Bitcoin and Quantum Computing

Author: Craig Wright

Abstract

This paper addresses recently raised concerns that cryptocurrency protocols are not quantum computer proof. We present clear evidence that attacks on bitcoin using quantum computers are not viable in terms of economic costs. The economic argument is presented under two strong assumptions: (i) availability of well-known bitcoin addresses that are single-key reused addresses with exposed public keys, and (ii) existence of universal fault-tolerant quantum computers (FTQCs) of sufficient processing power and size in qubits. If the assumptions are relaxed, existing evidence asserts that quantum computer attacks are not viable in any foreseeable future, irrespective of economic costs. The Bitcoin protocol enables individuals and organisations to move their funds to unused bitcoin addresses and to use multiple-key addresses. This prevents any scenarios implied with the first assumption, and bitcoin addresses cannot be attacked if the public keys have not been exposed. Thus, no scenario exists where a quantum computer attack is viable. Furthermore, restraints on and a slow progress in physically implementing FTQCs that are sufficiently powerful do not support claims about near-term solutions to NP-hard problems such as breaking encryption. The evidence and opposing research indicate that any scenarios under the assumption (ii) are at best a distant future. The paper concludes that while there are no attack-based use cases for quantum computers, there are viable use cases for QC recovery systems. These include scenarios where a public key associated with a hidden Bitcoin address and unknown private key is left with an escrow firm or family members and scenarios of long-term lost keys associated with early bitcoin addresses.

Keywords: Bitcoin, Quantum Computing, Encryption,

Electronic copy available at: https://ssrn.com/abstract=3152419

Introduction

The field of quantum computing offers a lot of theoretical promise to the computation of specialist problems. The use of Shor's algorithm (Shor, 1999) has been touted as an end to encryption and digital signatures, at least as we know them now. Since the 1980s, fault-tolerant quantum computing (FTQC) has been a breakthrough that is just around the corner. Quantum computing is a large-scale, expensive exercise. In this paper, we address both the problems with errors in quantum computing and the feasibility of such a system and then continue to look at the economic impact of such a machine. From this analysis, we demonstrate that the best case for quantum computing is far from threatening towards cryptology anytime in the foreseeable future and then, in fact, it may be infeasible.

The interesting thing with Moore's law and cryptography is that we double in computational power every 18 months and manage to increase the length of a key we can reasonably crack at the same rate. The result is that keys stated to last millions of years are only viable for a small fraction of that time. This is not a consequence of some mythical quantum system; rather it is a factor of classical computation and the advances in technology. We cannot expect to break 256 bit ECC in the next 10,000 years using any existing modern classical computer system. Yet, if we simply wait[1], we would have a home computer in under 200 years that could readily and quickly solve ECC and all other public-private key schemes in everyday use.

At this point, we could have moved to 512 or even 1024 Bit ECC, and we would still be secure from attack.

The requirements for encrypting data come from:

- The length of time that the information needs to be secured,
- The amount of time it would take to transition to a new algorithm or to increase key size,
- How long we can expect to have, an algorithm survive attacks (including from Quantum systems if these are developed).

Quantum Computation

Quantum computers are hypothetical machines that are based on several postulates from quantum mechanics in physics. If these hypothesises from Deutsch (1985) and others prove true, then it is possible that quantum computers could outpace classical calculation on an electro-mechanical computer. Much of the existing hype stems from Shor's finding (Shor, 1999) of a polynomial quantum algorithm that allows for the factorization of selected classes of numbers and algorithms (especially those associated with cryptographic processes).

As with all undeveloped but potentially promising technologies, the scientists creating these oversell the near-term capability. This is to be expected. Without funding, they would never come to exist. The result is that there are many purely theoretical attacks right now that are using Quantum Computation as an excuse to move people into new and untested areas. On such area of attack has been in cryptocurrency and Bitcoin were many false rumours have been spread ([2]). Some of this reporting (intentionally) obscures the forms of calculation needed to break a system ([3]) confounding the reader into a false belief that the end is high.

The reality is that the arguments are spurious at best, at worst, they are intentionally designed to deceive. In this paper, we demonstrate the flaws in these arguments and show that systems (such as Bitcoin) are safe for at least the next few decades and maybe for all time from such an attack.

[1] The assumption is that Moore's law or at least a computational equivalent continues to hold for this time.

[2] https://www.cryptocoinsnews.com/quantum-computers-will-destroy-bitcoin-scientists-warn/

[3] https://www.cryptocoinsnews.com/nsa-working-encryption-cracking-quantum-computer/

Electronic copy available at: https://ssrn.com/abstract=3152419

The postulate of quantum computation

Feynman (1982) and Deutsch (1985) provided us with the audacious conjecture that "*Computational devices based on quantum mechanics will be computationally superior compared to digital computers*". This was taken further by Shor (1999) and the proclamation that quantum computers will be capable of factoring integers in polynomial time.

Quantum systems are inherently noisy. Some, including Shor, believe this to be a minor issue with decoherence being a simple problem. Other researchers are far from certain ([4]).

No company or research group has created even the simplest of universal quantum computers yet. The systems are all specialised systems and not true Quantum Computers. This is as no system has been able to hold coherence to create even a single logical qubit for any amount of time.

IBM Marketing has announced that they "expect(s) to have a 5-8 Qubit universal system BY 2020" ([5]). Then again, this has been a consistent refrain since the 1980's with

A system to break 256 bit ECC will need to have at least 20,000 logical Qubits to be effective in factoring large numbers. Much of the theory shows that a 100,000 - 1 million logical Qubit machine would be required to equal existing systems that factor large primes. To do what is needed for ECDSA cracking in close to real time (under an hour), this could be as large as a 10 million logical qubit machine.

