Your Keys; Not your Bitcoin

Will Quantum Computing End Cryptocurrencies?

Source: [1]

CID: 01502658

Word Count: 2884

Department of Physics
Imperial College London
December 2020

"Not your keys; not your Bitcoin" is the mantra of the cryptocurrency community. It serves as a warning to newbies not to "HODL" (hold on for dear life) their "crypto" on an exchange as the exchange owns the private keys, not the hodler, leaving their crypto vulnerable to theft. Instead, they should store their crypto in a private wallet, where only they hold their private keys. But what if your private key isn't needed to steal your crypto? What if all that is needed is your public key, which you broadcast to the world every time you use your crypto? The blockchains that cryptos are built on, email, the internet, traditional banking and, one could argue, privacy itself in the information age, rely on asymmetric public-key-private-key cryptography. Quantum computers leverage superposition and entanglement to trivialise deciphering a private key from a public key – posing one of the biggest threats to modern society.

1 But what is a Blockchain?

A blockchain, the backbone of a cryptocurrency, is a distributed immutable ledger – a record book of data maintained by everyone who uses it that is immune to tampering. This immutability – built on asymmetric key cryptography – is what gives blockchains their utility and widespread use cases, such as logging a car's mileage to prevent odometer fraud.

A blockchain, as the name suggests, is a chain of "blocks": bundles of transactions added to the blockchain that consist of 3 parts [2]:

1. Data (transaction information in the case of Bitcoin)
2. The hash of the block (a unique identifier for each block that changes if the data is tampered with)
3. The hash of the previous block

The third of these puts the "chain" in blockchain as each new block will be linked to every previous block, meaning that tampering with one block (resulting in a change in its hash) will become apparent in all subsequent blocks – forming a Merkle tree [2, 3, 4].

1.1 Consensus Algorithms

However, classical computers are capable of calculating hundreds of thousands of hashes per second and can thus tamper with a block and then recalculate the hashes of all subsequent blocks to cover their tracks. To mitigate this, blockchains use consensus algorithms to slow down the production of blocks, as well as to ensure all nodes in the network agree with the data in the blockchain.

Bitcoin uses "Proof of Work" (PoW) which requires block "miners" to guess a nonce (a pseudo-random binary number) which when combined with the transactions in that block, and the previous hash in a hash function, will yield the new hash for that block.

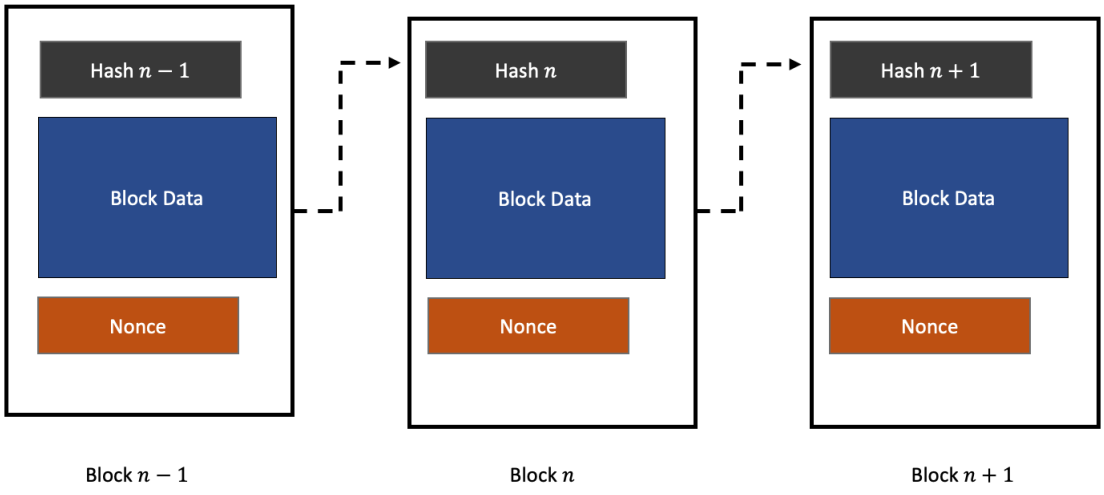


Figure 1: Schematic of a blockchain.

The hash algorithm used is SHA256, which is widely used on the internet, that gives a 256 bit hash (256 1s and 0s) [2]. This hash is determined by a difficulty adjustment system that scales with the computing power, or hash power, of the "miners" trying to "mine" the block, such that a new block is mined approximately every 10 minutes [2]. For example, the system might say that the next block has must start with n zeroes, where n rises with network hash power, and miners must find a nonce that when passed into the hash function, will yield this hash. Finding the nonce of a cryptographic hash function is difficult as they are "pre-image resistant", meaning a small change in the nonce gives a drastically different hash [5]. The only way to find the nonce is to try every possibility until you get the answer, thus the probability of guessing correctly is $1/2^n$ which is approximately one in a billion for $n = 30$. Once a block is verified, it is added to the blockchain and the first miner to obtain the correct nonce receives a block reward paid out in Bitcoin.

