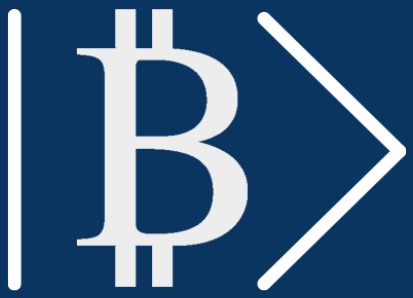
INSIGHTS

QUANTUM + BLOCKCHAIN
THREATS AND OPPORTUNITIES

Quantonation is an Early Stage Venture Fund dedicated to Deep Physics start-ups with a focus on the emerging and disruptive fields of Quantum Sensing, Communications and Computing as well as other new computing paradigms. Quantonation invests worldwide out of Paris and works closely with the start-ups it invests in, leveraging its partners expertise and network to their benefit.

"INSIGHTS" are short research reports by the team at Quantonation adressing challenges and opportunities in the fields of interest.

QUANTONATION



Blockchain, or more generally distributed ledger technologies, have the potential to disrupts whole segments of the economy: banking, investment, insurance, logistics, energy...

Scalability, altought the most commonly discussed blockchain challenge, is not the only one preventing its adoption by a wider audience.
The deployment of a durable trusted blockchain induces strong requirements in term of user privacy and data confidentiality.
With the rapidly increasing chances that a large quantum computer could happen within 10 years, future blockchains will have to be "Quantum-safe" to survive the peril endangering their core architectures.

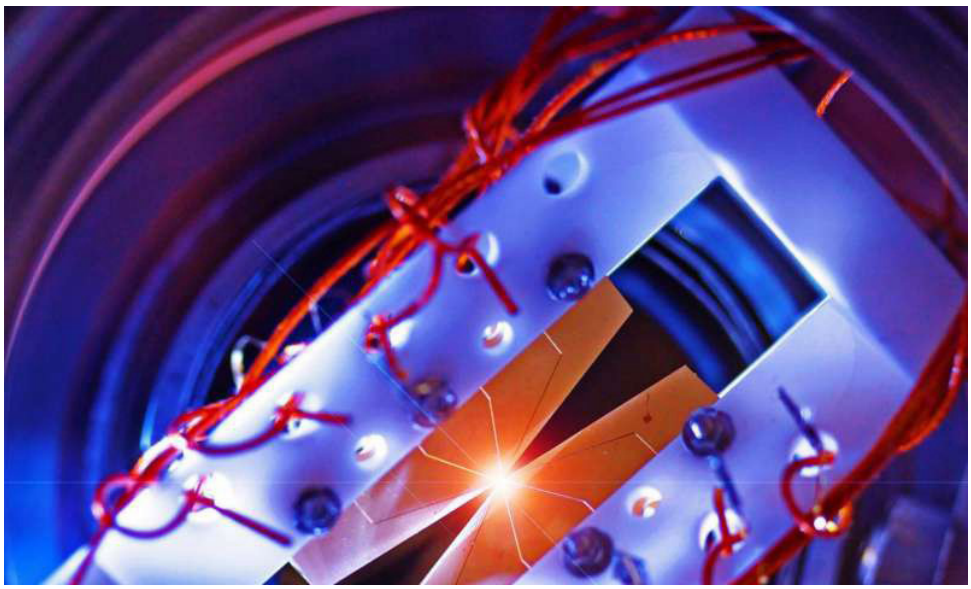
Quantum Technologies should not only be reduced to a threat for their inner mechanisms can also be used to strengthen blockchain security against any kind of attacker. This report will explore in detail some of the architectures that are already being considered for implementation following an introduction about the fundamental concepts of Quantum Computing and blockchain security.

Several startups are active in these fields, their progress should be closely monitored.

DR. CHRISTOPHE JURCZAK
Managing Partner

Figure 1

An ion trap with four segmented blade electrodes used to trap a linear chain of atomic ions to implement quantum gates for computation. Each ion is addressed optically for individual control and readout using the high optical access of the trap.
Source: Joint Quantum Institute
Credit: Emily Edwards.