The hypothesis of fault-tolerant quantum computation (FTQC) states that under selected conditions the threshold theorem on the expected expectations of statistical independence over the rate of noise will lead to the possibility that the noise per logical qubit could be sufficiently low per computer cycle to enable an FTQC to work (Aharonov, & Ben-Or, 1999; Kitaev, 1997; Knill, et. Al. 1998; & Gottesman, 1997).

Other researchers are complete sceptics and do not believe that FTQC is even feasible and will never be achieved ([6]). Kalai (2008) holds a position he calls the "postulate of noise: Quantum systems are noisy" which he conjectures cannot allow the creation of a large FTQC. He holds that "*computationally superior quantum computers depend on realizing quantum error correction codes, which are not witnessed in nature, weakens the initial rationale given for quantum computers*".

One of the primary concerns with the recovery of information from quantum systems is attributed to error recovery. In none quantum systems, errors are distributed as white noise. The distribution of errors is independent and identically distributed information that is stochastically varied around a central point at a time. This differs significantly from much of the results found in quantum computing. As noted with Gross, Flammia & Eisert (2009) quantum states are generally found to be entangled. This interferes with the recovery of information as existing statistical tools do not handle the separation of information and errors from highly correlated information very well.

[4] http://www.ijesi.org/papers/Vol(3)10/F031059070.pdf
https://arxiv.org/abs/1111.3965v3
https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.108.260501
https://arxiv.org/abs/1111.5425
Gross, Flammia, Eisert, "Most Quantum States Are Too Entangled To Be Useful As Computational Resources." Physical Review Letters (2009). Available online: http://link.aps.org/doi/10.1103/PhysRevLett.102.190501
https://eandt.theiet.org/content/articles/2016/11/the-trouble-with-quantum-computing/

[5] http://www.wtec.org/Nano_Research_Directions_to_2020.pdf

[6] https://gilkalai.files.wordpress.com/2009/12/qi.pdf
https://arxiv.org/pdf/1106.0485.pdf
https://arxiv.org/pdf/1605.00992.pdf

What are quantum computers and how they work

The complete definition of quantum mechanics and quantum computing is far beyond the scope of this paper. We will address only the basics and point the reader to several well-known papers on the topic.

Some of the primary problems with the understanding of any quantum system derive directly from the fundamental tenets of quantum mechanics. The mere observation of a phenomenon changes the outcome of the event that is to be measured. Any interaction with a quantum particle, (in the case of a quantum computer, the qubit) fundamentally and irreversibly alters the state of the system that is to be measured. This results in the problem of not knowing whether a quantum system is behaving as we would expect. In theory, we can create systems that work toward solutions with infinite precision allowing us to so problems such as the factorization of large numbers.

This problem requires the development of a universal quantum computer (). In order to create such a system, it would be required to implement quantum gates that measure the lattice vibrations and/or the nucleus been of the individual particles associated with the qubits to be measured. This, of course, led to the discovery of introduced decoherence effects. This effect introduces stochastically variable information that creates a level of errors in any measurement. The proposed solution in the development of an FTQC has been to decide upon an error rate and design around it. This error rate cannot be completely removed; however, the theorists believe that the introduction of additional qubits will provide sufficient error correction to enable the creation of a working quantum computer.

The creation of qubits is a difficult task, the introduction of multiple qubits to form a single logical qubit is incrementally more difficult. Some of the current implementation proposals call for the integration of seven physical qubits into the creation of a single first layer logical qubit. To reduce the error rate on calculations sufficiently at least two layers of logical qubits are reconstructed to create an array of 49 qubits that acts as a single fault resistant logical qubit.

The most important thing to note here is that we have not created a system with more than five qubits at present, so the creation of a logical qubit with either seven or 49 physical components remains speculative at best.

There are many proposals the detail novel ways of creating physical qubits ([7]). These are currently plausible at a small scale. The difficulty comes from the fact that we do not know how to scale these nor even if it would be possible to scale a quantum computer into the realms of what is expounded within the theory.

A working, scalable quantum computer would require a solution to the problem of quantum decoherence first. Any quantum system needs to be isolated from all surrounding interactions as any effects from surrounding particles will result in the particle decal hearing or collapsing into a binary

[7] J. J. L. Morton; et al. (2008). "Solid-state quantum memory using the 31P nuclear spin". Nature. 455 (7216): 1085–1088. arXiv:0803.2021Freely accessible. Bibcode:2008Natur.455.1085M. doi:10.1038/nature07295.

Kamyar Saeedi; et al. (2013). "Room-Temperature Quantum Bit Storage Exceeding 39 Minutes Using Ionized Donors in Silicon-28". Science. 342 (6160): 830–833. Bibcode:2013Sci...342..830S. doi:10.1126/science.1239584.

Náfrádi, Bálint; Choucair, Mohammad; Dinse, Klaus-Pete; Forró, László (July 18, 2016). "Room temperature manipulation of long lifetime spins in metallic-like carbon nanospheres". Nature Communications. 7: 12232. doi:10.1038/ncomms12232.

https://phys.org/news/2016-12-scientists-quantum-memory-cell-higher.html,

http://www.nature.com/articles/ncomms7979 state an analogous to a classical computer. For all the hype, no quantum computer has ever been judged empirically to be working as the theory would state. Quantum computing is not deterministic. The coding of a quantum system necessarily leads to a probabilistic result. We are used to running a program in obtaining the same result for each iteration that we engage with the same input. Quantum systems are inherently different to this. In order to gain an accurate result, the calculation on a quantum computer needs to be run as a repeated loop many times until the probabilistic likelihood of a different result is minimised. This is the reason why quantum computers office I little advantage to many forms of computation.

The magical properties of quantum computers have been linked to theoretical algorithms that are proposed to provide factorisation solutions in the realm of cryptography (this is recovering prime factors of very large numbers and related problems).