The computational power associated with finding nonces renders tampering a block too time consuming and uneconomical. Making the cost of attacking the network higher than the potential rewards of doing so is essential in the security of decentralised systems as the nodes' truthfulness cannot be relied on.

1.2 Digital Signatures

So we know that previous transactions have not been tampered with, but how do we know that those transactions are legitimate? While encryption scrambles data to prevent sensitive information from being intercepted, this is not an issue with cryptocurrencies as the data is just transaction information. What is more important is verifying that the person sending the transaction is actually in possession of those funds. This is the idea behind digital signature algorithms (DSAs) like Bitcoin's ECDSA [2]. The process is very similar to encryption, so the the threats to DSAs also apply to encryption. Say Alice wants to send Bob 0.1 Bitcoin. To prove it's her, she must use asymmetric key cryptography [6]: she "signs" her transaction with her wallet's private key, which is mathematically linked to her public key that she sends to Bob. Upon receiving the transaction, Bob verifies the transaction with Alice's public key to confirm the transaction was sent by Alice.

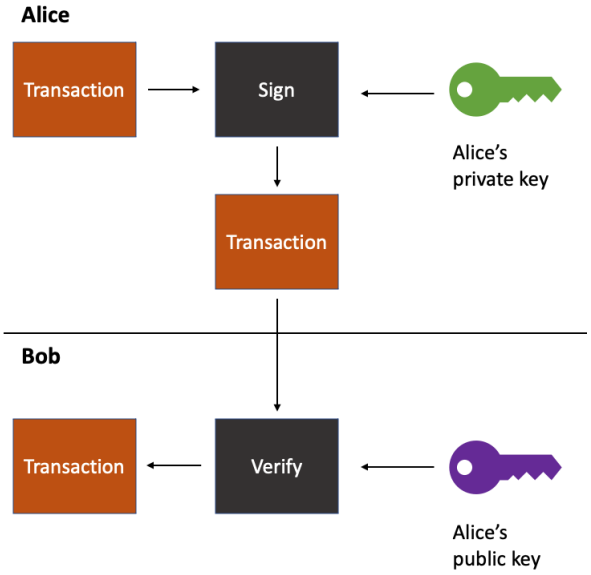


Figure 2: Pictorial representation of an asymmetric key DSA.

If the public key Bob receives does not verify the transaction, then Bob knows that it wasn't actually Alice that executed the transaction. This ensures that whoever is spending the cryptocurrency owns the private keys to the wallet holding it, preventing someone else spending Alice's hard-earned Bitcoin. Private keys are essentially proof of ownership of cryptocurrencies. Thankfully the prime factorisation required to find the private key from the public key takes far too long, unless you have a quantum computer...

2 How Quantum Computers Work

To appreciate how a quantum computer works, we must first appreciate how a classical computer works.

2.1 The Limits of Classical Computers

Classical computers are based on transistors – tiny switches can block and unblock electrical current to take two states: "on", corresponding to 1, and "off", corresponding to 0. These are called "bits". Transistors can be combined to form logic gates that perform very simple operations, which can then be combined to form meaningful modules, such as simple arithmetic. These are then be combined to perform complex operations. You can think of a classical computer as a bunch of primary school kids doing basic addition and multiplication. Gather enough of them and you can compute anything from black holes to Halo [7], with emphasis on "enough". Transistor sizes have been exponentially decreasing since the 1970s, becoming as small as a few nanometres to pack as many as possible in a computer.

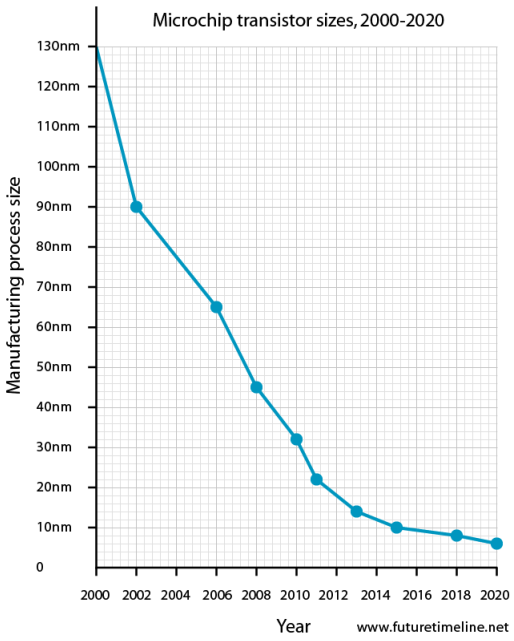


Figure 3: The exponential decay of transistor size from 2000 to 2020. Source: [8]

At these scales, quantum tunneling starts to take effect [9, 10] – electrons have a finite probability of traversing classically forbidden regions as a result the wave-like nature of matter on quantum scales (see Figure 4).

