kpn

National Cyber Security Centre
Ministry of Justice and Security

POLITIE

EUROPOL EC3 European Cybercrime Centre

Deloitte.

IDQ

accenture
High performance. Delivered

Check Point
SOFTWARE TECHNOLOGIES LTD.

pwc

KASPERSKY

TU Delft

ANALYZEDATA

TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

de volksbank

TNO

Piratenpartij

HITB

Universiteit Leiden
Governance and Global Affairs

QuSoft
Research Center for Quantum Software

Blockchain in a Post Quantum World

Kelly Richdale, Bruno Huttner, IDQuantique

Blockchain is a technology which provides immutable proof of time, identity and assets in a distributed digital ledger. These records may represent digital assets, such as ownership of a digital currency; information based on a smart contract; or even the geolocation of your car or shipping container.

Distributed ledger technologies are characterised by two key technical aspects. Firstly, they provide digital trust, which is not dependent on a central verification point or a central authority – the trust is distributed and validated by independent nodes on a network. Secondly the digital trust relationship between the nodes, the assets and the asset stakeholders is based on cryptographic algorithms.

Impact of a Quantum Computer

The advent of a universal quantum computer - which performs selected complicated computations in exponentially less steps than a classical computer- will fundamentally change the cryptographic paradigms on which the digital trust is based. Quantum algorithms – such as Shor's algorithm and Grover's algorithm - attack the foundations of today's cryptography. Such quantum algorithms already exist and are just waiting for a universal quantum computer powerful enough to run them, commonly estimated to be within the next 10 or so years.

The digital trust underpinning blockchain uses two fundamental cryptographic algorithms:

a) **cryptographic hashes** ensure the integrity of the blockchain. The integrity of each block of information is guaranteed by making a hash of the transactions of the previous block, which itself includes a hash of the all the previous transactions - hence the chain effect. Once a block is validated, it is integrated into the chain and shared by all the nodes (servers) on the network. The fact that is publicly distributed means that it is considered trustworthy, since a change in the block structure or deviation from the main blockchain would be noticeable in the distributed network. The hashing algorithm is often based on a cryptographic primitive (a primitive is the basic cryptographic building block) called SHA-256, an algorithm which is commonly held to be "quantum-safe"[1].

(1) The SHA-256 algorithm, as well as the AES symmetric key encryption algorithm, will be impacted by the quantum computer. Indeed, "Grover's algorithm", which runs on a quantum computer which will reduce the strength of a 256 bit key to 128 bits. However, this still holds sufficient security to be considered "quantum safe", as generally 80 bits of security is considered sufficient today. In addition, the keys can just be increased in size to provide longer term security.

b) **public-private key pairs (asymmetric algorithms)**, which ensure the authenticity of the transactions. In all blockchain systemsusers sign their transactions with their private key. Others can then verify the identity of the transaction owner using their published public key. People on the blockchain are therefore identified by their private key. In fact, in many blockchains such as bitcoin, which have no centrally controlled mechanism, they are their private key. The purpose of this private-public key pair is to cryptographically answer the question "am I really the person who has the right to spend money from this wallet" or in another context "am I really the entity who has the right to make changes to this smart contract?". Most current blockchain private-public key pairs are based on the cryptographic algorithm Elliptic Curve (ECC) which is known to be broken by a quantum computer[2]. This means that any bad actor, who has access to someone's public key and to a quantum computer, will be able to derive the corresponding private key. He will then be able to impersonate this person. Therefore in a post quantum world, this authentication mechanism will break down.

So, what is the practical impact of a quantum computer on the blockchain?

Firstly, as explained above, the private-public key pairs will be broken, allowing hackers to identify private keys from the public keys, and to then forge the identity of the private key owner, taking control of the information or asset linked to that private key. This would be a catastrophic event for them - for example, bitcoins and other blockchain assets could be transferred en masse to the quantum hacker's own wallet.

Secondly, quantum computers will also speed up the hashing process in proof-of-work-based schemes, creating an unequal playing field for those with access to a quantum computer. The potential vulnerability in this case is that the quantum hackers would be able to generate and and validate new blocks faster than the honest non-quantum nodes. This would allow them to selectively choose the blocks to be validated, effectively taking control of the blockchain. The asymmetry between a few rogue nodes with very large computing power and a large number of smaller honest nodes is already a concern with existing technology. Given the fact that Grover's quantum algorithm only allows a quadratic speed up in finding a solution to the hash, the advantage of the quantum computer is only quantitative. The advantage of a general purpose quantum computer with respect to the specialized classical hardware currently used in dedicated computing farms is not obvious. Therefore, the threat of the quantum computer in this context is not considered as major and is rejected in academic research[3]. Hashing is still considered to be quantum safe.

On a separate note though, it is hoped that by the time a quantum computer emerges blockchains based on proof-of-work will be extinct. The mathematically brilliant, but environmentally disastrous, invention of Satoshi Nakamoto requires solving hard problems (finding the preimage of a hash function, which hashes into a specific hash, with a given number of leading zeros) in order to validate a transaction, rewarding the miner with some bitcoins. This promotes energy consumption (mining) for the sake of itself. If bitcoin mining was taxed to reflect the true cost of the environmental externalities, the value of bitcoin would plummet. New blockchain schemes (proof of stake, proof of time) are more adapted to a sustainable green environment.

Quantum Solutions to Post-Quantum Problems

There are a number of areas where quantum physics and new mathematical algorithms can provide solutions in order to quantum-proof blockchain.