The next problem with the probabilistic system is that it is not necessary that it is feasible to determine if the has been produced. While we can take the results associated with the generation of a cryptographic private key and verify on a classical computer whether this value corresponds to the satiated private key is seeking to factor, there is no way to determine whether any of the output is correct before testing. The result is necessarily having to run many iterations before being able to determine whether the result is correct. Some promise has been proposed around the technique of "blind quantum computing"[8]. This technique has been demonstrated to work on a small-scale using a full qubit quantum computer to verify the results of a second computer.

As Scott Aaronson noted in Science[9], "*Like almost all current quantum computing experiments, this currently has the status of a fun demonstration proof of concept, rather than anything that's directly useful yet*".

Proposals exist for the creation of multiple quantum computers consisting of dual entangled qubits. The problem with these proposals is that not only are the solutions outside the range of present technology but that we don't even know if the fundamental particles that we seek to entangle exist.

Can a Quantum Computer even be built that can factor large numbers?

The initial question is can a quantum computer even exist on any scale and for any amount of time. The existing limit is five (5) physical qubits and 35 seconds of coherence ([10]). This is far too low a time before decoherence to solve any meaningful factorisation problem. The number of qubits is also too low to create even a single logical qubit. The goal of creating the holy grail of a single "logical qubit" ([11]) remains just as elusive as it was 30 years ago. We know far more of what we do not know, and yet we do not know whether it is even possible to solve for the errors in a noisy quantum system.

Physical 5 and 7-qubit machines were built 15 years ago [Vandersypen00[12], Laflamme99]. One of the reasons was noted in a presentation (Chong, [13]) presented in figure 1. One of the often overlooked aspects of existing quantum computing research comes in the differentiation between physical and logical qubits. The creation of effective logical qubits becomes elusive due to the entanglement of particles. Without the ability to filter noise statistically, the creation of individual qubits becomes elusive, exponentially more expensive and slower.

[8] http://www.nature.com/nphys/journal/v9/n11/full/nphys2763.html

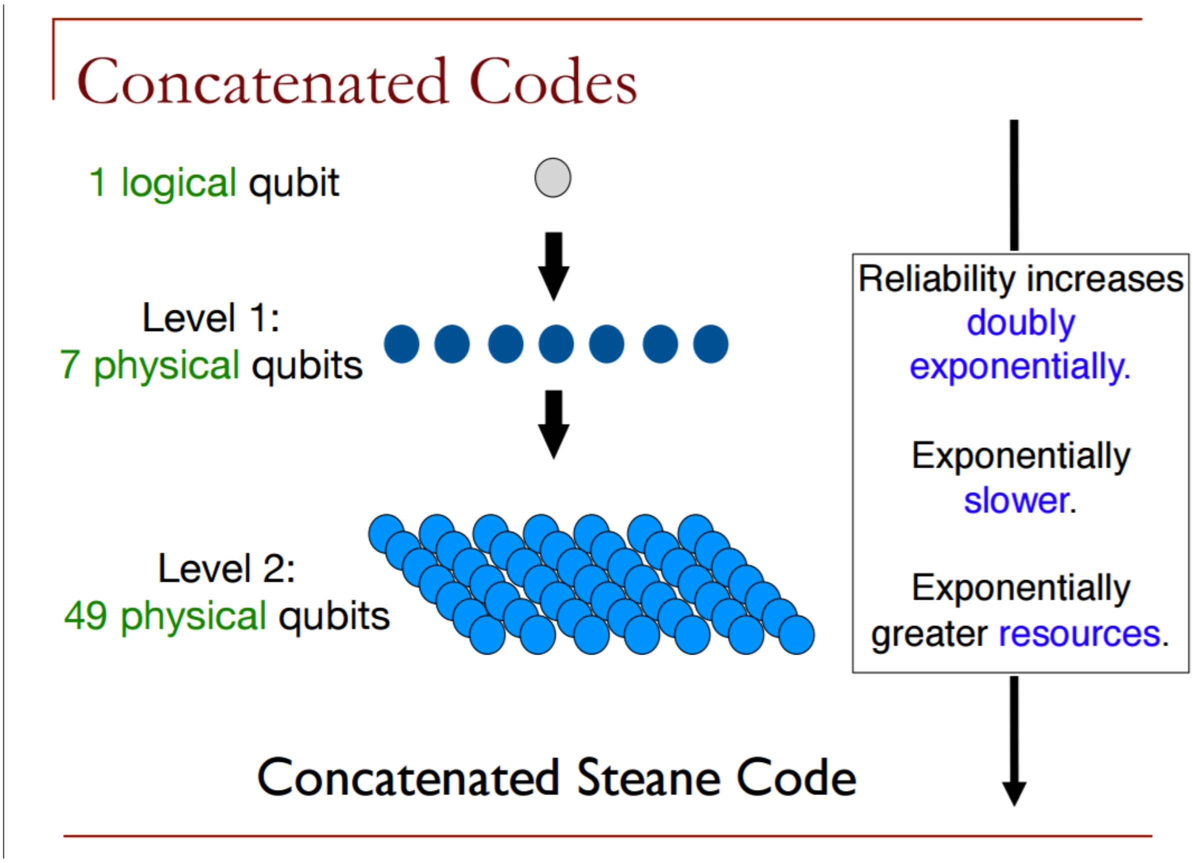
[9] http://www.sciencemag.org/news/2013/09/quantum-computers-check-each-other-s-work

[10] https://www.youtube.com/watch?v=kq2QrTgCZ3U

[11] https://www.fastcompany.com/3045708/big-tiny-problems-for-quantum-computing

[12] Vandersypen, Steffen, Breyta, Yannoni, Sherwood, and Chuang, 2001

[13] http://people.cs.uchicago.edu/~ftchong/Chong-QC-SFU-2015.pdf



Concatenated Codes

1 logical qubit

Level 1:
7 physical qubits

Level 2:
49 physical qubits

Reliability increases doubly exponentially.