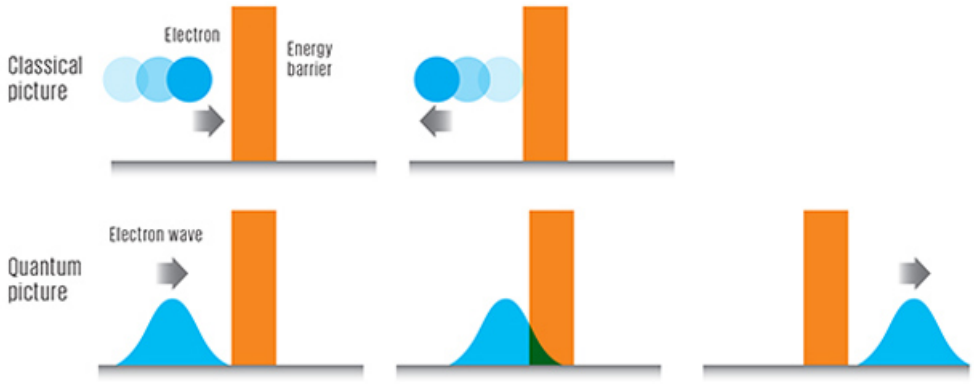


Figure 4: An electron particle reflecting off of a barrier in classical physics and an electron wave tunnelling through it in quantum physics. Source: [11]

Now the transistor is unable to "block" the electrons from passing to give a 0. But what if we can exploit an electron's quantum behaviour?

2.2 Bits to Qubits

A qubit is any two-level quantum system, like the spin of an electron in a magnetic field or the polarisation of a photon. Taking the spin of electrons, each qubit can have two states: up $|\uparrow\rangle$, corresponding to 1, and down $|\downarrow\rangle$, corresponding to 0. However, thanks to quantum superposition, a qubit doesn't have to be in either of these states – it can be a wavefunction consisting of any superposition of them, $|\psi\rangle$:

$$|\psi\rangle = \alpha\,|\uparrow\rangle + \beta\,|\downarrow\rangle$$

where $|\alpha|^2$ and $|\beta|^2$ are the probabilities of the electron being in an up state or a down state respectively. This is where the quantum power lies.

2 classical bits can be in one of 4 configurations at a time:

$$11$$
$$00$$
$$10$$
$$01$$

However, these still contain just 2 bits of information. All we need to know to determine which state the bits are in is the value of the first bit and the value of the second bit. 2 qubits also give us 4 configurations [12]:

$$\alpha\,|\uparrow\uparrow\rangle$$
$$\beta\,|\downarrow\downarrow\rangle$$
$$\gamma\,|\downarrow\uparrow + \uparrow\downarrow\rangle$$
$$\delta\,|\downarrow\uparrow - \uparrow\downarrow\rangle$$

but now, these contain 4 *bits of information*. To determine the state of this quantum two state system, we need to know what 4 numbers (α, β, γ and δ) are. In other words, the amount of information contained in n qubits is equivalent to 2^n classical bits. Moreover, while classical bits can only exist in one state at a time, qubits can exist all their allowed states at once. That said, when we come to measure the state of a qubit, its wavefunction will collapse to a single state within the

superposition with its associated probability [13]. This can be annoying. While classical gates take in input and give a definite output, a quantum gate takes in one superposition, rotates probabilities and spits out another superposition [7]. There is no guarantee that measuring this superposition will yield the output you desired.

2.3 Spooky Action at a Distance: Quantum Entanglement

Special relativity deems superluminal motion unphysical, so you can appreciate why Einstein called particles on opposites sides of the universe communicating with each other instantaneously "spooky" [14].

To understand entanglement, let's consider 2 electrons, labelled A and B respectively. Formally, the two electrons are entangled if the wavefunction cannot be factored into a part containing only the states of A and a part containing only the states of B.

The spin of an electron creates a small magnetic field and the electron can be made to "flip" from the down state to the up state by applying a magnetic field of frequency proportional to the energy difference between the states to it. Say we prepare A to be in a superposition of up and down, corresponding to right:

$$|\rightarrow_A\rangle = \frac{1}{\sqrt{2}}|\uparrow_A\rangle + \frac{1}{\sqrt{2}}|\downarrow_A\rangle$$

Now we bring B in its down state close to A and apply the frequency corresponding to the energy difference between its down and up states to try to flip it. However, this energy difference is altered by the magnetic field of A and since A is in both the up and down state, B both flips and doesn't flip, yielding an entangled Bell state – the simplest non-separable state of 2 electrons [15]:

$$|\psi\rangle = \frac{1}{\sqrt{2}}|\uparrow_A\downarrow_B\rangle + \frac{1}{\sqrt{2}}|\downarrow_A\uparrow_B\rangle$$

Here we have a $(\frac{1}{\sqrt{2}})^2 = 50\%$ chance of measuring either state. Suppose we only measured A and found it to be in the spin up state, now we know that the whole system is in the $|\uparrow_A\downarrow_B\rangle$ state, meaning that B must be in a down state. Therefore, measuring A has changed the probability of the outcome of measuring B – prior to measurement, we had no idea what states A and B were in, just that they were in opposite states. It doesn't matter how far apart they were, if they were entangled, it's as if A has communicated with B faster than the speed of light and told it to get down. So is special relativity wrong? No, the measurement outcome is still random, just the opposite random at A and B. So while "spooky", this doesn't facilitate transfer of information from one point to another faster than the speed of light as you can't pick what to send [16].

