The QMC - Quantum MetaChain

Quantum Blockchains whitepaper

Abstract

In this whitepaper we present the QMC – Quantum MetaChain. QMC Blockchain will serve the global blockchain community as the ultimate guardian or the ultimate source of truth, and the protector of all other blockchains against the attack of quantum computers.

<tbc>

Introduction

There is no doubt that the best solution for guaranteeing Blockchain security in the era of Quantum Computers is to upgrade existing Blockchain protocols by an introduction of quantum cryptography into the design of Blockchain. This certainty comes from the conviction that quantum cryptography can deliver an ultimate security. To quote the author of "The Code Book" Simon Singh:

"Quantum cryptography would mark the end of the battle between codemakers and codebreakers, and the codemakers emerge victorious. Quantum cryptography is an unbreakable system of encryption. (…)

the claim that quantum cryptography is secure is qualitatively different from all previous claims. Quantum cryptography is not just effectively unbreakable, it is absolutely unbreakable."

We claim that designing and building Blockchain based on quantum cryptography will lead to the absolutely secure blockchain.

Designing such a blockchain assumes the use of quantum cryptography in a way that was pioneered in papers of [Kitenko] and evolved into practically implementable concept by the shareholders of our startup.

The practical implementation assumes the use of QKD in a way as close as it is possible to the initial ideas presented in our paper [„Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic"].

However, as the QKD networks that will ultimately enable the creation of the Quantum Internet are now in their childhood years, it is impossible to assume that the globally distributed QKD enhanced blockchains can replace the existing blockchains in the near future. The nature of this difficulty lies not only in the technological immaturity of QKD networks. The fundamental problem is that to guarantee the absoluteness of the security, we do not have something that could be called "quantum router" which enables the construction of the global Quantum Internet from the existing QKD links, in a similar way to how the existing Internet has been built from copper wires, fiber optics cables or radio waves. The same rules of physics that guarantee the absolute unbreakability of quantum cryptography protocols, prohibit us from creating the quantum router. The situation will change when the "free-space" QKD becomes available realized by the satellite based

communication. While such QKD has already been tested [a], we are far from its availability for practical communication.

What is possible and technically feasible today is the creation of QKD-based quantum blockchain in a specific locality/geography, where it is possible to connect certain number of blockchain nodes with QKD links.

However, the design of Blockchain assumes peer-to-peer connectivity. In a network of N nodes, full peer-to-peer connectivity requires N*(N-1)/2 links. In other words, the number of QKD links would scale quadratically with the number of nodes. With the current high cost to setup QKD links, it would be technically and economically infeasible to design such a network.

What we propose in the paper is the quantum blockchain which uses standard classical networks in a peer-to-peer mode and QKD links in specific network topology mode that reduces the number of QKD links. Such network topologies were popular in the early days of parallel computing and they allow for much better scalability than "full mesh" characteristic of peer-to-peer networks.

To deliver functioning and provably secure quantum blockchain we propose a modified communication and consensus protocol. Our previous protocol QSYAC, conceptually based on YAC consensus protocol, assumed the existence of the direct quantum secured links between each node of the blockchain.

For the Quantum MetaChain blockchain proposed here, we modified the underlying protocol so that it has lower number of QKD links than in the "full mesh" network topology. Essentially, it means that not every pair of nodes is directly connected by a QKD link, i.e. for its secured communication and consensus protocol we use some special mechanisms for the transmission of keys.

For the "topological" reasons that will become clear in this paper, we envision as a reasonable initial goal is to assume blockchain with number of nodes given by powers of 2: 4,8,16,32,64… because such is the number of vertices in the "hypercube" topology that represents one of many network topologies that scales better than ~N^2.

Despite these limitations, our design represents provably secured quantum, QKD-based blockchain. Such a blockchain can be deployed by limited, mostly trusted number of node operators in a limited locality or geography where the lengths of fiber optics links on which WKQ can operate do not exceed ~100 km, even though there are developments (See e.g.: arXiv:1007.4645v1) allowing for much bigger distances.