PART I
QUANTUM COMPUTING AS A THREAT

A blockchain is a decentralized growing list of records called blocks, each containing a list of transactions, whose security is ensured by cryptographic algorithms. A new block is added upon completion and validation of a challenge that reaches consensus between all participants.
In the two most common consensus mechanisms, the challenge either relies on racing to be the first to solve a moderately hard computational problem (Proof-of-Work, PoW) or on being randomly selected as verifier depending on how active one participates in the blockchain, which is usually quantified by the amount of tokens possessed (Proof-of-Stake, PoS). In PoW, the successful miner will be rewarded by newly created tokens while in PoS, the selected minter will receive a fraction of the transaction fees.
There are pros and cons to each mechanism. PoW requires a lot of computational power, correlated with a very high and unsustainable consumption of electricity, but provides a high security. PoS is less resource-intensive, offers faster transactions, but is also (as of today) less secure.
Two mathematical disciplines play a fundamental role in cryptocurrencies, game theory and cryptography. Game theory studies logical decisions made by the participants in a blockchain network whereas cryptography ensures the security and provenance of each transaction.

Many blockchains, notably the Ethereum and Bitcoin blockchains, are built around two categories of cryptographic primitives : a hash function for the consensus mechanism and a digital signature based on Public-Key to securely manipulate blocks and transactions.
A hash function maps an input value of arbitrary size called preimage to a finite-size output called hash. Given the preimage, it is very easy to compute the corresponding hash but finding a correct preimage for a given hash require a computational power greatly exceeding our current capabilities.
In a consensus based on hash functions—notably PoW—the authenticity of all past blocks is verified thanks to the hash contained in the current block. Replace a valid block by a falsified one would require the ability to find a correct preimage that outputs this specific hash value. Solving this search problem is difficult for our computers, and that's what constitutes the safety net, but less so when considering future advances in computational capabilities, Quantum Computing among others.
A digital signature allows to verify the provenance of a message, check that it has not been altered during transit and ensure that its sender cannot deny having sent it—respectively authentication, integrity and non-repudiation. Not only it is widely used in distributed communications, but it also provides the necessary security to safely manipulate components added to the

blockchain.
During block validation, security is also ensured by the use of a Byzantine Agreement Protocol that enables the network of distributed participants, some of them being potentially dishonests, to agree about the updated state of the blockchain in a way that the final decision will reflect the decision of honest participants.
How safe are consensus and signatures for blockchains in a world where Quantum Computing is a reality ? For most of them, not so safe.
Grover's algorithm designed by Lov Grover in 1996 weakens search-based consensus and Shor's algorithm designed by Peter Shor in 1994 deals a crippling blow to the security of Public-Key algorithms which lie at the core of digital signatures.
Grover's algorithm would provide a quadratic speed-up in solving search problems with a Quantum Computer, considerably accelerating the discovery of an adequate preimage for a given hash. It has even been proven optimal in the sense that any future quantum algorithm trying to solve this preimage problem will not be able to solve it more quickly.
Breaking the digital signature scheme after a transaction could lead to disastrous consequences in blockchain security, especially when considering cryptocurrencies. First, the overall anonymity would no longer be ensured, allowing for identity theft and forcing transactions without the spender knowing it. Secondly, it would be possible to spend the same cryptocurrency twice—double-spending—without being noticed.
Several precautions have already been suggested to counter these vulnerabilities. For example, a fresh address should imperatively be used for every transaction, which is already recommended by several blockchains included Bitcoin but not often performed in practice. The time available to run a Quantum attack must also be considered ; in the Bitcoin design, the security is weak from the time a transaction is broadcasted until it is validated and followed by new blocks.
Similarly to classical algorithms, a quantum algorithm sequentially applies elementary operations—quantum gates—to modify the states (qubits) before measuring them and retrieving the desired result. In practice, each of these operations slightly deviates from the ideal model, resulting in an erroneous qubit that doesn't perfectly correspond to the target. The overall amount of errors introduced by applying all the gates to the qubits must be limited and controlled, which is why we need to correct these errors as much as possible.
Classical Error Correction techniques consist of adding extra information—redundancy—that enables recovery of the target information despite errors occurring during the transmission. In Quantum Error Correction (QEC), several « erroneous » physical qubits simultaneously hold the information that should be contained in one « perfect » logical qubit. It is still hard to evaluate the overhead for practical quantum computer and that depends on many factors but, just to give an order of magnitude, Fault-tolerant Quantum Computers using QEC could require as much as 1,000 to 100,000 physical qubits to emulate one single logical qubit.
In "Quantum attacks on Bitcoin, and how to protect against them", the authors provide a detailed analysis on the feasibility of attacking 1) a Bitcoin PoW based on a double SHA-256 hash

TWO KEY QUANTUM ALGORITHMS

Grover's algorithm—a variant for hash functions.
Let us consider a hash function f, a target hash y and a suitable preimage x amongst n possible inputs.
Grover's algorithm finds with high probability the value x such that f(x) = y in O(√n) evaluations of f where a classical computer would necessitate O(n) evaluations instead.
For a hash of length k bits, Grover's algorithm would provide a speed-up of factor 2k/2.