Entanglement is key in achieving quantum supremacy – the point at which a quantum computer can solve a problem unsolvable in polynomial time on a classical computer [17, 18] – as it drastically reduces the number of measurements needed in computation. There is no way you can write classical code where two bits have no value, but the opposite value [19]. It must be mentioned however, that entangled states are prone to quantum decoherence due to interaction with the environment changing their quantum states [20]. Therefore, they must be kept in a controlled environment.

3 Quantum Threats

Quantum computers are not faster than classical computers for everything, but there are 2 pretty important algorithms that have been proven to run *much* faster on quantum computers.

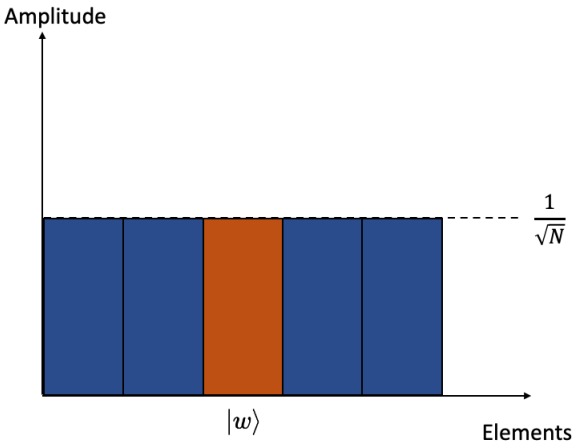
3.1 Finding a Needle in a Haystack: Grover's Algorithm

...or a nonce in a hash. Grover's algorithm provides a quadratic speedup on the best classical alternative – a linear search [21] – for searching an unstructured database. This means that instead of performing n checks in a database of n elements, it only has to check $\sqrt{n}$ elements. The algorithm works by maximising the amplitude of the the desired state, making it more likely to be measured, solving our quantum gate worries.

Consider searching a database of N elements looking for a specific state, $|w\rangle$. The algorithm consists of 4 steps [22, 23]:

1. A Hadamard gate initialises the quantum computer into an equal superposition of all elements [24, 25], meaning that they are all equally likely to be measured:

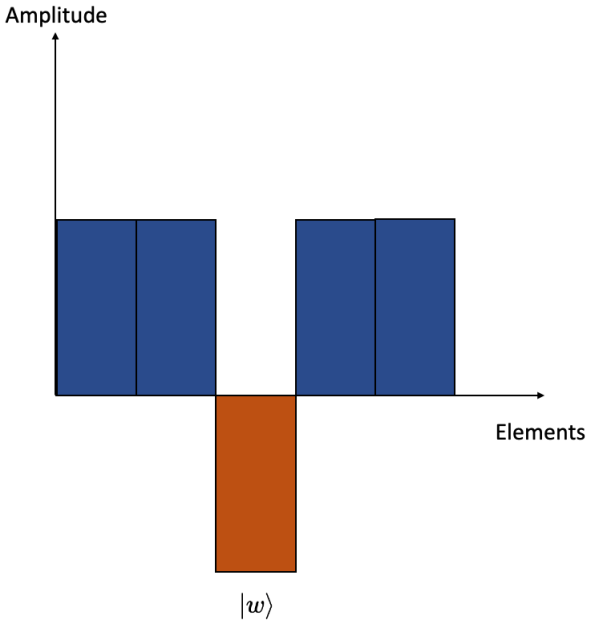
$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$



2. A unitary operator, U_ω, and an oracle function, $f(x)$:

$$U_\omega |x\rangle = (-1)^{f(x)} |x\rangle$$
$$f(x) = \begin{cases} 1 & x = w \\ 0 & x \neq w \end{cases}$$

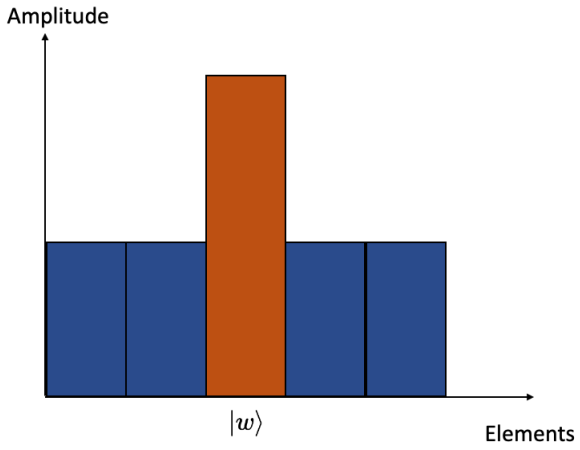
are used to "flip" the probability amplitude of $|w\rangle$ as shown.



3. A reflection,

$$U_s = 2|s\rangle\langle s| - 1,$$

where $\langle s|$ is the complex conjugate of $|s\rangle$, is then applied to "flip" $|w\rangle$ back to being positive while increasing its amplitude – making it more likely to be measured.