Exponentially slower.

Exponentially greater resources.

Concatenated Steane Code

Figure 1: Reliability and speed as QBits are created

As Gil Kalai states ([14]):

"*Quantum computers are larger-than-life. Quantum computers may well add to our long list of failures in larger-than-life human quests. Mathematically speaking, that large-than-life dreams end so often in disappointment demonstrates how large life itself is.*"

Noise ([15]), as we noted above is a major issue.

Conjecture: *The rate of noise in a time interval is bounded below by a measure of non-commutativity of the unitary evolutions* $U_{s,t}$ *in this interval.*

Probabilistic Turing Machines

The addition of stochastic processes into a Universal Turing Machine has been promoted in the concept of "Hypercomputation" ([16]) to which some class quantum computers ([17]). The problem is an old one ([18]). It is well known that randomness does not genuinely enhance the computational power (Sipser [19]). It has been proven that every nondeterministic machine can be simulated in the same space by a probabilistic machine with a small error probability ([20]). However, the power of such a machine is equivalent to a Universal Turing machine of a deterministic nature.

[14] https://rjlipton.wordpress.com/2012/10/03/quantum-supremacy-or-classical-control/
[15] https://gilkalai.files.wordpress.com/2009/12/qi.pdf
[16] http://www.dcs.shef.ac.uk/intranet/research/public/resmes/CS0203.pdf
[17] http://www.jstor.org/stable/10.1086/521969?seq=1#page_scan_tab_contents
[18] http://dl.acm.org/citation.cfm?id=803889
[19] https://books.google.co.uk/books?id=P3f6CAAAQBAJ
[20] http://epubs.siam.org/doi/abs/10.1137/0206049

D-Wave and Adiabatic computers

There has been a great deal of FUD[21] (Fear, uncertainty and doubt) spread through the use of Quantum Computers in cracking cryptographic algorithms. Some of this has derived from knowledgeable researchers who know better but see the profit in creating and disseminating fear. The results of which have led to a wide disparity in the knowledge held by the general computing community and that which is feasible ([22]).

The marketing around the so-called quantum systems[23] that have been developed and deployed in the real world ([24]) has failed to live up to the promises. D-Wave has shown promise in the use of its adiabatic quantum computer in the solution to quadratic unconstrained binary optimisation ([25] and [26]). However, this type of problem is unrelated to the solution of large number factorisation (this is the key aspect of brute forcing the solutions to cryptographic keys)

Umesh Vazirani (2009) in reply to an article by the Economist ([27]) espousing D-Wave's system and the forthcoming advances demonstrates that many of the claimed marketing devices are far from scientific:

> *"Your article regarding D-Wave's demonstration of a "practical quantum computer", sets a new standard for sloppy science journalism. Most egregious is your assertion that quantum computers can solve NP-complete problems in "one shot" by exploring exponentially many solutions at once. This mistaken view was put to rest in the infancy of quantum computation over a decade ago when it was established that the axioms of quantum physics severely restrict the type of information accessible during a measurement. For unstructured search problems like the NP-complete problems, this means that there is no exponential speed up but rather at most a quadratic speed up.*
>
> *Your assertions about D-Wave are equally specious. A 16 qubit quantum computer has smaller processing power than a cell phone and hardly represents a practical breakthrough. Any claims about D-Wave's accomplishments must therefore rest on their ability to increase the number of qubits by a couple of orders of magnitude while maintaining the fragile quantum states of the qubits. Unfortunately D-Wave, by their own admission, have not even tested whether the qubits in their current implementation are in a coherent quantum state. So it quite a stretch to assert that they have a working quantum computer let alone one that*

[21] http://www.newyorker.com/tech/elements/hacking-cryptography-and-the-countdown-to-quantum-computing https://blog.kaspersky.com/quantum-computers-and-the-end-of-security/2852/ , http://www.economist.com/news/science-and-technology/21654566-after-decades-languishing-laboratory-quantum-computers-are-attracting , https://www.extremetech.com/computing/243386-d-waves-quantum-computers-take-quantum-leap-forward-now-offer-2000-qubits , http://news.mit.edu/2016/quantum-computer-end-encryption-schemes-0303

[22] https://pdfs.semanticscholar.org/c343/b423982892adb4db3916a3a4325a4ff00462.pdf?_ga=1.119413641.1416926696.1485867148

[23] https://www.cyberscoop.com/looking-edge-cybersecurity-firms-spend-big-quantum-computing/

[24] http://www.economist.com/news/science-and-technology/21578027-first-real-world-contests-between-quantum-computers-and-standard-ones-faster

[25] Endre Boros, Peter L Hammer & Gabriel Tavares (April 2007). "Local search heuristics for Quadratic Unconstrained Binary Optimization (QUBO)". Journal of Heuristics. Association for Computing Machinery. 13 (2): 99–132. doi:10.1007/s10732-007-9009-3

[26] Di Wang & Robert Kleinberg (November 2009). "Analyzing quadratic unconstrained binary optimization problems via multicommodity flows". Discrete Applied Mathematics. Elsevier. 157 (18): 3746–3753. doi:10.1016/j.dam.2009.07.009

[27] http://www.economist.com/node/8697464

> *potentially scales. An even bleaker picture emerges when one more closely examines their algorithmic approach. Their claimed speed up over classical algorithms appears to be based on a misunderstanding of a paper my colleagues van Dam, Mosca and I wrote on "The power of adiabatic quantum computing". That speed up unfortunately does not hold in the setting at hand, and therefore D-Wave's "quantum computer" even if it turns out to be a true quantum computer, and even if it can be scaled to thousands of qubits, would likely not be more powerful than a cell phone".*

So, despite all the recent hype and aggrandisement, we are no closer to a Universal Quantum Computer for all the claims made by D-Wave at launch.