Shor's algorithm for integer factorization.
Given an integer N = p.q, the algorithm finds its prime factors p and q in polynomial time.
Solving the discrete logarithm problem with this algorithm roughly consists in a variant of solving the integer factorization where we look at pairs of integers instead of a single one.

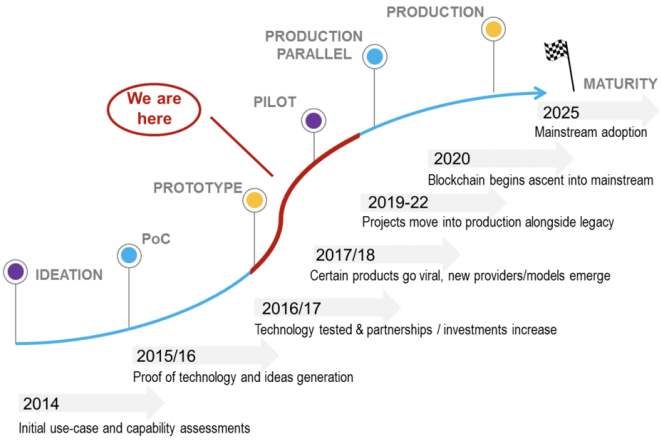


Figure 2

Development timeline of Blockchain technology. Source: Crédit Suisse, 2018

function with Grover's algorithm and 2) a Bitcoin digital signature secured by a 256-bit Elliptic Curve algorithm (ECDSA) with Shor's. Both attacks use 2300 to 2400 logical qubits and are limited by their requirements in term of the number of quantum gates that are quite slow to perform with a quantum computer based on superconducting qubits. When finding a preimage associated to a hash with Grover, this low speed negates the quantum speedup and results in a hashing power lower than what is and will be achieved with specialized ASIC hardware. But unlike the Bitcoin PoW that offers an acceptable resistance to quantum attacks, a Bitcoin digital signature can be cracked with Shor's algorithm in less than 30 minutes with this kind of machine.

The authors estimate that a Quantum Computer powerful enough to break Bitcoin's signature protocol in less than 10 minutes — Bitcoin's block time length — may be available as soon as 2027. If so, a quantum attacker could recover the secret key corresponding to a given public key and use it to insert forged transactions in the current block, successfully stealing bitcoins from the owner.

These estimations hold in the context of our current technological capabilities but could change drastically depending on future progress in Quantum hardware and algorithms design, e.g. with more efficient Quantum Error Correction codes, or with new approaches.

Of interest, instead of waiting for a Quantum Computer large enough to implement algorithms that require perfect qubits, the community has been focusing its efforts lately on algorithms that would run on « imperfect » devices, without error correction, and still achieve a benefit, even if modest. These are the Quantum computers that are currently being built, so-called Noisy Intermediate-Scale Quantum (NISQ) computers, with qubit counts expected to be in the 100–500 range within 2023.

For example, a variant of Shor's algorithm, the Variational Quantum Factoring (VQF) algorithm, combines classical pre-processing with the Quantum Approximate Optimization Algorithm (QAOA) to decompose in prime factors a given integer with a NISQ computer, making the Quantum threat toward blockchains much more real in a near future.

Quantum Computing implementations are still at an early stage and current architectures do not provide a quantum advantage compared to fast ASIC or GPU mining-dedicated hardware, but the emergence of Quantum Processors should not be taken lightly by the Blockchain community.

Blockchain and Quantum Computing are emerging technologies. The current architectures of Bitcoin and Ethereum are not optimal by far for mainstream adoption and now is a good point to start thinking about future "quantum-safe" blockchains and cryptocurrencies, with new signature schemes and consensus mechanisms.

PART II
QUANTUM TECHNOLOGIES TO THE RESCUE

A new type of blockchain architecture where the consensus is based on a Byzantine agreement protocol has been recently presented by Russian researchers led by Pr. E. O. Kiktenko.
The consensus relies on pairwise authentication of each communication channel provided via Quantum Key Distribution. Two communication layers are used, one optical that establishes secret keys through QKD and one classical, authenticated with a Toeplitz hashing scheme, that is used to exchange public informations.