4. Repeat steps 2 and 3 until the expectation value of $|w\rangle$, $\langle w\rangle \approx 1$.

Graphically, we can see that repeating steps 2 and 3 brings the superposition closer and closer to being $|w\rangle$:

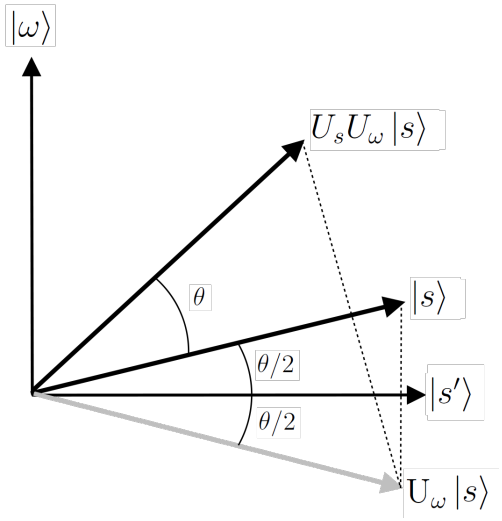


Figure 5: Graphical representation of the first iteration of Grover's algorithm. $|s'\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \omega} |x\rangle$ denotes the state "perpendicular" to $|w\rangle$, which is the superposition of all states excluding $|w\rangle$. We can see that repeated application of the algorithm will cause the $U_s U_\omega |s\rangle$ phasor to tend to $|w\rangle$. Source: [26]

If you haven't realised by now, this is a catastrophic problem for PoW, your email and anything else that uses SHA256. A quantum computer running Grover's algorithm will find a nonce several billion times faster than the fastest miners today [27]. After this quantum node gets bored of collecting all the mining rewards and leaves to leak your emails, the network will be crippled as the dramatic increase in hash power leaves the difficulty adjustment system believing the entire population is mining Bitcoin. Classical computers no longer stand a chance of mining new blocks.

3.2 You're Big? I'm Fast: Shor's Algorithm

So a quantum computer running Grover's algorithm would mean that your transaction won't get mined, but at least you still have your Bitcoin... or maybe you don't. Both encryption and DSAs rely on classical computers being terrible at factorising large numbers into their prime factors, but this is no problem for Peter Shor. A quantum computer running Shor's algorithm factors large numbers *exponentially* faster than a classical computer.

Skipping the boring number theory, the problem boils down to finding an even integer, p, such that

$$(g^{p/2}+1)(g^{p/2}-1) = m \cdot N$$

where g is a (probably) bad initial guess, N is the large number we're trying to factorise and m is some integer [28, 29]. This returns two better guesses, $g^{p/2} \pm 1$, that might share a common factor with N, which we can use to find factors of N using Euclid's algorithm [30]. Determining p is where classical computers show their age and quantum computers flex their muscles.

A quantum computer utilises superposition to calculate all possible answers simultaneously. The issue is that this yields a superposition and we can only measure one state at a time within that superposition. The trickery lies in ensuring that all the wrong answers destructively interfere with each other. This is non-trivial, but Peter's a clever guy. He realised that if we raise g to an arbitrary power, x, we will overshoot $m \cdot N$ by r. Moreover, if we multiply this by g^{np}, where n is an integer, we will still overshoot a different multiple of N by r:

$$g^x = m \cdot N + r$$
$$g^{x+np} = m_2 \cdot N + r$$

Why do we care? Imagine we have a superposition of the form $|x, +r\rangle$,

$$|1, +13\rangle + |2, +2\rangle + |3, +6\rangle + \cdots,$$

and we make a measurement of r which turns out to be $r = 6$. This will cause the wavefunction to collapse into as superposition of only states with $r = 6$ [13]:

$$|3, +6\rangle + |17, +6\rangle + |26, +6\rangle + \cdots$$

We now know that these states are all p apart (they repeat with a frequency of $f = 1/p$). Enter the quantum fourier transform (QFT) which when given a superposition containing one frequency, will output that frequency [31]:

$$|x\rangle + |x+p\rangle + |x+2p\rangle + \cdots \rightarrow QFT \rightarrow \left|\frac{1}{p}\right\rangle$$

Now anyone with your public key, which is everyone, can get your private keys and your Bitcoin [32]. Don't worry though, Bitcoin will be the least of your issues once all your private conversations become public. Thanks Peter!

4 Looking Ahead

There are still many practical difficulties holding quantum computing back. Shor's algorithm is estimated to require thousands of qubits, while today we have a few dozen [33]. Quantum computers also need to be maintained at no more than a few microkelvin to prevent qubits from having enough kinetic energy to spontaneously change states [34, 35]. While Google claimed its Sycamore chip demonstrated quantum supremacy in 2019 [36], it did so for a very specific, not so useful problem [37]. With only 53 qubits, Sycamore is years away from finding your private keys [1].

4.1 Quantum Key Distribution

In the meantime, the world is scrambling to develop quantum-resistant cryptography to keep civilisation from ending (if COVID doesn't do it first). The crypto world is no different, with a lot of hope going into quantum key distribution [38, 39, 32]. This relies on our good friend Alice sending photons to Bob in two different bases: rectilinear and diagonal polarisations and telling him what basis to measure each photon in. They will both know if an eavesdropper tried to listen in as their measurements will randomise the photon state if measured in the wrong basis. They also cannot get around this by copying their own set of the photons due to the no-cloning theorem [40]. Sounds too good to be true? That's because it is as of now. So far this has only been managed over a distance of 200 km [41], as even exposure to light can lead to decoherence and ruin things [20].