State of the Art of Quantum Resistant Blockchains

Despite progress in quantum cryptography and in post-quantum cryptography, the number of realistic solutions that were designed to protect Blockchains from the risk of being compromised in the era of quantum computing is unsatisfactory. A review published in 2020 ("Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks" DOI: 10.1109/ACCESS.2020.2968985) lists just few realistic blockchains based on quantum-resistant PQC algorithms. An excellent 2021 work ("Quantum-resistance in blockchain networks", https://doi.org/10.48550/arXiv.2106.06640) proposes a PQC based mechanism for securitization of Ethereum Blockchain, but falls short with references to existing realistic solutions.

To date, the most serious proposal directly using Post-Quantum Cryptography on realistically running mainnet is TheQRL (Quantum Resistant Ledger): https://www.theqrl.org/

Recently, there was a serious upgrade to QAN Platform, which we already named our competitor in the beginning of our startup. This upgrade includes PoR – Proof-of-Work consensus algorithm. The most serious resource about the platform is available here: https://learn.qanplatform.com/papers/white-paper

Beyond our work, there was only one high-level reference to the use of Quantum Cryptography for Blockchains. The work was done by JPMorgan, Toshiba and Ciena ("Paving the Way towards 800 Gbps Quantum-Secured Optical Channel Deployment in Mission-Critical Environments" https://arxiv.org/pdf/2202.07764.pdf) which involved routing a blockchain application over a single quantum-secured optical channel.

To summarize the state-of-art it is necessary to say that while there are realistic attempts to build or modify existing blockchains with Post-Quantum Cryptography, there is no realistic blockchain that is based in its entirety on quantum cryptography to protect itself from the imminent threats.

It is also debatable if the solutions based on PQC can offer sustainable solution for the future. After all, PQC algorithms are based on computational security. Although today we do not know quantum algorithms that could break PQC algorithms, it is not certain that the rapid advances in quantum algorithms would not bring these types of algorithms to their knees.

The purpose of Quantum MetaChain

The purpose of the Quantum Metachain is to create the first realistic Blockchain based on Quantum Cryptography that would offer security as high as it is offered by QKD networks (ITS – Information-theoretic Security) and use it to help any other blockchain to resists a potential attack of quantum computers. While QMC can be deployed in restricted geography where building QKD links would be feasible, there are a number of such geographies on the world where the nodes of the blockchain could be run by independent organizations to avoid an objection of "hidden centralization". What is more, there is a possibility of using Quantum Entanglement controllers like this one: https://syderal.pl/content/quantum-entanglement-controllers to connect such separated "geographies" into a global system. We will describe such an architecture later in this paper.

QMC basic operational function is to accept cryptographic information from other blockchains that can be securely stored in the quantum vault that QMC provides and can be retrieved on demand. We code-named such information as The Grain-of-Truth[1] (GoT).

The cryptographic information stored in GoT can at very minimum be a block hash or a root of Merkle tree build on a potentially large number of blocks of the original blockchain. The QMC mechanism applied here is similar in its basic design to the mechanisms which Layer2 blockchains use for "tethering" (or "pegging") into the mainnet of the their parent blockchain. We will describe one such idea of tethering later in this paper.

The information stored on QMC can at a very minimum be used to future validate the integrity of the blockchain that stored it on QMC. However, it will also be possible to store (and retrieve later) much richer information, enabling the future restoration of the information from QMC. By acting as

[1] Inspired by the title of Andrzej Sapkowski sci-fi novel "A Grain of Truth": http://www.andrzejsapkowski.pl/agrainoftruthuk.html (but not quite by its plot :-))

the ultimate guardian of other blockchains, QMC can also protect the other blockchains from more mundane attacks (like “51%” attack).

The architecture of Quantum MetaChain network

QMC uses QKD and quantum cryptography for creation of theoretically secure architecture.

