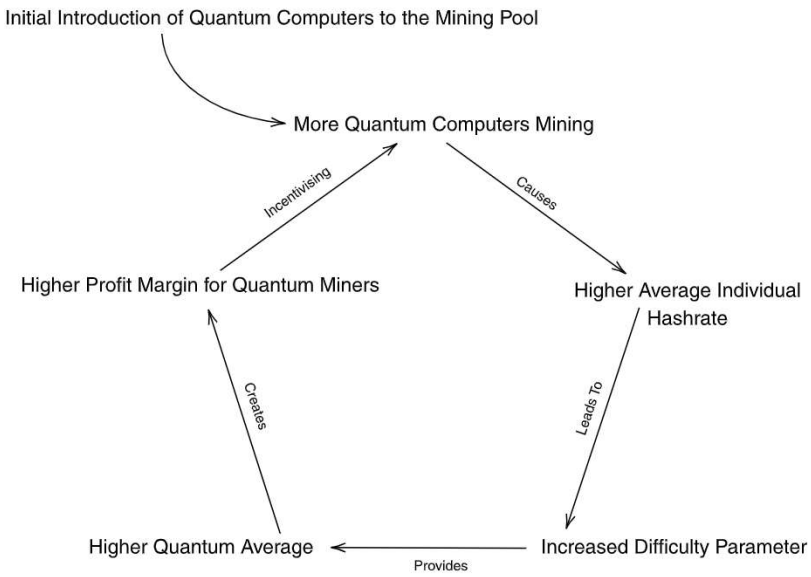


Fig. 2. Self-propagating cycle of increasing quantum advantage on PoW networks. Adding quantum miners to the cryptocurrency network increases the network's hash-rate. An increased hash-rate will raise the difficulty parameter. An increased difficulty parameter increases the relative quantum-advantage. This, in turn, increases the profitability of quantum-mining, which in turn motivates the introduction of more quantum miners.

Moreover, it is unlikely that any PoW system can be derived that is not susceptible to some form of quantum advantage. This is because PoW, by definition, requires a problem whose solution is hard to *compute* (to ensure miners are required to do meaningful *work* for their PoW), while being fairly easy to *verify* (to ensure any third party can verify that the work has been performed). And these are exactly the type of problems where quantum search algorithms provide definite advantage over classical.

This means that once a quantum computer *does* exist that can attack the network in this way, there will be very little that can be done to safeguard the blockchain network against said attacks. This has not stopped some researchers from studying quantum-resistant PoW systems.

One suggestion is to switch the method of PoW from a hashing function to another computationally hard problem, such as lattice based PoW schemes [43] or schemes involving multivariate quadratic functions [44,45]. These schemes may indeed *reduce* the quantum advantage, but they cannot remove it. Grover's algorithm has already been shown to provide a speed-up in solving the shortest vector problem in lattice problems over the best known classical algorithms [46].

More generally, as discussed earlier, PoW requires a mathematical problem that is hard to solve, but easy to verify. In order to remove any quantum advantage, the best classical algorithms that solve the problem must not only be inefficient, they would also have to not rely at all on brute-force search (with or without heuristics). This makes the creation of a quantum-resistant PoW consensus mechanism very unlikely.

Another possible avenue is to drop the use of PoW by the blockchain completely, and move to another consensus mechanism entirely—such as *Proof of Space* [47], *Proof of Stake* [48–50], *Proof of Sequential Work* [51] or other alternatives [52]. All of these consensus systems are different enough from PoW – and from each other – that they would require their own post-quantum security analysis. The work presented here focuses on PoW, as it is today *by far* the most widely deployed—both in terms of number of users and the market capitalization of the cryptocurrencies that use it.

Another safeguarding mechanism would be to move the entire cryptocurrency from ASIC miners to quantum miners. In Section 4, we discussed the possibility of doing this. We showed that mining cryptocurrency, using quantum computation, can quickly become a profitable proposition. In Section 4.1 we gave a precise formula that allows one to calculate a potential profit of using quantum computation for PoW.