4.2 To HODL or not to HODL?

Quantum computers are still around a decade away from doing anything useful. Even then, they won't be commercially viable for another decade or so, leaving them in the hands of Silicon Valley and government agencies. Taking the example of the British after they cracked Enigma [42], the NSA is not going to waste revealing the fact that they can access every other nuclear nation's launch codes on your 0.1 Bitcoin, so you only need to worry about Silicon Valley. Large tech corporations have society's best interests at heart, right?

References

[1] Cointelegraph Japan. (2020). "How the crypto world is preparing for quantum computing, explained," [Online]. Available: https://cointelegraph.com/explained/how-the-crypto-world-is-preparing-for-quantum-computing-explained (visited on Jan. 7, 2021).

[2] N. Satoshi, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: https://www.bitcoinpaper.info/bitcoinpaper-html/ (visited on Dec. 5, 2020).

[3] R. C. Merkle, "Protocols for public key cryptosystems," Piscataway: The Institute of Electrical and Electronics Engineers, Inc. (IEEE), 1980, p. 122. [Online]. Available: https://search.proquest.com/docview/1687310642 (visited on Jan. 2, 2021).

[4] P. Garry. (2019). "Merkle trees and their use in Blockchain transaction validation," [Online]. Available: https://medium.com/@garry.passarella/merkle-trees-and-their-use-in-blockchain-transaction-validation-13eafdab6f82 (visited on Dec. 31, 2020).

[5] B. Preneel, "Preimage resistance," in, ser. Encyclopedia of Cryptography and Security. Boston, MA: Springer US, 2011, pp. 952–953, ISBN: 978-1-4419-5906-5. [Online]. Available: https://doi.org/10.1007/978-1-4419-5906-5_604 (visited on Jan. 6, 2021).

[6] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976. DOI: 10.1109/TIT.1976.1055638.

[7] Kurzgesagt – In a Nutshell, *Quantum Computers Explained – Limits of Human Technology*, 2015. [Online]. Available: https://www.youtube.com/watch?v=JhHMJCUmq28\&t=274s\&ab_channel=Kurzgesagt\%E2\%80\%93InaNutshell (visited on Dec. 5, 2020).

[8] W. J. Fox. (2011). "Moore's law," [Online]. Available: https://www.futuretimeline.net/subject/computers-internet.htm#ref8 (visited on Jan. 5, 2021).

[9] S. Ed, *Quantum effects at 7/5nm and beyond*, 2018. [Online]. Available: https://semiengineering.com/quantum-effects-at-7-5nm/ (visited on Dec. 31, 2020).

[10] J. R. Powell, "The quantum limit to Moore's law," *Proceedings of the IEEE*, vol. 96, no. 8, pp. 1247–1248, 2008. [Online]. Available: https://ieeexplore.ieee.org/document/4567410 (visited on Jan. 6, 2021).

[11] A. Seabaugh, *The tunneling transistor*, 2013. [Online]. Available: https://mensdocta.wordpress.com/2013/12/11/the-tunneling-transistor/ (visited on Jan. 1, 2021).

[12] Veritasium, *How Does a Quantum Computer Work?* 2013. [Online]. Available: https://www.youtube.com/watch?v=g_IaVepNDT4&list=PLrE-PbIs3CoP_uuTpXo_uz_jVPglNGTFN&index=26&ab_channel=Veritasium (visited on Jan. 1, 2021).

[13] J. Pritchard, *Second Year Quantum Mechanics Notes*. Imperial College London, 2020.

[14] A. Einstein and M. Born, *Born-Einstein Letters, 1916-1955: Friendship, Politics and Physics in Uncertain Times*. Palgrave Macmillan US, 2005, ISBN: 9781403944962.

[15] D. Sych and G. Leuchs, "A complete basis of generalized Bell states," *New Journal of Physics*, vol. 11, no. 1, p. 013 006, 2009. [Online]. Available: https://doi.org/10.1088/1367-2630/11/1/013006 (visited on Jan. 5, 2021).

[16] A. Peres and D. R. Terno, "Quantum information and relativity theory," 2002. [Online]. Available: https://arxiv.org/abs/quant-ph/0212023v2 (visited on Jan. 5, 2021).

[17] A. W. Harrow and A. Montanaro, "Quantum computational supremacy," *Nature (London)*, vol. 549, no. 7671, pp. 203–209, 2017. [Online]. Available: https://www.nature.com/articles/nature23458#article-info (visited on Jan. 1, 2021).

[18] J. Preskill, "Quantum computing and the entanglement frontier," 2012. [Online]. Available: https://arxiv.org/abs/1203.5813v3 (visited on Jan. 1, 2021).