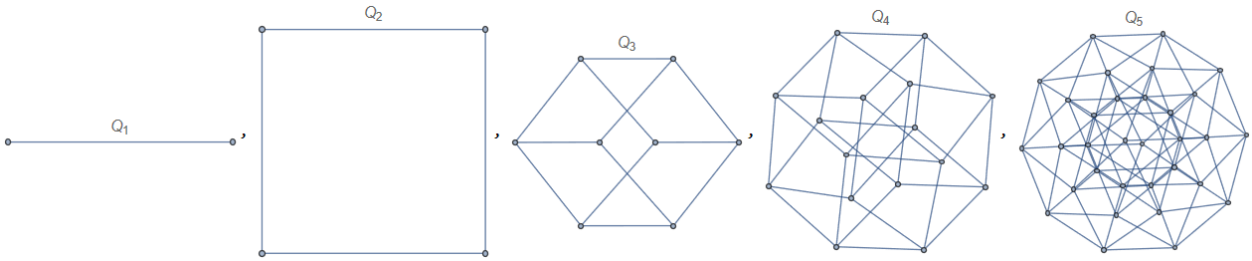
However, by its very nature, QKD network is extremely hard to build in practice. As it is based on quantum communication, creation of fully fledged routers, is not easy. So, it is very hard to go beyond point-to-point links with the key exchange mechanism of QKD.

If we wanted a fully secured network for any blockchain, it would demand a full mesh architecture, with links between every pair of nodes, leading to the number of QKD links growing as a square of the number of nodes.

This renders the simple use of QKD for creation of blockchains impractical. The problem is not simply technological (i.e. it does not come from underdeveloped technology) – it is of fundamental nature of quantum communication – we can’t “route” a stream of qubits because we can’t copy them (due to the no-cloning theorem). Thus the QKD networks do not allow for the end-to-end (node-to-node) transmission.

A possible solution is apply a specific network architecture that minimizes both the number of connections and the maximum number of “hops” needed to go from one node to an arbitrary other one (network diameter).

For example Hypercube network, illustrated here by hypercubes of dimensions from 1 to 5:



offers a good balance between number of links (2^N) in an N-node network and good network diameter (N).

There are many other types of networks that may have interesting properties from the perspective of the creation of QKD network. See [2] for an excellent study.

[2] David S. Lee and Jeffrey L. Kalb “Network Topology Analysis” SANDIA REPORT, 2008

Xin Sun has recently proposed a possible use of the small-world networks for the creation of quantum blockchain architecture[3].

Such networks represent a balanced number of “jumps” needed to transfer an info from anyone node to any other node.

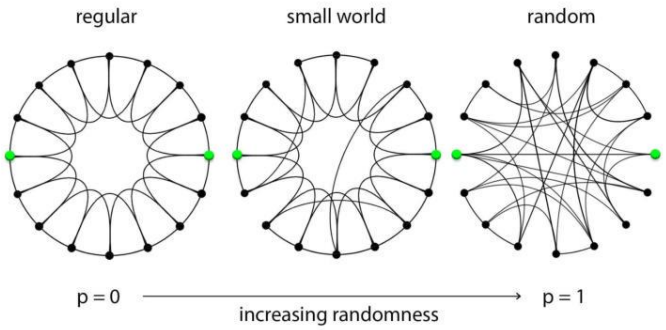
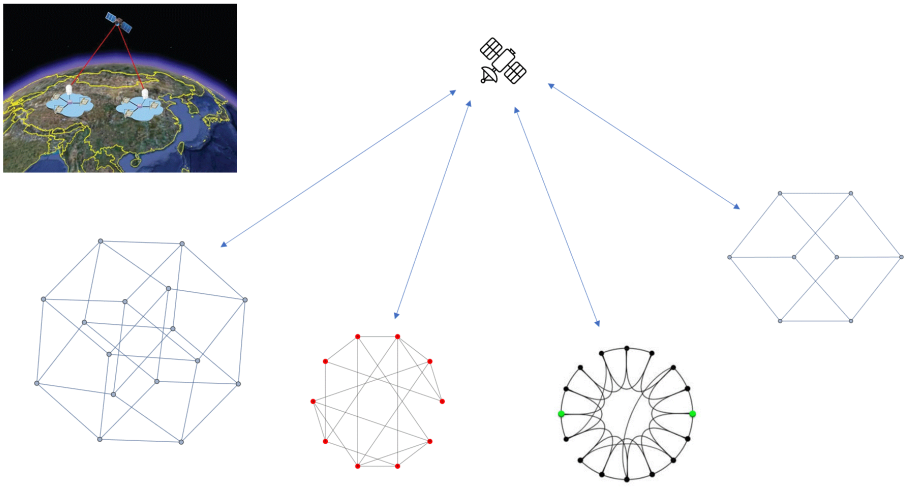


Figure 1. Small-world network from https://tagsync.com/small-world-networks-neurofeedback.htm