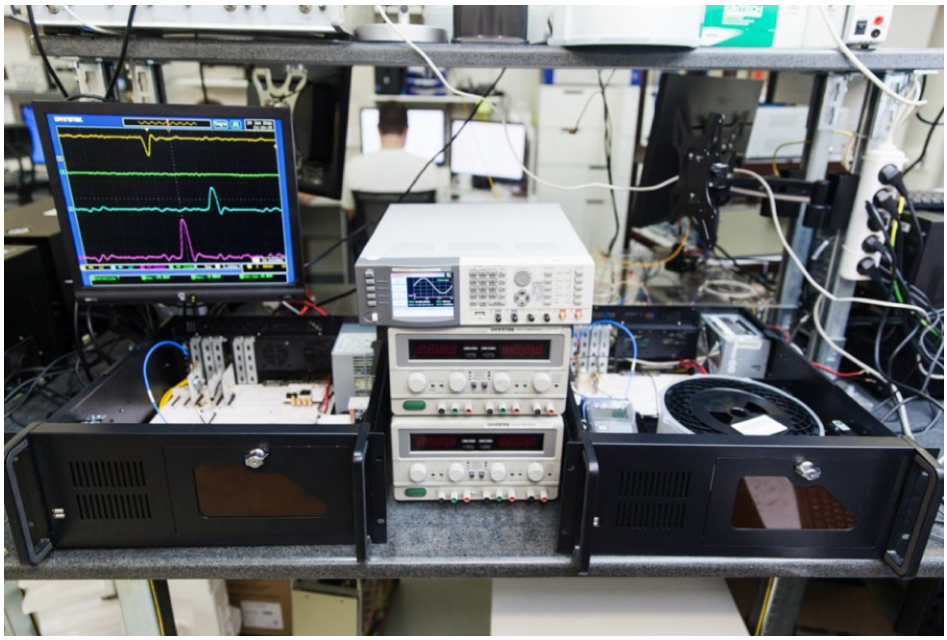


Figure 3

QKD-secured blockchain from an experiment conducted by Pr. E.O. Kiktenko et al.
Source : International Business Times, 2018.

After its creation, a new transaction is sent via authenticated channels to all the other nodes. Each node compares this new data with their own local database for verification and emits an opinion on the validity of the transaction. All the unconfirmed transactions are then aggregated into a new block.
At a pre-determined time frequency—e.g. 10 minutes—the Byzantine agreement protocol is applied to each unconfirmed transaction by the whole network, defining a consensus on the correctness of each transaction. Each node forms a block out of all admissible transactions sorted by time stamps and adds it to its local database. Not only this collective procedure avoid double-spending but it also prevent forks—situations in which several versions of the same block are simultaneously created by different users.
The authors have tested this new quantum-secured architecture on an urban-fiber QKD network constituted of four nodes, including a malicious one. The QKD key consumption required for performing 10 transactions per minute, which is less than 7 bit/s from their experiment, is easily ensured by current QKD devices.
They were even able to simulate and successfully prevent an intrusion attempt by considering a block construction from a pool of four unauthorized transactions, including one false transaction produced by the malicious node. This node is recognized and eliminated after applying the broadcast protocol.
In real life, security is never perfect and this proposal is not exempt of limitations. An ill-intended participant provided with a Quantum Computer could attempt to forge a false database offline by modifying a past transaction record. By running Grover's algorithm, this attacker could find a variant of the target

transaction within the same block, resulting in the same hash. Such rigged transaction will then appear as legitimate to the other users and the dishonest participant will be able to substitute his forged database to all other databases in the network provided that he can hack simultaneously at least one-third of the nodes. In this platform, the number of QKD-secured communications required during the block construction procedure is of the order of n square for n participants, making it highly impracticable beyond private blockchains with a limited number of nodes. However, in addition to providing a first interesting example of hybridization between QKD and blockchain, this platform can still be considered to secure small sensitive parts of a wider network, for example in the context of a global Quantum Internet.

Apart from this QKD-secure blockchain, other Quantum algorithms implemented with future Quantum Computers could be considered to enhance blockchain security. The first Quantum Digital Signatures (QDS) scheme designed in 2001 is very similar to a classical signature algorithm called Lamport-OTS (One Time Signature) where the classical one-way function has been replaced by a quantum one-way function.

Classical Post-Quantum signature schemes are based on diverse mathematical constructions that are supposedly resistant to Quantum Computers, i.e. it is not easier to crack them with a Quantum Computer than it is with a Classical Computers.

Their security is still under scrutiny: their security proofs are either based on unproven—but conjectured to be—mathematical hard problems or on alternate versions of proven hard problems—called security reductions—for which the security is unclear. But they have the huge benefit of not necessitating Quantum hardware to provide safety, contrary to solutions based on Quantum Key Distribution.

Several candidates for signature, key exchange and encryption are under evaluations in the recent NIST Post-Quantum cryptography certification process, which began in late 2017 and is expected to run at least until 2021. No less than 79 proposals covering various mathematical problems were submitted during the first round. Their security and requirements will be exhaustively examined, and the NIST expects to select several of them for certification. As of October 2018, several of these algorithms have been withdrawn due to unfixable security flaws. Many others have suffered attacks with various degrees of severity and are being adjusted (source: Post-Quantum Crypto Lounge).