[19] The University of New South Wales, *Quantum Computing Concepts – Entanglement*, 2016. [Online]. Available: https://www.youtube.com/watch?v=EjdIMBOWCWo&list=PLrE-PbIs3CoP_uuTpXo_uz_jVPglNGTFN&index=30&ab_channel=UNSW (visited on Jan. 1, 2021).

[20] K. McCormick, "Decoherence Is a Problem for Quantum Computing, But ...," *Scientific American*, [Online]. Available: https://blogs.scientificamerican.com/observations/decoherence-is-a-problem-for-quantum-computing-but/ (visited on Jan. 6, 2021).

[21] D. E. Knuth, *The Art of Computer Programming, Volume 3: Sorting and Searching*, Second edition. Upper Saddle River, NJ: Addison-Wesley, 1998, ISBN: 9780201896855. [Online]. Available: http://proquest.tech.safaribooksonline.de/9780321635792 (visited on Jan. 4, 2021).

[22] L. K. Grover, "A fast quantum mechanical algorithm for database search," 1996. [Online]. Available: https://arxiv.org/abs/quant-ph/9605043v3 (visited on Jan. 2, 2021).

[23] The Jupyter Book Community. (2020). "Grover's Algorithm," [Online]. Available: https://community.qiskit.org/textbook/ch-algorithms/grover.html (visited on Jan. 6, 2021).

[24] D. Voorhoede. (2020). "Hadamard gate," [Online]. Available: https://www.quantum-inspire.com/kbase/hadamard/ (visited on Jan. 6, 2021).

[25] The Jupyter Book Community. (2020). "Single Qubit Gates," [Online]. Available: https://community.qiskit.org/textbook/ch-states/single-qubit-gates.html (visited on Jan. 6, 2021).

[26] Danski14. (2012). "Picture showing the geometric interpretation of the first iteration of Grover's algorithm," [Online]. Available: https://commons.wikimedia.org/w/index.php?curid=18415805 (visited on Jan. 5, 2021).

[27] S. Naihin, *Goodbye Bitcoin... Hello Quantum*, 2019. [Online]. Available: https://blog.usejournal.com/goodbye-bitcoin-hello-quantum-9749ed451872 (visited on Jan. 6, 2021).

[28] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," 1995. [Online]. Available: https://arxiv.org/abs/quant-ph/9508027v2 (visited on Jan. 4, 2021).

[29] M. Amico, Z. H. Saleem, and M. Kumph, "An experimental study of Shor's factoring algorithm on IBM Q," 2019. [Online]. Available: https://arxiv.org/abs/1903.00768v3 (visited on Jan. 3, 2021).

[30] D. H. Lehmer, "Euclid's algorithm for large numbers," *The American Mathematical Monthly*, vol. 45, no. 4, pp. 227–233, 1938, doi: 10.1080/00029890.1938.11990797. [Online]. Available: https://doi.org/10.1080/00029890.1938.11990797 (visited on Jan. 3, 2021).

[31] The Jupyter Book Community. (2020). "Quantum Fourier Transform," [Online]. Available: https://community.qiskit.org/textbook/ch-algorithms/quantum-fourier-transform.html (visited on Jan. 6, 2021).

[32] A. K. Fedorov, E. O. Kiktenko, and A. I. Lvovsky, "Quantum computers put blockchain security at risk," *Nature*, vol. 563, no. 7732, pp. 465–467, 2018. [Online]. Available: https://www.nature.com/articles/d41586-018-07449-z (visited on Jan. 4, 2021).

[33] M. Brooks, "Beyond quantum supremacy: The hunt for useful quantum computers," *Nature*, vol. 574, no. 7776, pp. 19–21, 2019. [Online]. Available: https://www.nature.com/articles/d41586-019-02936-3 (visited on Jan. 6, 2021).

[34] J. Wall, *Ice Ice Baby — Why Quantum Computers have to be cold*, 2018. [Online]. Available: https://medium.com/the-quantum-authority/ice-ice-baby-why-quantum-computers-have-to-be-cold-3a7f777d9728 (visited on Jan. 6, 2021).

[35] C. Baraniuk, *The coldest computers in the world*, 2020. [Online]. Available: https://www.bbc.co.uk/news/business-53413931 (visited on Jan. 6, 2021).

[36] F. Arute *et al.*, "Supplementary information for "quantum supremacy using a programmable superconducting processor"," 2019. [Online]. Available: https://arxiv.org/abs/1910.11333v2 (visited on Jan. 3, 2021).

[37] E. Gibney, "Hello quantum world! Google publishes landmark quantum supremacy claim," *Nature*, vol. 574, no. 7779, pp. 461–462, 2019. [Online]. Available: https://www.nature.com/articles/d41586-019-03213-z (visited on Jan. 3, 2021).

[38] E. O. Kiktenko *et al.*, "Quantum-secured blockchain," *Quantum Science and Technology*, vol. 3, no. 3, p. 035 004, 2018. [Online]. Available: https://arxiv.org/abs/1705.09258 (visited on Dec. 5, 2020).

[39] T. M. Fernández-Caramès and P. Fraga-Lamas, "Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks," *IEEE Access*, vol. 8, pp. 21 091–21 116, 2020. (visited on Dec. 5, 2020).