How profitable this is will clearly depend on considerations such as the running cost of a quantum computer, and the initial costs of setting one up. This latter cost can be removed if one chooses to use cloud quantum computation. We calculated the precise revenue that one can expect from mining bitcoin in 2025 across the period of a year using predicted available cloud quantum computing at that time to be between $44,184.12 and $425,440.90, depending on whether the most conservative or optimistic parameters are used. This variable is based on the conversion rate of Bitcoin and the exact hashing power of the quantum device at the time. Whether this is profitable will depend on how much quantum cloud CPU time is charged for at that time. The existence of secure remote quantum computing protocols such as *blind quantum computation* [53], means that a client can safely use a cloud quantum server for the purposes of mining Bitcoin, or other cryptocurrencies, without any interference from the server. In short, this shows a very likely profitable use of quantum computational resources in the coming decades. As shown in Fig. 2, and described more generally in Section 4.3, the introduction of quantum computers into a mining ecosystem will make subsequent use of quantum computers even more profitable, as compared to classical computers—which in turn will become less profitable over time.

6. Conclusion

In closing, we have introduced the mathematical machinery necessary to understand, accurately, the impact of introducing quantum PoW technology into cryptocurrency ecosystems—used both by malicious, and non-malicious actors. A clear next step is to branch out the analysis we have done here to other blockchain consensus mechanisms that were outside the scope of this work.

Another clear next step is to take the work we have developed here, as well as real-world economic data, and use both together to create accurate, predictive, models. Several useful predictive models could be developed to help inform, say, investment strategies into quantum technologies, hedging strategies for cryptocurrency investors and miners, etc. We have made some simple predictions here, in Section 4.3. These simple models are meant, mostly, to showcase the power of the mathematical machinery we have introduced—and to hopefully motivate their use in creating more accurate, powerful, predictive models. Even

our very simplistic models already suggest a trend however: we expect all PoW-based cryptocurrency mining to move to quantum platforms in the coming decades.

CRediT authorship contribution statement

Dan A. Bard: Validation, Formal analysis, Investigation, Writing – original draft, Writing – review & editing. **Joseph J. Kearney:** Validation, Formal analysis, Investigation, Writing – original draft, Writing – review & editing. **Carlos A. Perez-Delgado:** Conceptualization, Methodology, Investigation, Writing – original draft, Writing – review & editing, Supervision, Funding acquisition.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors would like to acknowledge funding through the EPSRC, United Kingdom Quantum Communications Hub (EP/T001011/1), and from the Casper Association Academic Grants Program. The authors would also like to thank Joanna I. Ziembicka for useful comments during the preparation on this manuscript.