"Quantum annealing does not bring us closer to universal quantum computing," says Jerry Chow, manager of IBM's Experimental Quantum Computing team. "It is unclear whether there are any speed-ups that can be gotten from a quantum annealing system over classical algorithms." ([28]).

Not all classical problems can be solved on a Quantum Computer

A recent discovery (Eisert, Müller, & Gogolin, 2012) has revealed that the many problems undecidability may be a quantum property. The authors state that:

"*Undecidability hence appears as a genuine quantum property here. Formally, an undecidable problem is a decision problem for which one cannot construct a single algorithm that will always provide a correct answer in finite time.*"

The implication implies that Gödel's first incompleteness theorem (Kleene, 1967) cannot be achieved using quantum tools. The extension of this is that many problems that are decidable under classical systems may not be decidable under a quantum system. The takeaway of this is that even if it was possible to solve simple private key based solutions, it might not be possible to solve more complex scripted scenarios and bitcoin. The takeaway from this is that we could feasibly create small addresses holding little value that are not worth attacking that are coupled with more complex scripts that are insoluble even when attacked by quantum computers should one come to exist. The creation of a tree of possible solutions leaves the holy grail of a cryptographic backdoor unlikely, to say the least.

Wu (2014[29]) takes this argument further arguing that general-purpose quantum computing through the use of qubits is fundamentally flawed. In his argument, Wu points out that flux qubits operate only in a point contact process he states that the harmonic oscillator rings are only weakly coupled but that to be useful the readout process needs to be coupled strongly to a harmonic process. He notes other problems such as the superposition of states leading to closely coupled errors. Overall, when taken together these may not be insurmountable obstacles, but they do limit any capability of a system to be developed that efficiently reverses encryption. This, of course, is the primary concern. It is not whether encryption can be broken, but whether it can be broken within a reasonable timeframe and for an economically viable investment. All modern encryption is probabilistically based and hence can be broken based on an economic calculation. The reality is that it is rarely the case that any key would be worth the investment.

With the march of time, we lose one it of encryption every 18 months or so due to Moore's law. A machine that can break 100 bits worth of encryption and 150 years is of little economic benefit for this reason.

[28] https://eandt.theiet.org/content/articles/2016/11/the-trouble-with-quantum-computing/

[29] http://www.ijesi.org/papers/Vol(3)10/F031059070.pdf

The Economics

When we start to analyse the cost impacts of attacking bitcoin using a quantum computer we can see the fallacy of the arguments made against changing protocols. To be effective, any attack launched from a quantum computer needs to be successful before the owner of the private key can spend the bitcoin and move it to a new address. We present research demonstrating that it would be expected to take about 110 days on average to resolve a bitcoin public key into a private key value if the surrounding difficulties associated with quantum computing can be solved. For this section, we will assume that is the case. It is well known that Grosvenor's algorithm will solve hash puzzles at a rate that is far too slow to be effective in attacking bitcoin. If we take the assumption that sometime in the future Shor's algorithm coupled with hypothetical advances in theoretical quantum computers will lead to a scenario that produces optimised attacks against keys that far exceeds anything that is considered to be currently possible we may be able to create a system that could reduce an individual public key into the associated private key within a reduced timeframe of only 30 days.

This is what is presented by many as the nightmare scenario. In this scenario, a quantum computer costing and expected 1-20 billion US dollars would be able to crack 12 ECC private keys associated with bitcoin addresses each year. The conditions on this of course link directly to knowledge of the bitcoin public key. Without inside knowledge, such as that which could come from a system compromise or the prior use of a bitcoin address leading to the exposure of the public key there is no known manner in which a quantum computer can attack bitcoin. The limitations of a quantum computer do not extend to reversing hashed values, and as such, there is no way for a quantum computer to recover bitcoin public keys within the lifespan of our solar system. Given this information, we can see very simply that any attack must either incorporate external knowledge about the source of a public key or wait until a transaction has occurred and which has moved funds to a new address. Hence, any attack against and exposed public key relies heavily on key re-use. In not reusing a key, and attack on a public key becomes hollow and unprofitable.

Economically, it thus only becomes viable to attack well-known and reused bitcoin addresses that have exposed public keys and which hold large amounts of value for periods greater than 30 days. Even at face value we can demonstrate that this is not a concern. A large organisation that has a fixed address for receiving payments and ones that are derived from this is still not vulnerable. Any payments being received and first be moved between addresses from the receiving address to an alternate address owned by the corporation or another group within minutes of receipt. Further, any attack on a Bitcoin address requires an attack on all the keys associated with the address. Using multi-signature addresses, an organisation could create a 15 of 15 key. Even allowing for the hypothetical scenario where an exposed private key could be reverse engineered in under 30 days we come to the creation of a multiple key address that would take 18 months to compromise.

If an organisation used such a key and simply changed the payment address on a 12-monthly basis with three months leeway, they would solve any vulnerability to attacks from a quantum computer. The addition of the hash puzzle within a more complex script would completely remove any such attack. The creation of a script that incorporates both an EcDSA signature set coupled with a hash puzzle would mitigate any ability for a quantum computer to attack bitcoin.

Finally, we can address the feasibility of such a system. A large-scale quantum computer will not be a system that ever scales along the lines of more traditional computer and Moore's law. Some orders of growth may be possible, but it is also feasible that the systems will remain as large-scale specialist systems requiring oversized facilities to manage and maintain them. In the best case, we see a facility costing in the order of $1 billion US as a minimum. Even given this theoretical best case scenario, we could expect costs between 150 and $200 million US including depreciation to cover the operational range of this machine. Again it the best case scenario we would have a situation where a machine that costs in the order of $150 million US per annum to run would be able to crack 12 private keys in a single year. To make sense, the creation of such a system dedicated to cracking bitcoin keys would need to find abandoned public keys that hold Bitcoin valued at $12.5 million each on a consistent basis. As we have demonstrated, it is simple to move between bitcoin addresses and to use a combination of multisig addresses and hash puzzles to thwart any attack in an active organisation. We also cannot forget that quantum computers cannot attack bitcoin addresses where the public key has not been exposed.

