INFO3616—Principles of Security and Security Engineering

Assignment 2, Group 15

SID: 310322316, SID: 470011746

Introduction

In this report we look at four research papers (please see References section for full list) which explore the topic of blockchain security. In the first section of our report we will discuss the context of the problem, including the importance of blockchain, its relevance to various industries and the cryptographic principles underlying its security. In the second part we will discuss the broader problem and challenges including the impact quantum computing advances could have on blockchain security and the vulnerability of existing cryptographic methods to quantum computers. In the third part, we will discuss the various methodologies proposed to counteract these vulnerabilities and futureproof the security of blockchain technologies. In the fourth part, we will discuss future challenges in the development of such methods to maintain blockchain security and possible improvements that could be made. In the fifth part, we will give a critical analysis and thoughts on the proposed methodologies presented in each paper.

Context

Blockchain is an increasingly important technology for maintaining an immutable digital public record or ledger, “which is shared among multiple entities that do not necessarily trust each other” (Fernandez-Carames and Fraga-Lamas, 2020). It was firstly designed by ‘Satoshi Nakamoto’ in the form of Bitcoin (still one of the most important applications of blockchain technology) as a peer-to-peer electronic cash system which can protect clients from leakage of personal privacy and security threats during online transactions (Gao et al., 2018). Blockchain has applications in many industries, from finance, manufacturing and healthcare (Fedorov, Kiktenko and Lvovsky, 2018) to smart health, measuring systems, logistics, e-voting or smart factories (Fernandez-Carames and Fraga-Lamas, 2020), with an estimated market size of US$150 billion (Fedorov, Kiktenko and Lvovsky, 2018). It is estimated that by 2025, blockchain-related technologies will store 10% of global GDP(Kiktenko et al., 2018). As a billion-dollar technology with the potential to impact so many industries, the security of blockchain is of utmost importance.

The two most important cryptographic principles employed to secure blockchain are:

- Cryptographic hash functions: One-way trapdoor functions, such as large prime factorisation, used to calculate the hash of a block in order to authenticate user identity by generating digital signatures, and to validate the history of transactions by linking blocks in the chain (Fedorov, Kiktenko and Lvovsky, 2018). Each block contains a hash of the data and the hash value of the previous block, linking it to that block. If an attacker were to attempt to modify a block in the chain, this would mean the hash of the next block will not match, which prevents tampering.

- Digital signatures: Generated using public key cryptography (like RSA) or large integer factorization (Kiktenko et al., 2018). The public key cryptography is an asymmetric cryptographic protocol used to authenticate transactions and secure wallets, which are private key containers that store files and simple data (Fernandez-Carames and Fraga-Lamas, 2020).

Some of the security benefits (Fernandez-Carames and Fraga-Lamas, 2020) of these cryptographic measures inherent to blockchain are:

- Decentralization: Data from a blockchain node is still available through the other nodes even if the original node is attacked or shut down.
- Data integrity: Using a highly redundant database to ensure the integrity of information.
- Data privacy : Using multiple private keys for access control.
- Data immutability: Using cryptography for data verification to ensure that it cannot be tampered with. Once a node is added to the blockchain, its data can't be modified.

Broader Problem and Challenges

As the security of blockchain currently relies on hash functions and public key cryptography, this makes it particularly vulnerable to advances in quantum computing. For example, an attacker with a quantum computer could attack a blockchain that relies on the factorization of integers as a hash function by using Shor's algorithm to forge a signature, impersonate another user and "appropriate their digital assets" (Fedorov, Kiktenko and Lvovsky, 2018). Having a QC would also allow a user to censor transactions and monopolise the addition of blocks. In bitcoin for example, this is how coins are mined, so a QC would give a user a computational advantage in the mining of bitcoins. It would allow an attacker to "sabotage transactions, prevent their own from being recorded or double spend" (Fedorov, Kiktenko and Lvovsky, 2018).