References

[1] Crosby M, Pattanayak P, Verma S, Kalyanaraman V, et al. Blockchain technology: Beyond bitcoin. Appl Innov 2016;2(6–10):71.
[2] Bach LM, Mihaljevic B, Zagar M. Comparative analysis of blockchain consensus algorithms. In: 2018 41st international convention on information and communication technology, electronics and microelectronics (MIPRO). 2018.
[3] Anand A, McKibbin M, Pichel F. Colored coins: Bitcoin, blockchain, and land administration. In: Annual world bank conference on land and poverty. 2016.
[4] Cryptocurrency prices, charts and market capitalizations. 2021, URL https://coinmarketcap.com/, Accessed: Apr. 15, 2021.
[5] Aggarwal D, Brennen GK, Lee T, Santha M, Tomamichel M. Quantum attacks on bitcoin, and how to protect against them. 2017, arXiv preprint arXiv:1710.10377.
[6] Kearney JJ, Perez-Delgado CA. Blockchain technologies vulnerability to quantum attacks. Array 2021;100065.
[7] Van Meter R, Horsman C. A blueprint for building a quantum computer. Commun ACM 2013;56(10):84–93.
[8] Mosca M. Cybersecurity in an era with quantum computers: Will we be ready? IEEE Secur Priv 2018;16(5):38–41. http://dx.doi.org/10.1109/MSP.2018.3761723.
[9] Ye C, Li G, Cai H, Gu Y, Fukuda A. Analysis of security in blockchain: Case study in 51%-attack detecting. In: 2018 5th international conference on dependable systems and their applications (DSA). IEEE; 2018, p. 15–24.
[10] Alagic G, Alagic G, Alperin-Sheriff J, Apon D, Cooper D, Dang Q, Liu Y-K, Miller C, Moody D, Peralta R, et al. Status report on the first round of the NIST post-quantum cryptography standardization process. US Department of Commerce, National Institute of Standards and Technology …; 2019.
[11] Fernández-Caramés TM, Fraga-Lamas P. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. IEEE Access 2020;8:21091–116.
[12] Nejatollahi H, Dutt N, Ray S, Regazzoni F, Banerjee I, Cammarota R. Post-quantum lattice-based cryptography implementations: A survey. ACM Comput Surv 2019;51(6):1–41.
[13] Waterland P. Quantum resistant ledger (QRL). 2021, URL https://github.com/theQRL/Whitepaper, Accessed: Apr. 15, 2021.
[14] Anderson B, Bunje A, Cantrell C, Laver S, Moreno V. Nexus: A new internet protocol. 2021, URL https://tech.nexus.io/files/nexus_protocol/Nexus_Protocol_1.0.0.pdf, Accessed: Apr. 15, 2021.
[15] Antonopoulos AM. Mastering bitcoin: Unlocking digital cryptocurrencies. O'Reilly Media, Inc.; 2014.
[16] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. Tech. rep., Manubot; 2019.
[17] Back A, et al. Hashcash-a denial of service counter-measure. 2002.
[18] Ren L. Analysis of nakamoto consensus. IACR Cryptol ePrint Arch 2019;2019:943.
[19] Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science. IEEE; 1994, p. 124–34.
[20] Grover LK. A fast quantum mechanical algorithm for database search. In: Proceedings of the twenty-eighth annual ACM symposium on theory of computing; 1996, p. 212–19.
[21] Kwiat PG, Mitchell JR, Schwindt PDD, White AG. Grover's search algorithm: An optical approach. J Modern Opt 2000;47(2–3):257–66. http://dx.doi.org/10.1080/09500340008244040, arXiv:https://www.tandfonline.com/doi/pdf/10.1080/09500340008244040. URL https://www.tandfonline.com/doi/abs/10.1080/09500340008244040.
[22] Gambetta J. IBM's roadmap for scaling quantum technology. 2021, URL https://www.ibm.com/blogs/research/2020/09/ibm-quantum-roadmap/, Accessed: Apr. 15, 2021.
[23] Arute F, Arya K, Babbush R, Bacon D, Bardin JC, Barends R, Biswas R, Boixo S, Brandao FG, Buell DA, et al. Quantum supremacy using a programmable superconducting processor. Nature 2019;574(7779):505–10.
[24] Hash-rate in bitcoin. 2021, URL https://www.blockchain.com/charts/hash-rate, Accessed: Apr. 15, 2021.
[25] Moore GE. Cramming more components onto integrated circuits. 1965.
[26] Shalf J. The future of computing beyond Moore's law. Phil Trans R Soc A 2020;378(2166):20190061.