At present, the largest individual bitcoin address holds an amount equal in value to $150 million US[30] in a single address. This it seems is viable to attack. However, remember the simple solution if this was to be exposed such that the public key on this address was known would be to move the funds to another address. This can be done in under 10 minutes. An attack using a quantum computer would require over a month. Even this address is safe. The largest address with an exposed public key[31] (from 2014) holds a balance of only $14.5 Million USD. Individually, this address from 2014 could be attacked profitably. The problem is that a quantum computer dedicated to reversing bitcoin public addresses would need to find several hundred such addresses all holding an average of 12.5 million USD in Bitcoin. The totality of such addresses at present would not pay for four months of operation of this machine.

Even targeting the largest known addresses would only lead to a scenario where individuals move their funds to an unused bitcoin address. The simple reality is that no scenario exists where it would be viable to use a quantum computer to attack bitcoin. Was such a system to be developed to pre-image bitcoin addresses, we would find that classical computers using vanity addressing algorithms would, in fact, outperform the quantum computer. Although the quantum computer can in theory individually reverse a single known private key given an exposed public key, Shor's algorithm does not lead to a methodology that is superior to known methods on classical computers of creating pre-images of private keys and bitcoin addresses that can be added to a lookup table. Seeing such a system would still require longer than the life span of this universe to make any effective system we can discard it.

The future opportunities

In the long term, there is no attack based use cases for a quantum computer. For larger values, quantum computers could be used as recovery systems. At present, attempting to recover addresses with 50 bitcoin remains uneconomical. In a future scenario where the value of Bitcoin exceeds $1 million US per bitcoin, there are many addresses that could be recovered potentially in a salvage environment where the owner is known. Here, an individual could note the public key associated with a private key and save this knowing that the public key will only be tied back to the private key in cases where the information they maintain is released. Such a situation could involve leaving public keys with escrow firms or with family members. An untimely death where the private key has been lost could result in a scenario where family members know the public key associated with a hidden Bitcoin address and unknown private key. This future quantum computer scenario is not an attack but rather a recovery feature. Long-term lost keys where the private key is unknown, but there is a public key that has been disclosed (including some early Bitcoin addresses) using pay to pub key addressing would also be viable. As noted above, none of this could be considered or construed to be an attack.

What does this mean to Bitcoin?

Hype has been a constant in the Bitcoin reporting world ([32]). Andersen Cheng ([33]), who was noted as "the co-founder of a UK-based cyber security firm, Post-Quantum" in NewsBTC was quoted stating:

[30] 1JCe8z4jJVNXSjohjM4i9Hh813dLCNx2Sy

[31] 19tuxqhzgwC6B9hhLHDLJkocx8LaaCS56s

[32] http://www.businessinsider.com/bitcoin-is-dead-2016-4

[33] http://www.newsbtc.com/2016/10/16/will-quantum-computers-spell-doom-bitcoin/

"*Bitcoin is definitely not quantum computer proof… Bitcoin will expire the very day first quantum computer appears.*"

The reason is simple; there are large pools of funds ([34]) for companies to develop solutions to these yet unknown and untested problems. Fear is a powerful motivator. When selling solutions, the ability to sell a solution to a problem that is likely not to exist ([35]) in the short term (if ever) can be an incredibly profitable scenario.

Core Bitcoin developers have been using the uncertainty around a non-existent quantum code cracking system to convince people of the requirements to change to alternative cryptographic primates that suit the implementation of Sidechains. They have been pushing the use of Lamport signatures [Lam79], stating that "while large, are secure against quantum computers". This addition of large and unneeded computation into the Bitcoin signature scheme is unnecessary and is designed to fend off an imaginary attack from a non-existent foe. The true reason for the change to Lamport signatures is not quantum hardening; it is to enable the adoption of Sidechains ([36]) in a manner that can be released by the funder of Core, Blockstream. In fact, the CEO of Blockstream, Adam Back has been a long-term proponent of altering ([37]) Bitcoin fundamentally with the desire to "introduce a new signature type" that will change the structure of the protocol irrevocably. This is not a solution to attack from a quantum computer; it is an attempt to alter the underlying system and protocol.

The reality is there is nothing to fear

Most importantly, Bitcoin uses a double hashing algorithm. The results of this scenario are that any unused bitcoin address will not be reversible to the public key, let alone able to be attacked through a reversal of the ECDSA key pair. An algorithm such as Grover's algorithm (Grover, 1996) are touted as being able to speed up the searching through possible collisions in the reversing of hashing algorithms including SHA-256.

This algorithm is known to be at best a solution in BPP ([38]), a class of decision problem that is decidable in polynomial time with an error probability bounded by 1/3 (for all inputs). The idea is that this error rate can be minimised or made to be exponentially small in 'k" using a process of iterating the algorithm 'k' times with the most frequent value returned as a result. This process ignores the noise of the quantum computer and reports an error rate based on the ideal system alone. Bennet et al. (1997) demonstrate how an ideal quantum Turning machine cannot find a solution to an NP problem in less than time $O(2^{n/2})$. For SHA-256, this is time $O(2^{128})$ and is a far more difficult problem when the true problem, the solution of a bounded size hash to a hash puzzle is introduced. His conclusion was that "*Anyone afraid of quantum hash-collision algorithms already has much more to fear from non-quantum hash-collision algorithms*".