In our recent exchange with Syderal company, we discussed the possibility of using their Quantum Entanglement Controllers[4] to provide satellite based communication that would be capable of connecting the fiber-optics QKD based, separated blockchains, into one system by providing quantum secured satellite links as depicted in the following picture:



[3] Xin Sun, QBCK internal communication. Small-world networks are defined here: https://en.wikipedia.org/wiki/Small-world_network
Interesting post is available here: https://medium.com/@HugoAContrerasP/small-world-networks-2faa5323a77e , another here: https://tagsync.com/small-world-networks-neurofeedback.htm
and a paper:
https://www.researchgate.net/publication/224453450_Toward_Efficient_Failure_Management_for_Reliable_Transparent_Optical_Networks

[4] https://syderal.pl/content/quantum-entanglement-controllers

For any type of the network we will adopt, we must design two operations for such a network:

1) Communication (sending transactions through the entire network to form distributed ledger)
2) Consensus (achieving agreement about the values in the blocks of the ledger)

Assuming that we can create secure communication and consensus protocols for a given network topology, we are not restricted by the choice of any particular topology.

The another assumption is that every node in QMC can easily and inexpensively communicate classically with every other node in a typical peer-to-peer mode. The special topologies for communication are only needed for QKD links.

A possible communication mechanism

We assume that we must send message M of length l_M bits from node A to node B.

If nodes A and B are connected, we can send the message directly using standard QKD protocol: we use QKD device to generate KEY at node A (of l_M bits) and securely send it to the node B. After the key is distributed, we use OTP (One-Time Pad) to encrypt the message at A and decrypt it at B.

If nodes A and B are not connected we must send the message M with the help of the intermediate nodes. Without a loss of generality, we can assume that:

1) There is at least one intermediate node IN_k
2) There is more than one route between A and B, engaging different intermediate nodes IN_i

One possible solution could be constructed as follows:

When the sender A wants to send a message to B, the follow the steps:

a) A uses and independent QRNG to generate a key K_q intended to be used by B to decrypt the message A wants to send.
b) It concatenates the key K_q with the message M and the address of node B (the concatenation may be done in a more secure way than just by sticking K_q, M and the address together) to form a special message called KMA.
c) Node A sends KMA using QKD to the node IN_1.
d) If the node IN1 is connected to the node B it sends the message using QKD
e) If not – it chooses another intermediate node IN_n until it reaches a node directly connected to the node B. All connections are made using QKD.
f) Node B deciphers the message KMA and extracts M from it.

For easier reference in this paper let's call this solution – "an indirect key transfer" – 'IKT' .

We need to verify the security of the IKT mechanism.

There is an alternative possible mechanism where PQC asymmetric cryptographic method is used to protect M from being deciphered at the intermediate nodes IN_n. We can develop the details later.

A possible consensus mechanism

The consensus mechanism for QMC is voting-based as in the original design of our blockchain. It is described in the part 3.1 (The QSYAC Protocol) of our paper "Towards Quantum-Secured Permissioned Blockchain: Signature, Consensus, and Logic"[5]. (If we convert this document to the public whitepaper, we need to rewrite the parts of that paper (2.1, 2.2, 3.1) and put it here).

Until we design a better protocol suitable for the selected topology, we can use the existing one where we make the following modification:

1) In the TGS signature we adopt a mechanism described in the previous section ("A possible communication mechanism") as IKT - which assumes that the keys are transferred between nodes unconnected by direct QKD links using a scheme described there. This scheme is used for secure transfer of bit strings in the TGS distribution phase (step 4.a.ii in the Definition of TGS) and possibly for sending the Toeplitz matrix (or its generator).
2) In the QSYAC protocol's decision phase we need to send votes for blocks securely using the IKT mechanism

Such a protocol would represent an entry-level consensus mechanism, we could use, until we invent the ultimate one.

The Quantum Vault of QMC

Quantum MetaChain shall provide ITS level secure storage for the data it stores in its nodes. In other words, QMC must be secure not only for the "data-in-transit" as it flows in the blockchain network, but also for the "data-at-rest", when it is stored in the nodes' vaults (or safes).

We have described a potential mechanism for protecting "data-in-transit" with the use of QKD and our blockchain mechanisms as well as an entry-level consensus mechanism using QKD.