Quantum computers also threaten the security of many popular public key algorithms, "including RSA (Rivest, Shamir, Adleman), ECDSA (Elliptic Curve Digital Signature Algorithm), ECDH (Elliptic Curve Diffie-Hellman) or DSA (Digital Signature Algorithm), which can be broken in polynomial-time with Shor's algorithm on a sufficiently powerful quantum computer." (Fernandez-Carames and Fraga-Lamas, 2020) An attacker with a quantum computer could also use Grover's algorithm "to accelerate brute force attacks by a quadratic factor" and "to detect hash collisions, which can be used to replace blocks of a blockchain while preserving its integrity." (Fernandez-Carames and Fraga-Lamas, 2020) Grover's algorithm could also be used in the so-called 51% attack "to accelerate mining in blockchains like Bitcoin… which would allow for recreating entire blockchains fast, thus undermining their integrity." (Fernandez-Carames and Fraga-Lamas, 2020)

Methodologies

With the security of such an important technology at stake, coming up with ways to mitigate these vulnerabilities is extremely important. The papers reviewed in this report propose several different kinds of solutions.

Yu-Long Gao and his team first define the Post-quantum blockchain (PQB) - the combination of blockchain technology and post-quantum cryptography which can resist known classic and quantum algorithm attacks. The signature scheme should be linkable and traceable. Then they propose a lattice-based delegation signature scheme so that the key can be generated with a random value. There are four advantages of using such a scheme. It will: (1) Improve the security of the private key (2) Make it nearly impossible for other people to forge a valid signature (3) Protect the privacy of users and (4) Provide many transaction keys.

Then, a preimage sampling algorithm is used to sign messages. They create a double-signature which uses both first and last signatures so that the correlation between message and signature can be reduced. What's more, the new signature scheme's size is shorter than others which means computational complexity will be reduced and efficiency improved.

E O Kiktenko et al. (2018) think post-quantum digital signature schemes can be robust against QC attack. However, their robustness against attacks that use quantum computers to control the network's hash rate mining is not proven. They describe a blockchain platform which combines a broadcast protocol, proposed by Shostak, Lamport and Pease, using the original BFT state-machine replication without digital signature and quantum key distribution (QKD), which is used to provide identity verification instead of digital signature.

They consider a blockchain protocol with two layers and *n* nodes. The first layer is a QKD network with a pair of communication channels, which theoretically allows the establishment of a secure private key for each pair of nodes. The second (classical) layer is used to transmit messages, which are created by the private key in the first layer, with authentication tags based on the theoretically secure Toeplitz hash. The broadcast protocol is used to create blocks in a decentralized fashion to eliminate the possibility of 'fork', the situation that different miners create multiple blocks of different versions at the same time, enabling the 51% attack. Since the broadcast protocol is data-intensive, the quantum channels are only used to generate private keys so that it would not cause further problems due to such a two layer structure. This block chain protocol can ensure the transparency and integrity of transactions and protect them from QC attack (Kiktenko et al., 2018).

Fedorov, Kiktenko and Lvovsky (2018) also propose quantum-safe encryption to "replace classical digital signatures and to encrypt all peer-to-peer communications in the blockchain network." By using quantum cryptography, "quantum communications are inherently authenticated — no user can impersonate another… quantum states cannot be copied or measured without being altered. Any eavesdropper will be immediately uncovered." They also propose the possibility of a quantum internet, arguing that "using quantum technology for communicating as well as for the computational processing of blockchain data would further enhance security and enable blockchains to become faster and more efficient.” However, they concede that such a development is several decades away. They also propose blind quantum computation as an interim step. In this method, “a user with a conventional computer could run an algorithm on a remote quantum computer without sharing the input data or algorithm.” They also propose increased adaptivity of blockchain security in response to greater security pressures, arguing that “platforms must be flexible and capable of changing cryptographic algorithms on the fly” in response to various security threats.