More importantly, when Bernstein (2009, [39]) analysed the known quantum algorithms, he demonstrated conclusively that "all the quantum-collision algorithms in the literature are steps backwards from the

[34] https://techcrunch.com/2016/07/07/quantum-encryption-startup-pq-bags-10-3m-series-a/

[35] Nickell, J (1998-12-01). "Peddling Snake Oil; Investigative Files". Skeptical Inquirer. Committee for Skeptical Inquiry. 8 (4). Retrieved 2011-12-04.

[36] https://bitcoinmagazine.com/articles/side-chains-challenges-potential-1397614121/

[37] http://www.mail-archive.com/bitcoin-development@lists.sourceforge.net/msg07122.html

[38] Bennett C.H.; Bernstein E.; Brassard G.; Vazirani U. (1997). "The strengths and weaknesses of quantum computation". SIAM Journal on Computing. 26(5): 1510–1523.

[39] "Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete?", Daniel J. Bernstein 2009. https://cr.yp.to/hash/collisioncost-20090517.pdf

non-quantum algorithm of (Oorschot, et al. [40]). In other words, any attack on the hash functions of Bitcoin would be more effective using a classical computer.

Bitcoin is thus secure against (theoretical) quantum computer attacks against a key that has not been used. Once a transaction is signed and sent to the blockchain, an attacker can extract the public key. This is not a flaw in the algorithm but a standard part of the functioning of ECC and ECDSA based systems. The question is then, what is the cost to an attacker to break the ECDSA key itself?

Grover's algorithm could be said to reduce the bit-security of such primitives by half; one might say that a 256-bit pre-quantum primitive offers only 128-bit security in a post-quantum setting. This is far too large to be broken on any QC any time in the foreseeable future. However, Bitcoin uses the Hash of a Hash. The combination of both SHA256 bit hashes of SHA256 values and the use of a 160Bit RipeMD hash of a SHA256 value for an address makes the analysis of bitcoin addresses to uncover the private key infeasible.

Attacking ECDSA with Shor

Let us for a moment assume that a working solution to the problem of creating logical qubits on a FTQC that can maintain coherence for long time periods can be achieved. We next need to note that Shor's algorithm is not simple and a Universal QC would need specialised breaks - you cannot just solve ECC in one hit as is suggested by many pundits.

The other common fallacy ([41]) and assumption are that a FTQC will just factor the private key before you can spend. It is more probable that even a 1 million logical qubit FTQC system would likely take weeks or months to break 256-bit ECDSA keys.

A Bitcoin user that never spends or receives Bitcoin to the same address and only uses an address once remains safe under all circumstances from quantum computers as the hashing process leaves the hacker unable to recover the public-key used to generate the address before the single spend event occurs. As we further note, the time to recover an ECDSA private key using only the public key is far greater than the time to settle the transaction (an average of 10 minutes).

To be vulnerable, singly used Bitcoin addresses would need to have a system that can break ECC in seconds. Yet if we take the analysis a comparable crypto systems by Proos and Zalka (2008, P. 2642) we see that their analysis leads to an equivalent processing time for performing a 2048-bit number Shor factorisation with a 224 bit elliptic curve key. The difficulty is a little bit greater than this but we have rounded down providing the benefit of the doubt towards the attacker. using the values presented in the paper we see that an attack against a known EcDSA bitcoin key will require the use of the system for around 110 days given a system size of 2×10^9 trapped ions. The development of a quantum computer built through the trapping of 2×10^9 ions it is estimated to require in the order of more than 500 (23 × 23) vacuum chambers (Lekitsch et. Al., 2017[43]) occupying an area of ca. 103.5 × 103.5 m^2.

Quantum algorithms Including Shor's require a substantial overhead in mapping the problem you want to solve onto the QC architecture. Consequently, the arguments on how many qubits are needed are wrong. You will require much more than N qubits to do what would classically take 2N steps. The ECDSA curve in Bitcoin has "*Good protection against quantum computers unless Shor's algorithm applies*" ([44]). We can conclude that we have at least until 2030 - 2040 and this is more than sufficient

[40] Paul C. van Oorschot, Michael Wiener, Parallel collision search with application to hash functions and discrete logarithms, in [2] (1994), 210–218

[41] http://spectrum.ieee.org/tech-talk/computing/hardware/encryptionbusting-quantum-computer-practices-factoring-in-scalable-fiveatom-experiment

[42] https://arxiv.org/pdf/quant-ph/0301141.pdf

[43] http://advances.sciencemag.org/content/3/2/e1601540.full

[44] http://cordis.europa.eu/docs/projects/cnect/6/216676/080/deliverables/002-DSPA20.pdf

time to change the algorithm if it was necessary. SHA 256 with QC has until at least 2080, and the likely attack is not quantum computers. The runtime bottleneck of Shor's algorithm is quantum modular exponentiation, which means that the (re)introduction of **OP_Mod** in Bitcoin script (and the alterations this can provide to key security - [45]) makes QC based solutions infeasible and takes the algorithm past 2080. We are sure that people will have other solutions before 2080.

The result is that a massively scaled quantum computer of a size beyond anything that is currently deemed possible would still require more time than is necessary to break bitcoin keys. A worst-case scenario would allow attackers to recover up to 3 keys a year. The cost of any such attack would be over $100 million US per key recovered aching any such attack infeasible. Even was an address to exist that held enough bitcoin to make such an attack warranted, the attack could be simply thwarted if the attacker was to use multiple keys. A standard 15 of 15 multi-signature address would provide five years' worth of security even if the public key was exposed on all 15 keys. For an attacker to target this address, the bitcoin address would be required to hold over US$1.5 billion worth of bitcoin.

Bitcoin Mining.