For protection of "data-at-rest" with Information-Theoretic Security (ITS level) the method of Secret Sharing shall be used.

Invented independently by Adi Shamir and George Blakley (1979) Secret Sharing is a method of distributing a secret data set to a group of participants. Every participant is allocated only a part of data - the secret share. The entire secret data set can only be reconstructed from an enough number of possibly different kinds of shares. It is impossible to use individual shares alone to reconstruct the data. Assuming that the retrieval of the shares for reconstruction is done using ITS Level communication, like QKD, we can achieve ITS Level storage of data.

An example of such secure storage (for medical data) is briefly described in the Conference on Lasers and Electro-Optics Europe (CLEO EUROPE)[6] conference paper[7]. The idea of the Quantum Vault was also an object of a use case demonstrated by the three companies: Equinix, Mt Pelerin and ID Quantique. There is a brief presentation of the concept available[8].

There is additional considerations needed here. First, if we applied secret-sharing in a simplistic manner, it would create a blockchain system where each node would not have the entire history of

[5] doi:10.3390/exx010005
[6] https://ieeexplore.ieee.org/xpl/conhome/9541543/proceeding
[7] https://ieeexplore.ieee.org/document/9542590
[8] https://youtu.be/CtMrCcTFMDk?t=3134

the QMC. It is not clear now, if we could safely construct such a system. Alternatively we could have all the data at every node but in encrypted form, and to use secret sharing to handle encryption/decryption keys.

Second, it is important to decide upon the basic data model for QMC storage of the GoT (Grain of Turth) that will be used to protect the other blockchains. We need to consider architectures like GraphChain[9] or similar for that purpose[10].

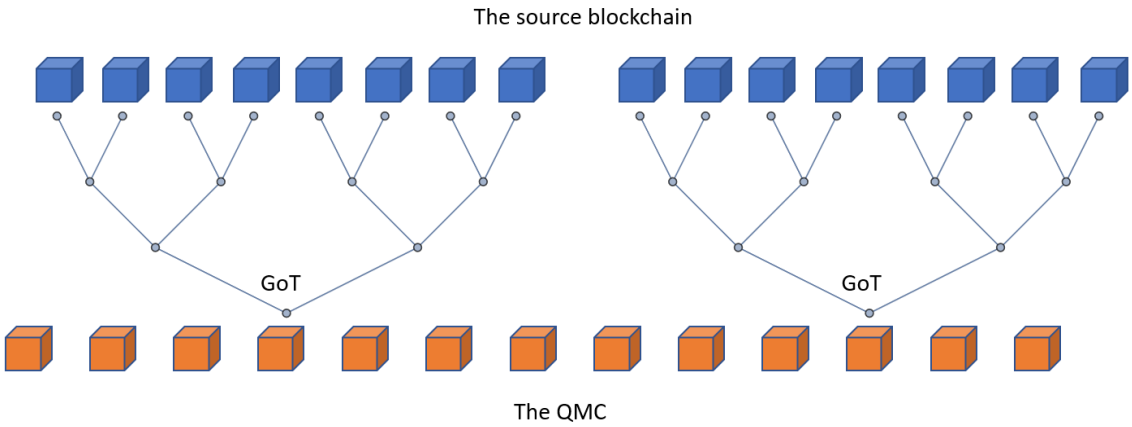
Posting data to QMC – Passing the Grains of Truth (GoTs) to the QMC

The fundamental mechanism of QMC which delivers its safeguarding capacity for other blockchains is based on the idea of passing a cryptographic material generated by the blockchains, which works as a generalized signature for their data, to QMC for safe storage and which allows for future validation of the original data immutability. The material, code names GoT (Grain of Truth) can be generated by multiple different mechanisms. What is more the actual content for the GoT may be different for different source blockchains.