Fernandez-Carames and Fraga-Lamas (2020) suggest that post-quantum cryptosystems are needed which provide five main features in order to be efficient: small key sizes, small signature and hash length, fast execution, low computational complexity and low energy consumption. They describe several different kinds of post-quantum cryptosystems which are currently being developed. Among public-key post-quantum cryptosystems, there are:

- Code-based cryptosystems, which are based on the theory of error correcting codes.
- Multivariate-based schemes which rely on the complexity of solving systems of multivariate equations that have been demonstrated to be NP-hard or NP-complete.
- Lattice-based cryptosystems which are based on lattices, sets of points in n-dimensional space with a periodic structure. These schemes rely on the computational hardness of lattice problems.
- Supersingular elliptic curve isogeny cryptosystems which are based on the isogeny protocol for ordinary elliptic curves and enhanced to withstand quantum attack.
- Hybrid cryptosystems which merge pre-quantum and post-quantum methods in order to protect exchanged data both from quantum attacks and from attacks against post-quantum schemes.

Fernandez-Carames and Fraga-Lamas (2020) also describe several post-quantum signing algorithms, that involve many of the above techniques and also hash-based signature schemes, which depend on the security of the underlying hash function instead of on the hardness of a mathematical problem. The authors compare the performance of state-of-the-art examples of each of these kinds of algorithms in their paper in terms of execution time on several different kinds of processors.

Future Challenges and Possible Improvements

Yu-Long Gao et al. (2018) conducted four analyses of the correctness, security, one-more unforgeability and efficiency for their proposed cryptocurrency scheme. Both correctness and one-more unforgeability are proved exactly, such that “even in the worst-case of the lattice SIS problem, it is still able to resist quantum attack”. It cannot be broken as long as the lattice SIS problem is not cracked. Such a scheme could be further developed by optimising efficiency and achieving practical results. Since the size of the public key is still longer than other schemes, this can also be improved.

The broadcast protocols used in the blockchain platform of Kiktenko et al. (2018) have one limitation - they are relatively tolerant of dishonest or faulty nodes. Such a blockchain has a great tolerance for certain nodes or communication channels that cannot operate normally during the implementation process, which needs to be improved. It follows Byzantine Fault Tolerance (BFT) which may cause low efficiency but has no influences on correctness of the transaction.

One more problem of such a blockchain platform is that the database is still fragile while the data is being stored. One possible attack situation is where a QC forges the database by working offline and changes past transaction records. Then Grover search is performed for variants of other transactions within the same block to replicate the hash, making the fake version look legitimate. After that, it can invade all network nodes and replace the legitimate database with its fake version (Kiktenko et al., 2018). Compared to classical search algorithms, the Grover algorithm provides a quadratic speedup, but this can be mitigated by increasing the block hash length to the square of its safe non-quantum value.

Fedorov, Kiktenko and Lvovsky (2018) suggest that the factors limiting the adoption of quantum cryptography are complexity, cost and accessibility to consumers. They also suggest that there is a physical issue relating to photon losses in optical fibres, which limits the range of modern quantum-key distribution systems to a few tens of kilometres. They propose that the solution “is to develop a quantum repeater, which uses quantum teleportation and quantum optical memory to distribute entangled states between the communicating parties.” They concede that while research is progressing, it is still a long way from delivering a practical device. As an interim improvement, they suggest that one-way functions should be tightened, saying “some alternative encryption functions have been proposed that should be equally difficult to reverse using conventional or quantum computers.” They concede that these are not completely secure and will probably be deciphered in the long term but could be run on existing hardware to buy time.

A key finding for Fernandez-Carames and Fraga-Lamas (2020) from their literature review is that at the moment, “there are no post-quantum blockchain algorithms that provide, at the same time, small key size, short signature/hash sizes, fast execution, low computational complexity and low energy consumption”. Of the possible methods they described which may be used to secure blockchain, they point out the following problems and needed improvements:

- Code-based cryptosystems use large keys that require a lot of computational resources. They argue that more research is needed on key compression techniques and coding techniques.
- Lattice-based cryptosystems are currently some of the most promising candidates but also need to be improved in terms of key size.
- Multivariate-based public-key cryptosystems need improved decryption speed and reduced key size.
- Hybrid schemes seem promising, but they need hardware that is able to handle two advanced security mechanisms and large payloads simultaneously.

