elenjical
SOLUTIONS

Analysing the effect of quantum computing on Bitcoin

Sias Repsold

1 Introduction

Bitcoin is a digital currency that utilises cryptography to ensure transactions are secured (Zamyatin, et al., 2018). In other words, a cryptocurrency. The most recent price increase of Bitcoin has attracted the attention of the public to what significant role cryptocurrencies like Bitcoin will play in the near future. There are various advantageous features of Bitcoin that led to its further increase in popularity over conventional currency systems such as being decentralised and having increased security (Tessler & Byrnes, 2017). Bitcoin operates using a peer-to-peer distributed network where every member sustains a full list of all historic transactions in a public ledger. The list of transactions is grouped in blocks within the ledger also known as the blockchain (Zamyatin, et al., 2018). These blocks are linked together via hashes which allows the sharing of information between participants (Fernández-Caramés & Fraga-Lamas, 2020).

As with the rise of major cryptocurrencies like Bitcoin, quantum computing has also gained increasing popularity. By the middle of the 20th century, there was a rapid advance in classical computing, which led to the powerful computational machines we know and use today. In the 1980s, scientists started to consider a new method of approaching numerical problems. To solve difficult calculations scientists started to consider the quantum mechanical properties of matter (Orús, et al., 2019). In 1982, Richard Feynman introduced the concept of quantum computing and the theory behind quantum computing has been greatly researched since its introduction (Mavroeidis, et al., 2018). According to Mavroeidis, et al. (2018), present-day asymmetric cryptography is in danger through the continuous advancements in quantum computing and Tessler & Byrnes (2017) states that it is not uncommon to hear that scalability within quantum computing is within reach. There are continuous advancements in quantum computing like that of Peter Shor’s polynomial-time quantum algorithm Shor (1999), that can break the elliptic curve digital signature algorithm (ECDSA) (Zamyatin, et al., 2018). This raises a serious question of how big of a threat is quantum computing toward Bitcoin as ECDSA is implemented within Bitcoin to ensure that the cryptocurrency is only spent by their lawful owners (Tessler & Byrnes, 2017). This article aims to discuss and analyse this question to shine some light on the future of Bitcoin with the advancements of quantum computing.

2 Background

This section aims to provide background information regarding quantum computing and Bitcoin, discussing core concepts and principles relevant to this paper.

2.1 Quantum computing

All computers rely on the ability to store and manipulate data. In classical computing systems information is stored in binary states, either 0 or 1. Quantum computing leverages three quantum mechanical properties called, superposition, entanglement, and interference to present and manipulate data to provide results. To manipulate information the quantum computing system relies on qubits or quantum bits (Zamyatin, et al., 2018).

2.2 Qubits

De Wolf (2001) states that qubits fulfil the role as a unit of information, similar to that of bits in classical computing systems. Bits can either be 0 or 1, whereas a qubit is in a superposition of 0 and 1. A qubit in its more formal definition is a two-dimensional complex vector. The base states of 0 and 1 are denoted by $|0\rangle$ and $|1\rangle$ and the associated qubit is in a superposition of the two base states. It can then be concluded that every qubit is a linear combination of the two base states,

$$|\emptyset\rangle = \beta|0\rangle + \alpha|1\rangle \qquad (1)$$

where β denotes the amplitude of being in state $|0\rangle$ and α represents the amplitude of being in state $|1\rangle$ (De Wolf, 2001). This entails that while a computation is being processed on a quantum computer, the state of the quantum computer will always be a linear combination of the two base states with each state having a certain probability to be obtained. If the system is measured to extract information the superposition will collapse to one of the two base states (Zamyatin, et al., 2018).