For each transaction occurring in the blockchain, a public key and a signature value are stored to allow for a validity check. Small parameter sizes and fast execution times are of the utmost importance when choosing suitable security solutions. Unfortunately, in many Post-Quantum algorithms, acceptable parameter sizes and efficiencies come at the expense of assumptions on the algorithm's security that make it vulnerable.

There are more than 10 startups worldwide working on blockchain designs based on Post-Quantum signature schemes. The most frequently mentioned candidates are Hash-based Merkle tree schemes such as the eXtended Merkle Signature Scheme (XMSS) which is designed from One-Time Signatures, e.g. Lamport-OTS or Winternitz-OTS. Another widely considered category, lattice-based cryptography, is constructed around mathematical lattice problems, e.g. finding the shortest non-zero vector between two points in a given lattice. The BLISS or CRYSTAL-DILITHIUM signature schemes are considered as promising candidates to construct new post-quantum blockchains.

Another, and complementary, angle towards quantum-safe blockchains is the choice of an adequate consensus that should at least be able to satisfy the following requirements. The new challenge should be difficult to solve but easy to verify and it should not be solved faster with a Quantum Computer than with a classical computer. Concerning Proof-of-Work, the difficulty of the underlying mathematical problem should also be tunable in accordance with the network overall computing power.

Some interesting short-term candidates based on search

POST-QUANTUM CYBERSECURITY FOR BLOCKCHAIN

CRYPTONEXT

Post-Quantum

QuantiCor

Figure 4 (left)

Cybersecurity compagnies that are developing a specific quantum-safe offer to secure blockchain architectures.

QUANTUM-SAFE LEDGERS

QRL

SHIELD

NEXUS

ArQit

MOCHIMO
Future State Cryptocurrency

Figure 4 (right)

Startups building new blockchain designs revolving around quantum-safe mechanisms.

problems are called memory-intensive PoW. The Momentum consensus (Haschcash) is based on the difficulty of finding two pre-images resulting in the same hash, a collision problem which admits a quantum speed-up with Grover's algorithm but reduced vs the standard PoW consensus. In a completely different way, Cuckoo Cycle (CodeChain) relies on the difficulty of finding constant sized subgraphs in a random graph and Equihash (Zcash) is based on the generalized birthday problem.
Another interesting possibility is to replace the Proof-of-Work consensus by a Proof-of-Stake consensus, the later being safe against Grover's algorithm by design. This replacement could also result in a very cost-efficient alternative provided the reduction of the energy necessary to append new blocks to the blockchain.
An important technical challenge in the establishment of a PoS protocol is to provide entropy for the randomized election process to avoid influence by a malicious party. In current PoS, this is ensured by multi-party coin flipping algorithms which are based on Public-Key algorithms and thus also vulnerable against Quantum attacks. Unconditionally secure multi-party coin flipping and computation algorithms must be considered and implemented in PoS to ensure their security in the future Quantum world.

It is clear now that in the coming age of Quantum Computing, all cryptography-related industries will be immensely impacted. Quantum Technologies such as QKD as well as Post-Quantum cryptography running on classical computers could provide adequate solutions for cybersecurity in this era.

What is less clear though is how the data that will have been generated and encrypted until this time will be kept secured...

TO KNOW MORE

Quantum attacks on Bitcoin, and how to protect against them. Divesh Aggarwal, Gavin Brennen, Troy Lee, Miklos Santha, Marco Tomamichel. Ledger Vol. 3 (2018).

Quantum Computing in the NISQ era and beyond. John Preskill. Quantum 2, 79 (2018).

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

Applying Grover's Algorithm to AES: Quantum Resource Estimates. Markus Grassl, Brandon Langenberg, Martin Roetteler and Rainer Steinwandt. PQCrypto 2016: Post-Quantum Cryptography pp 29-43 (2016).

Factoring with n+2 clean qubits and n-1 dirty qubits. Craig Gidney. arXiv:1706.07884 (2017).

Quantum Digital Signatures. Daniel Gottesman and Isaac Chuang. arXiv:quant-ph/0105032 (2001).

http://cryptonext-security.com

https://www.post-quantum.com

https://quanticor-security.de

https://theqrl.org

https://www.shieldx.sh

https://nexusearth.com

https://mochimo.org

https://www.arqit.io

QUANTONATION

58, rue d'Hauteville
75010 Paris - France

Medium

Edition: December 2018