- **Quantum resistant algorithms (QRA):** The public-private key pairs should be upgraded to new cryptographic primitives which are resistant to Shor's algorithm. These are termed quantum resistant algorithms, or post-quantum cryptography. Such algorithms are under review for standardisation by NIST[4] . In new (future) blockchains use of such QRA will be easier to implement at the outset. However, QRAs will not be ready & tested for the next 5-7 years. In the meantime existing cryptographic schemes can be used, but architected to foresee an algorithmic upgrade in the future, thus providing cryptographic agility. This will be particularly complex in permission-less blockchains, where a hard fork of the blockchain (incorporating the new QRAs) would have to be created & accepted by all the nodes. All future transactions should thereafter be based on quantum resistant private public key pairs. With regards to previous (non quantum resistant) transactions – although the integrity of previous blocks in the chain would be protected by quantum-safe hashing[5], the transaction validation of previous blocks would be vulnerable as anybody with a quantum computer could hack the ECC private key and claim the assets linked to it. In cases

(2) Shor's algorithm is a quantum algorithm for integer factorisation which will render vulnerable today's widely used public key cryptography - RSA, Elliptic Curve Cryptography and Diffie Hellman. Shor's algorithm will reduce these algorithms from exponential to polynomial time so that increasing the size of the key will not increase security.

(3) https://www.evolutionq.com/assets/mosca_quantum-proofing-the-blockchain_blockchain-research-institute.pdf

(4) NIST Post Quantum Cryptography Standardisation - https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

(5) The integrity of previous non-quantum safe blocks in the chain would be protected since they are hashed by quantum resistant algorithms & changes would be noted since the blocks are stored in distributed nodes, all with a copy of the previous blocks.

where the blockchain is used for proof of ownership (eg. bitcoin, ownership of intellectual property rights or land registers) all the assets linked to that (now compromised) private key would have to be transferred to a new quantum resistant private key. This can be easily carried out by performing a self-transaction, transferring all possibly compromised assets to the new quantum resistant private key. However, a serious constraint is that blockchain owners and users should become aware of the threat early enough, and act before an effective quantum computer is available.

- **Quantum Random Number Generation:**
  The trust engendered in blockchain depends on strong cryptography. And all of the cryptography used in blockchains (generation of public- private key pairs or hashing) itself depends on very strong random number generation.

  Weaknesses in the randomness could be exploited by an attacker to obtain information on the crypto assets generated and to breach the system. One concrete example of a vulnerability linked to weak random number generation would be a public key collision, where two bitcoin users are given the same public-private key pairs, thus creating doubt about the ownership of a bitcoin wallet[6].

  At the quantum level, everything is random, and Quantum random Number Generators (QRNGs) harness the power of quantum mechanics to create true randomness. Moreover the high availability of randomness from a QRNG ensures instant inexhaustible entropy to avoid delays in transaction processing.

- **Quantum-secured back-up of private keys:**
  As previously mentioned, in the world of most blockchains, you are your private key. Therefore protection of the private key – to ensure it is not lost, compromised or duplicated – is paramount to retaining control of the information or virtual currency assets linked to it.

  The highest level of information theoretic security in protecting data at rest comes from a combination of two technologies: Shamir's Secret Sharing Protocol (SSSP) and Quantum Key Distribution (QKD). SSSP allows to shard the token (private key) into

  multiple parts & store these separately in different databases. Reconstruction of the secret key requires M out of N consensus[7]. This system offers secure backup with no duplication of the asset and protection against a single point of failure, such as a hacked or malevolent node.

  QKD provides an information theoretic security for sharing the N different elements of the secret to different databases, and then re-grouping them. QKD works by sending photons, which are "quantum particles" of light, across an optical link. The Heisenberg Uncertainty Principle stipulates that in quantum physics observation causes perturbation. This is used to verify the security of the distributed keys. Combining QKD with encryption techniques like One Time Pad allows a provably secure exchange of the N secrets of the private keys, secured against future attacks by quantum computers.

Future implications: combining quantum computing & blockchain

Possibly the most striking point about blockchain is that it facilitates trust establishment not just between anonymised persons, but also between machines themselves – for example in IoT networks, between connected cars, or in the future – with the advent of Artificial Intelligence speeded up with quantum computing – between autonomous robots. Blockchain payment systems will allow machines to transact with each other directly, without interference or even control by humans[8], and they will allow machines a level of financial autonomy never previously experienced. Connected cars will be able not just to pay for their parking space & petrol. They could order new cars to augment their own self driving taxi fleet when capacity runs low. They could even start transacting in a meaningful financial way between each other for other purposes.
Trading systems in ancient civilisations allowed the exchange of goods and knowledge, which hugely accelerated the development of human societies. What if blockchain has the same effect on machines? Combine self-learning algorithms from AI with financial autonomy, and a new society of connected autonomous machines does not seem so impossible or outlandish.

At what point will connected cars start selling data about their passengers, rather than vice versa? If robots are taking the financial decisions about where to spend money & how & for what (fill up on petrol, or where to drive) at what point does this translate (together with their autonomous, self learning processes) into actually having a level of actional autonomy. At what point does actionable autonomy translate into political will & human rights?

(6) The key space should be large enough to avoid such collisions if a true RNG is used.

(7) Shamir M-out-of-N Secret Sharing Protocol (SSSP) offers an Information Theoretically Secure (IT-secure) solution for splitting a secret between N entities, in such a way that: if M out of N (M<N) of these entities collaborate, they can recover the secret; if less then M entities collaborate, they get no information on the secret. For more information see "Quantum Security for token Custody" (provide link)

(8) Other forms of currency do not lend themselves to this – cash needs a physical transfer and credit cards/ bank transactions need to be linked to an individual (Know Your Customer KYC). Blockchain will allow machines to establish financial transaction mechanisms (eg. Bitcoin), legal infrastructures (eg. Smart contracts) and other trust mechanisms which are fundamental to a developing society.