2.3 Shor's quantum algorithm

In 1994, Shor (1999) developed polynomial-time algorithms to help compute factoring integers and discrete logarithms on a quantum computing system. Shor's algorithm developed for integer factoring is known to be exponentially faster than current classical algorithms. In simpler terms, Shor's algorithm can be deduced to finding the period of the following function,

$$f(y) = n^{y} \, mod \, K \qquad (2)$$

where K is the number that needs to be factored and n is a random integer. The algorithm operates by creating a superposition of the base states. Each base state is created by concatenating the value of $f(y)$ with y. After the qubits are measured which stored the value of $f(y)$, it will leave behind a value x as a result of the superposition collapsing. The qubits which stored y will still be in superposition with different $y's$ where $f(y) = x$. To compute the period, it is required for the remaining algorithm to compute the difference between any of the states that are in superposition. The implementation of Shor's algorithm will greatly weaken certain public-key cryptography systems such as the well-known RSA cryptography system (Zamyatin, et al., 2018). Proos & Zalka (2003) adapted the algorithm to help solve the elliptic curve discrete logarithm problem (ECDLP) in fewer steps which in turn offers a polynomial-time algorithm that threatens the security of ECDSA.

2.4 Bitcoin

Every Bitcoin transaction is stored in the blockchain (a public ledger). Transactions are grouped into blocks and every transaction in the block are assumed to have happened simultaneously. For each transaction, a time ordering is placed by adding the transactions in a chain. Every block in the chain contains a pointer in the form of a hash that references the previous block. Miners are responsible for adding blocks to the chain. Miners group transactions that still need to be processed into a block and then adds the block to the chain through proof-of-work (PoW) (Aggarwal, et al., 2017). Users in the blockchain interact with one another securely through the means of public-key or asymmetric cryptography (Fernández-Caramés & Fraga-Lamas, 2020). In simple terms, for person A to send Bitcoin to person B. Person B must first create a private-public key pair. The public key is then hashed to generate an address. The address generated is what person B presents to person A as the required address to send the Bitcoin to. For person A to send the Bitcoin, person A must also point to the transactions in the blockchain where Bitcoin was originally sent to destinations/addresses that he owns. The total sum of Bitcoin received by these addresses must be at least the total amount person A wants to send to person B. Person A must prove that he is the owner of these addresses by providing the public key associated with each address. Person A must then use his private key associated with the specific address to sign the corresponding message that states he is giving his Bitcoin to person B (Aggarwal, et al., 2017). ECDSA which ensures that Bitcoin is spent by its lawful owners is based on asymmetric/public-key cryptography (Tessler & Byrnes, 2017). The next section will elaborate more on ECDSA.

2.5 Elliptical curve digital signature algorithm (ECDSA)

ECDSA is the implementation of the Digital Signature Standard or DSS. DSS is based on elliptic curve cryptography. The goal behind the signature is to provide permissions to third parties that will determine the integrity and legitimacy of the message that is signed. In Bitcoin transactions, the transactions are signed digitally using ECDSA. This secures the transfer of Bitcoin from one person to another. ECC is based on public-key cryptography that utilizes the properties of elliptic curves over finite fields. The elliptic curve cryptography system can be explained as follow. In this system, a curve is chosen as C. A public point T is selected on C. To generate a key pair a random number x is selected as the private key. Using elliptic curve point multiplication ANSI (2005) to multiply T with itself x times. This in turn will provide the public key y. The public key in itself is also a point on C. The key assumption with ECC, is that it relies on the difficulty to solve ECDLP (Zamyatin, et al., 2018).

The following section will discuss the impact of quantum computing on the security of Bitcoin.

3 Impact of quantum computing on Bitcoin security

Bitcoin's digital transaction signature is created using ECDSA. The level of security this system provides depends on ECDLP. As stated, Shor's quantum algorithm combined with a powerful enough quantum computer can solve this problem. In essence, with a powerful enough quantum computing system the private key of an associated public key can efficiently be computed, which in turn makes the scheme insecure (Aggarwal, et al., 2017). The consequences include the following.

3.1 The reusing of addresses

When a Bitcoin transaction occurs from an address the public key is revealed. This will result in the address no longer being safe in the presence of a strong enough quantum computer. The associated address should then never be used again. Even though it is already suggested as best practice to use a fresh address for each transaction, it is not always followed. This entails when an address' public key has been revealed the address is no longer secure (Aggarwal, et al., 2017).