As we noted from Bernstein's (2009) results, quantum computers are slower at solving hash collision than are algorithms for the deployment on classical systems. Hence, there is no economic benefit for a miner to use Quantum Computers for the solution of hash puzzles as they would solve fewer hashes than a miner on a more traditional ASIC. This excludes the costs of the Quantum computer as well (which is significant) and does not consider the fact that qubits are slower to process than bits (Bernstein, 2009). The result is that a miner who was to deploy a Quantum computer for the mining of Bitcoin (if one was to ever exist in the first place) would be at an economic disadvantage to a miner using more traditional ASIC-based systems.

Post-quantum cryptography ([46]), a purported non-partisan site for the scientific dissemination of information concerning the effects of quantum computing on cryptography that is heavily used by partisan personalities including Vitalik Buterin, (co-founder of Ethereum) starts with the doom saying prophecy:

> “"*Imagine that it's fifteen years from now. Somebody announces that he's built a large quantum computer. RSA is dead. DSA is dead. Elliptic curves, hyperelliptic curves, class groups, whatever, dead, dead, dead. So users are going to run around screaming and say 'Oh my God, what do we do?*"”

This false prophecy is misleadingly designed to read as if it was a quote from Daniel Bernstein's ([47]) analysis. The removal of the line “*The New York Times runs a frontpage article reporting that all of the public-key algorithms used to protect the Internet have been broken”* changes the context where the author starts by stating, “*A closer look reveals, however, that there is no justification for the leap from “quantum computers destroy RSA and DSA and ECDSA” to “quantum computers destroy cryptography.”*”

More importantly, no consideration of the costs and time in uncovering a private key has been announced. As Bernstein (2009 [48]) also demonstrated, the move to alternate hashing algorithms is unwarranted due to theoretical quantum computers even were they to become a reality.

[45] Patent – x, type 42 addresses in script

[46] http://pqcrypto.org/

[47] "Introduction to post-quantum cryptography." http://pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf

[48] https://cr.yp.to/hash/collisioncost-20090517.pdf

So, please never listen to the FUD. Forget ideas such as Lamport Signatures (Lamport, 1979). Bitcoin is as it is for a reason and the reason that these others who worry about science fiction did not create it is the reason we need to maintain it as the protocol was created.

Conclusion

Scientific scepticism over quantum fault tolerance stems from a wide belief in its possibility with a little-associated investigation into its impossibility.

Many of the claims surrounding the imminent development of quantum computing systems have been echoed since the 80s. This is not a position we would expect to see otherwise. The long-term promise of quantum computing has a huge potential upside in many industries making it a valuable research topic even if it is a long shot. This comes to the economic problem of overpromising. Large-scale quantum computing is not in anyway analogous to classical computing. In the early days of classical computers, large, expensive machines were required to do simple calculations. Over time and along with developments in technology the economics of classical computing has led to rapid advances and increasingly available computer power.

Quantum computers do not work in this manner. It is unlikely in fact highly improbable that any small-scale low energy quantum computer will ever exist. For this to be wrong, it is not simply a matter of discovering new technology but that our existing knowledge of physics and particles must be radically misaligned to reality. The result is that quantum computing even if it is possible will remain in the realm of large data centres and government facilities.

This is a classical large-scale research problem. For any researcher to be funded, they must oversell both the result and the likelihood of achieving the result. This is not to state that there is no promise in Quantum computers, just that any claims to near-term solutions to NP-hard problems such as breaking encryption are more than grossly overstated.

Whereas sites (such as http://pqcrypto.org/) and people commonly misrepresent the capabilities of quantum based computing in compromising cryptography, the reality is we have little to fear. It is clear that bitcoin users have no need to lose sleep over the development of a quantum computer should even be possible.

References

1. Aharonov, D. & Ben-Or, M. (1999) "Fault-tolerant quantum computation with constant error", STOC '97, ACM, New York, pp. 176-188.
2. Deutsch, D., (1985) "Quantum theory, the Church-Turing principle and the universal quantum computer", Proc. Roy. Soc. Lond. A 400, 96–117.
3. Eisert, J., M. P. Mueller, and C. Gogolin. "Quantum Measurement Occurrence Is Undecidable." Physical Review Letters 108 (2012): 260501.
4. Feynman, R. P. (1982) "Simulating physics with computers, Int. J. Theor. Phys. 21, 467–488
5. Gottesman, D. "Stabilizer codes and quantum error-correction", Ph. D. Thesis, Caltech, quant-ph/9705052.
6. Gross, Flammia, Eisert, "Most Quantum States Are Too Entangled To Be Useful As Computational Resources." Physical Review Letters (2009). Available online: http://link.aps.org/doi/10.1103/PhysRevLett.102.190501
7. Grover L.K.: A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996) p. 212
8. Kalai, G., (2011) "How Quantum Computers Fail: Quantum Codes, Correlations in Physical Systems, and Noise Accumulation" Quantum Physics (quant-ph); Computational Complexity (cs.CC) Microsoft Research

9. Kitaev, A. Y., (1997) “Quantum error correction with imperfect gates”, in Quantum Communication, Computing, and Measurement (Proc. 3rd Int. Conf. of Quantum Communication and Measurement), Plenum Press, New York, pp. 181-188.
10. Kleene, S. C., Mathematical Logic (Wiley, New York, 1967)
11. Knill, E., Laflamme, R. & Zurek, W. H.. (1998) “Resilient quantum computation: error models and thresholds”, Proc. Royal Soc. London A 454, 365-384, quant-ph/9702058
12. L. Lamport, Constructing digital signatures from a one-way function, Tech. Report SRI-CSL-98, SRI International Computer Science Laboratory, October 1979.
13. Shor, P. W., (1999) “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”, SIAM Rev. 41 (1999), 303-332. (Earlier version, Proceedings of the 35th Annual Symposium on Foundations of Computer Science, 1994.)
14. Vazirani, Umesh "A Reply to "Quantum Computing"." The Economist (2007).