[27] Forget moore's law - quantum computers are improving according to a spooky 'doubly exponential rate'. 2021, URL https://www.livescience.com/65651-quantum-computers-get-scary-fast.html, Accessed: Apr. 15, 2021.
[28] Coin metrics bitcoin charts. 2021, URL https://coinmetrics.io/charts/, Accessed: Apr. 15, 2021.
[29] Klemens S. Monero mining hardware comparison 2021 (recently updated). 2021, URL https://www.exodus.io/blog/monero-mining-hardware-comparison/, Accessed: Apr. 15, 2021.
[30] Ethereum classic hash rate chart. 2021, URL https://bitinfocharts.com/comparison/ethereumclassic-hashrate.html, Accessed: Apr. 15, 2021.
[31] Bitcoin. 2021, URL https://bitcoin.org/, Accessed: Apr. 15, 2021.
[32] Ethereum (ETH) blockchain explorer. 2021, URL https://etherscan.io/, Accessed: Apr. 15, 2021.
[33] Garay J, Kiayias A, Leonardos N. The bitcoin backbone protocol: Analysis and applications. In: Annual international conference on the theory and applications of cryptographic techniques. Springer; 2015, p. 281–310.
[34] Meynkhard A. Fair market value of bitcoin: Halving effect. Invest Manage Financ Innov 2019;16:72–85.
[35] Controlled supply. 2021, URL https://en.bitcoin.it/wiki/Controlled_supply, Accessed: Apr. 15, 2021.
[36] IBM quantum experience. 2021, URL https://quantum-computing.ibm.com/, Accessed: Apr. 15, 2021.
[37] Devitt SJ. Performing quantum computing experiments in the cloud. Phys Rev A 2016;94(3):032329.
[38] Castelvecchi D. IBM's quantum cloud computer goes commercial. Nat News 2017;543(7644):159.
[39] Bitcoin clock. 2021, URL https://www.buybitcoinworldwide.com/bitcoin-clock/, Accessed: Apr. 15, 2021.
[40] Kraft D. Difficulty control for blockchain-based consensus systems. Peer-to-Peer Netw Appl 2016;9(2):397–413.
[41] Hopwood D, Bowe S, Hornby T, Wilcox N. Zcash protocol specification. San Francisco, CA, USA: GitHub; 2016.
[42] Cojocaru A, Garay JA, Kiayias A, Song F, Wallden P. The bitcoin backbone protocol against quantum adversaries. IACR Cryptol ePrint Arch 2019;2019:1150.
[43] Behnia R, Postlethwaite EW, Ozmen MO, Yavuz AA. Lattice-based proof-of-work for post-quantum blockchains. IACR Cryptol ePrint Arch 2020;2020:1362.
[44] Chen J, Gan W, Hu M, Chen C-M. On the construction of a post-quantum blockchain. In: 2021 IEEE conference on dependable and secure computing (DSC). IEEE; 2021, p. 1–8.
[45] Faugere J-C, Horan K, Kahrobaei D, Kaplan M, Kashefi E, Perret L. Fast quantum algorithm for solving multivariate quadratic equations. 2017, arXiv preprint arXiv:1712.07211.
[46] Laarhoven T, Mosca M, Van De Pol J. Solving the shortest vector problem in lattices faster using quantum search. In: International workshop on post-quantum cryptography. Springer; 2013, p. 83–101.
[47] Dziembowski S, Faust S, Kolmogorov V, Pietrzak K. Proofs of space. In: Annual cryptology conference. Springer; 2015, p. 585–605.
[48] Bentov I, Lee C, Mizrahi A, Rosenfeld M. Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. ACM SIGMETRICS Perform Eval Rev 2014;42(3):34–7.
[49] Li W, Andreina S, Bohli J-M, Karame G. Securing proof-of-stake blockchain protocols. In: Data privacy management, cryptocurrencies and blockchain technology. Springer; 2017, p. 297–315.
[50] Khalifa AM, Bahaa-Eldin AM, Sobh MA. Quantum attacks and defenses for proof-of-stake. In: 2019 14th international conference on computer engineering and systems (ICCES). IEEE; 2019, p. 112–7.
[51] Blocki J, Lee S, Zhou S. On the security of proofs of sequential work in a post-quantum world. 2020, arXiv preprint arXiv:2006.10972.
[52] Alwen J, Chen B, Pietrzak K, Reyzin L, Tessaro S. Scrypt is maximally memory-hard. In: Annual international conference on the theory and applications of cryptographic techniques. Springer; 2017, p. 33–62.
[53] Barz S, Kashefi E, Broadbent A, Fitzsimons JF, Zeilinger A, Walther P. Demonstration of blind quantum computing. Science 2012;335(6066):303–8.