3.2 Transactions that are not processed

There is a risk involved in the scenario where a transaction has been broadcasted to the network but has not been placed into the blockchain. In the case where the secret key can be obtained from the public key that was broadcasted before the transaction can be placed in the blockchain, the infiltrator can then use the derived secret key to broadcast a different transaction from the original address to his/her address. If the infiltrator can then ensure that the different transaction is placed first on the blockchain, he/she can steal the remaining Bitcoin in the original address (Aggarwal, et al., 2017).

4 Present-day capabilities of quantum computing systems

This section will look at the current development in quantum computing and how far away we are from achieving quantum computing that can execute algorithms of relevance.

To execute quantum algorithms which will have practical implications a quantum computer with thousands of qubits and a very low error rate will be required (Olejnik, et al., 2020). It is estimated that in the next 20 years there will be powerful enough quantum computers to break all public key schemas currently used (Chen, et al., 2016). In 2019 Google stated they have reached quantum supremacy with a quantum computer with 54 qubits. The claim included that the quantum computer achieved results in hundreds of seconds whereas it would have taken a non-quantum computer thousands of years to compute. The solved task, unfortunately, had no practical impact but it did serve as a proof of concept. To perform algorithms with significant practical impact there is a desire to build quantum computers with a smaller error rate and with more qubits which is not possible in the next 10 years (Olejnik, et al., 2020)

5 Conclusion

With the increasing popularity and real-world implementations of cryptocurrencies like Bitcoin, it is always best practice to question the security and future sustainability as companies start to implement Bitcoin as part of their business to allow customers to make payments. At the time of writing this, Bitcoin remains one of the safest and most secure ways of concluding transactions. With the rise of Bitcoin so continues the development and research into quantum computing. Quantum algorithms like that of Shor's algorithm implemented with a powerful enough quantum computer has the potential to disrupt most public-key schemas used today and from a theoretical point of view Bitcoin as well. With that said most expectations is that quantum computing will only have a real-world impact in the next 20 years. This provides enough time to further develop cryptography to even be secure from quantum attacks. In essence, quantum computing is not a threat for Bitcoin as of the present, but further development is required to make Bitcoin secure from a quantum computing standpoint.

6 Bibliography

Aggarwal, D. et al., 2017. Quantum attacks on Bitcoin, and how to protect against them. *arXiv preprint arXiv:1710.10377.*

ANSI, X., 2005. Public key cryptography for the financial services industry: The Elliptic Curve Digital Signature Algorithm (ECDSA). *American National Standards Institute.*

Chen, L. et al., 2016. Report on Post-Quantum Cryptography. *US Department of Commerce, National Institute of Standards and Technology,* Volume 12.

De Wolf, R., 2001. *Quantum Computing and Communication Complexity.* s.l.:Inst. for Logic, Language and Computation.

Fernández-Caramés, T. & Fraga-Lamas, P., 2020. Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access,* Volume 8, pp. 21091-21116.

Mavroeidis, V., Vishi, K., Zych, M. D. & Jøsang, A., 2018. The Impact of Quantum Computing on Present Cryptography. *International Journal of Advanced Computer Science and Applications,* 9(3).

Olejnik, L., Riemann, R. & Zedrick, T., 2020. Quantum Computing and Cryptography. *Tech Dispatch,* Issue 2.

Orús, R., Mugel, S. & Lizaso, E., 2019. Quantum computing for finance: Overview and prospects. *Reviews in Physics,* Volume 4, p. 100028.

Proos, J. & Zalka, C., 2003. Shor's discrete logarithm quantum algorithm for elliptic curves. *QIC,* 3(4), pp. 317-344.

Shor, P., 1999. Shor, P.W., 1999. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review,* 41(2), pp. 303-332.

Tessler, L. & Byrnes, T., 2017. *Bitcoin and quantum computing,* s.l.: arXiv preprint arXiv.

Zamyatin, A. et al., 2018. Committing to quantum resistance: a slow defence for Bitcoin against a fast quantum computing attack. *Royal Society Open Science,* 5(6).