- Super-singular elliptic-curve isogeny cryptosystems need to be optimized to decrease signature size.
- Hash-based digital signature cryptosystems have poor performance in general, but some researchers have suggested new faster algorithms that may be practical for blockchain.

Critical Analysis and Conclusion

The papers surveyed in this report indicate that there are many promising avenues of research at various stages of development currently being pursued. For example, while the methods offered by Fedorov, Kiktenko and Lvovsky (2018) seem speculative, many of the methods discussed by Fernandez-Carames and Fraga-Lamas (2020) are currently being researched and are derived from academic papers which they surveyed in their literature review. The scheme proposed by Yu-long Gao et al. (2018) still needs to be practically tested, but they lay a good foundation for a Post-quantum blockchain which can be further researched and improved upon. The blockchain platform proposed by Kiktenko et al. (2018) has been proved feasible experimentally. Although not very efficient, it still provides several unique innovations such as using the broadcast protocol as the way to add new blocks and using the QKD channel to obtain private keys but still using classic channels to send data.

As Fernandez-Carames and Fraga-Lamas (2020) point out though, quantum computing is itself a very active area of research and those trying to keep up with the security challenges posed to technologies like blockchain may find themselves trying to stay ahead of a fast-moving target. In our opinion, this makes theoretical guarantees much more important than practical benchmarks, as hardware and software can change but the physical universe operates within certain parameters. Understanding the fundamental capabilities and limitations of quantum computers is the most important issue for those attempting to secure current technologies against their advancement.

References

Fedorov, A.K., Kiktenko, E.O., & Lvovsky, A.I. (2018). Quantum computers put blockchain security at risk. Nature, 563(7732), 465-467

Fernandez-Carames, T.M., & Fraga-Lamas, P. (2020). Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks. IEEE Access, 8, 21091-21116

Gao, Y.L., Chen, X.B., Chen, Y.L., Sun, Y., Niu, X.X., & Yang, Y.X. (2018). A Secure Cryptocurrency Scheme Based on Post-Quantum Blockchain. *IEEE Access*, 6, 27205-27213

Kiktenko, E.O., Pozhar, N.O., Anufriev, M.N, Trushechkin, A.S., Yunusov, R.R., Kurochkin, Y.V., Lvovsky, A.I., & Fedorov, A.K. (2018). Quantum-secured blockchain. *Quantum Science and Technology*, 3, 035004

NOTES

Not relevant to the problem of QCs impacting blockchain security

Furthermore, the efficiency and anonymity benefits can also be shortcomings. In terms of efficiency, since there is no single node in the blockchain that can be trusted and trust is obtained through computational work, interacting with the blockchain requires substantial computing power. Take the Bitcoin system as an example. Theoretically, only 6.6 Bitcoin transactions can be processed per second at present. In terms of anonymity, Bitcoin's developers believe that anonymity is an important part of Bitcoin transactions. However, the guarantee of anonymity allows Bitcoin to be used for illegal transactions, which poses problems for law enforcement agencies. If the miner decides not to process the sending and receiving of a transaction between addresses, it proves that the transaction is subject to review by the miner. If the transaction is anonymous, the miner cannot decide which transactions to prioritize and they cannot be reviewed.

It would then become possible to run fully quantum blockchains. These would bypass some computationally intensive steps of the current verification and consensus processes, and thus be more efficient and more secure.

which they point out are critical factors especially for resource-constrained embedded devices such as those used for Internet of Things applications

Fernandez-Carames and Fraga-Lamas also point out that "it is not straightforward to choose a blockchain post-quantum cryptosystem. Future developers will have to take such a decision based on their blockchain node hardware, on the available resources (i.e., memory, speed), on the required blockchain node performance and on the necessary security level." They also suggest several important features which could be developed and added to post-quantum blockchains in the future, including aggregate signatures, ring signatures, Identity-Based Encryption, secret sharing, homomorphic encryption, Zero-Knowledge Proofs, and Secure Multi-Party Computation (SMPC).