[40] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature (London)*, vol. 299, no. 5886, pp. 802–803, 1982. [Online]. Available: https://www.nature.com/articles/299802a0 (visited on Jan. 3, 2021).

[41] Y.-L. Tang *et al.*, "Measurement-device-independent quantum key distribution over 200 km," *Physical Review Letters*, vol. 113, no. 19, p. 190 501, 2014. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.113.190501 (visited on Jan. 6, 2021).

[42] F. W. Winterbotham, *The Ultra Secret*, First. HarperCollins, 1974.

Will Quantum Computing Spell the End of the Blockchain?

Motivation: the internet, email, traditional banking, blockchains and, one could argue, privacy itself in the information age rely on cryptography. Quantum computers exploit superposition and entanglement to trivialise modern encryption-- posing one of the biggest threats to modern society in the last century-- making them a very topical subject.
Take away message: The reader should come to understand the basics of how a quantum computer works and appreciate that if encryption stagnates between now and quantum supremacy, encryption will be trivialised by quantum computers. In this case, blockchains won't be the only things to slip into irrelevance-- anything that relies on storing sensitive information digitally (the internet, email, traditional banking, medical records etc) will too. For this reason, it is highly unlikely that a solution won't be born out of necessity from at least one of the multitude of stakeholders.

What is a Blockchain? ~ 500 words. [Satoshi N. Bitcoin: A Peer-to-Peer Electronic Cash System]

The reader should come to understand the meaning of a distributed, immutable ledger:

- Explain the concept of a "block"
- (Classical) computers can still recalculate the hashes of all subsequent blocks to hide this tampering: discussion of consensus algorithms (specifically proof of work) to counter this
- Use cases: cryptocurrencies (the focus use case in this article), medical records, voting etc

How Encryption Works and how Blockchains use it ~ 400 words. [W. Diffie, M. Hellman. *New directions in cryptography]*

Symmetric encryption and its faults-- motivation for asymmetric encryption:

- Explain public and private keys ("Not your keys; not your Bitcoin")
- Bitcoin uses Elliptic curve digital signature algorithm (ECDSA) [relies on the factorisation of large prime numbers being too computationally "expensive"]
- Perhaps, if there is enough space, describe how cryptocurrencies rely on P != NP and whether quantum computers will prove P = NP (Probably outside of the article's scope however)

How a Quantum Computer Works ~ 800 words. [*Quantum Computers Explained – Limits of Human Technology*-- Kurzgesagt-- In a Nutshell, Youtube]

Qubits instead of bits (connection to quantum physics)

- Brief overview of classical bits, transistors, logic gates and modules
    - Very brief discussion of the limit of the smallest transistor possible, before electron tunnelling becomes significant
- A qubit as a two level quantum system, such as the polarisation of a single photon, to serve as a proxy for "0" and "1". Superposition allows qubits to exist in any proportion of "0" and "1" prior to measurement and wavefunction collapse (revisited later)
- Entanglement-- measuring one entangled qubit, determines the state of the other qubit without the need for direct measurement

Quantum Threats to Encryption ~ 600 words. [Bouguera A. *How Will Quantum Supremacy Affect Blockchain?]*

Quantum gates and wavefunction collapse to classical bits

- Utilise entanglement to perform "brute force" tasks in the square root of the time required by classical computers

Find private key from the public key (overcome asymmetric encryption)

- Shor's algorithm and prime factorisation
- By extension, threats to blockchains (using Bitcoin as example: loss of decentralisation and ruining the difficulty adjustment system for mining blocks)

Looking ahead ~ 600 words. [Gao Y, *et al.* A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain]

- Discuss quantum supremacy and approximate timeframe this will be achieved by
- Discuss how a cryptographic defense against quantum computers must be developed by this point just by virtue of how much is at stake.
- Discuss crypto projects already developing "quantum blockchains" (Cardano, Ethereum 2.0 etc)

Plan Feedback

CID: 01502658

Topic: Quantum computing is clearly matched to the quantum requirement for the article, so this is a good choice of topic. The focus on a particular aspect is good also, although the author needs to make sure the encryption/blockchain parts do not squeeze out the quantum material.

Structure: The article plan is thorough and clearly carefully thought out. While it is ambitious and covers a lot of material, the author has already suggested sections which could be dropped if space becomes tight. The words counts are indeed possibly a bit optimistic (meaning they are likely to increase given the material listed) so some reduction will probably be needed. The logical structure proposed is good.

Resources: These are a reasonable mix of formal and informal sources, showing a good awareness of the available material. Note, although not needed for the plan, a more formal referencing style will be needed for the article itself.

Response to Feedback

As suggested, I reduced the blockchain and encryption sections to approximately 760 words, instead of the proposed 900 words, to allow for more discussion of quantum material. I also decided against discussing the P vs NP problem for the same reason. The relative length of the sections evolved during writing, straying away from the plan at times, in order to retain the key messages of the article without compromising the flow of the narrative. I have read more papers and articles while writing the article to get a more rigorous understanding of the material before distilling it. As suggested, I have used a formal referencing style for the article (BibLateX IEEE).