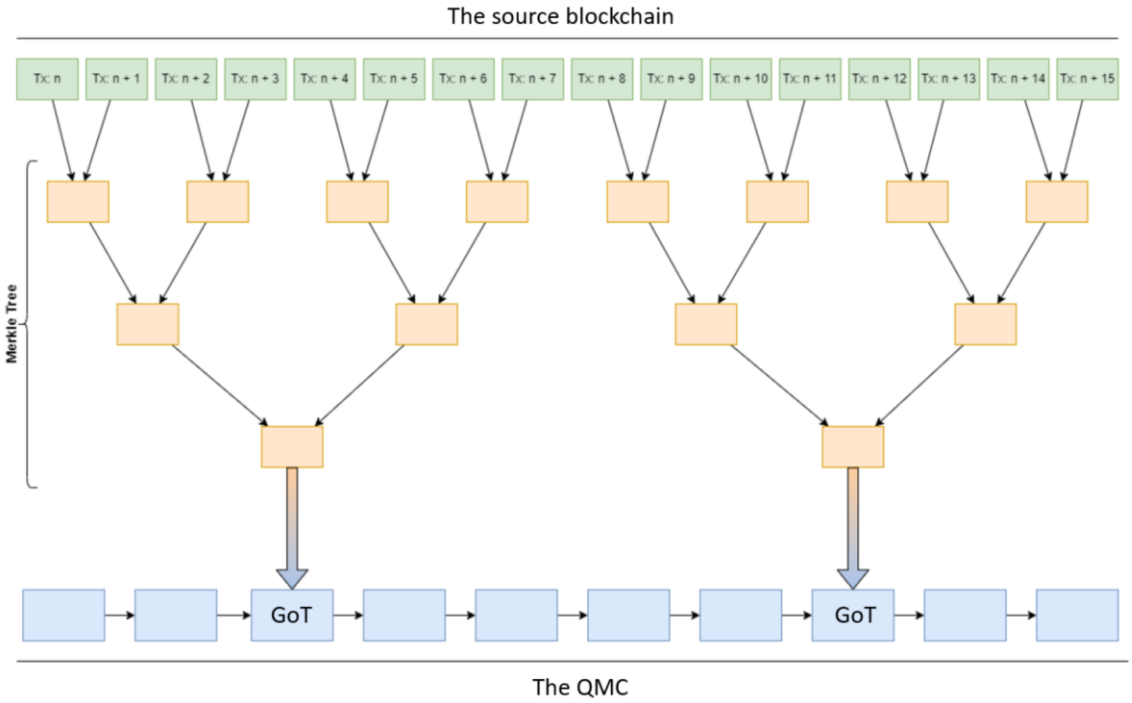
From the high-level perspective, the mechanism resembles mechanisms which Layer-2 protocols use while tethering a sidechain to a parent chain.

One of the mechanisms is based on Merkle Trees. Depending on the source blockchain activity (number of new transactions or blocks generated per unit of time), every 2^n transactions (blocks) of the source, a Merkle Tree is generated. In the leaves of the tree the mechanism stores both Blockchain transaction hash and any other data important for immutability preservation.

The mechanism can be depicted in the diagrams:



[9] https://ieeexplore.ieee.org/document/9672134
[10] https://flur.ee/



Of course, the mechanism may be quite different and will depend on the needs and constrains of the source blockchain. Also the actual content for the GoT will differ. Because of the that, the design of GoT data model will have fundamental importance for the QMC.

Addresses, private & public keys and the wallets on the QMC

While there exists research on Quantum Digital Signature - QDS[11], it is quite unlikely that we can use them on QMC as a replacement for classical Digital Signatures. This aspect requires more research. However, some more advanced PQC – Post-Quantum Cryptography signature schemes are available[12]. It seems that the choice should be made from the small set of three NIST announced finalist algorithms: CRYSTALS-DILITHIUM, FALCON and Rainbow.

Independent of the final choice, it is obvious that we shall expect much larger sizes for addresses, and for private and public keys.

For example, for the Crystals-Dilithium algorithm[13] we shall expect the following lengths, depending on the assumed security level[13]:

Parameter set	Security model	Claimed NIST Level	Public key size (bytes)	Secret key size (bytes)	Signature size (bytes)
Dilithium2	EUF-CMA	2	1312	2528	2420
Dilithium3	EUF-CMA	3	1952	4000	3293
Dilithium5	EUF-CMA	5	2592	4864	4595

[11] https://en.wikipedia.org/wiki/Quantum_digital_signature
[12] https://arxiv.org/abs/2107.11082
[13] https://openquantumsafe.org/liboqs/algorithms/sig/dilithium.html

The other algorithms offer the wide range of the key sizes:

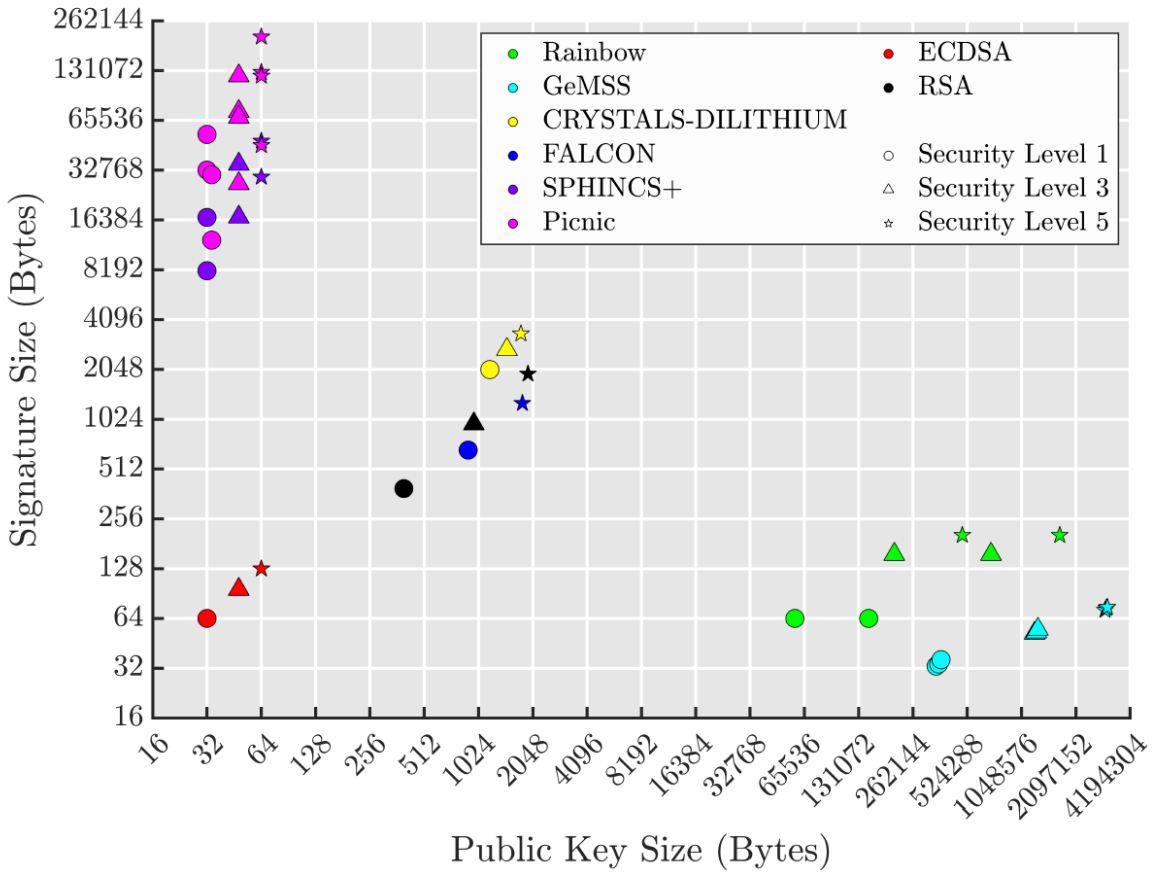


Figure 2 The picture from reference [12]

It is obvious that the workings of wallets shall change too. While we still could expect the possibility of the use of mnemonics for the regeneration of the private keys, their length as well as the size of the vocabularies shall change.

The another aspect is that the users of the QMC blockchain (source blockchain custodians and QMC operators), shall be strongly identified and authenticated in a way that possibly transcends the capacity of private/public keys mechanism. We will have to consider much more secure and reliable mechanisms like quantum-resistant PUF (Physically Unclonable Functions)[14] .

Source of randomness

As the source of randomness for the QMC it is obligatory to use QRNGs (Quantum Random Number Generators). As the QRNG is a part of the QKD devices, this requirement shall be quite easy. In all

[14] https://en.wikipedia.org/wiki/Physical_unclonable_function

instances where QKD's QRNG could not be used, we shall use high quality Entropy As a services mechanism (the one we have already build at our website[15]

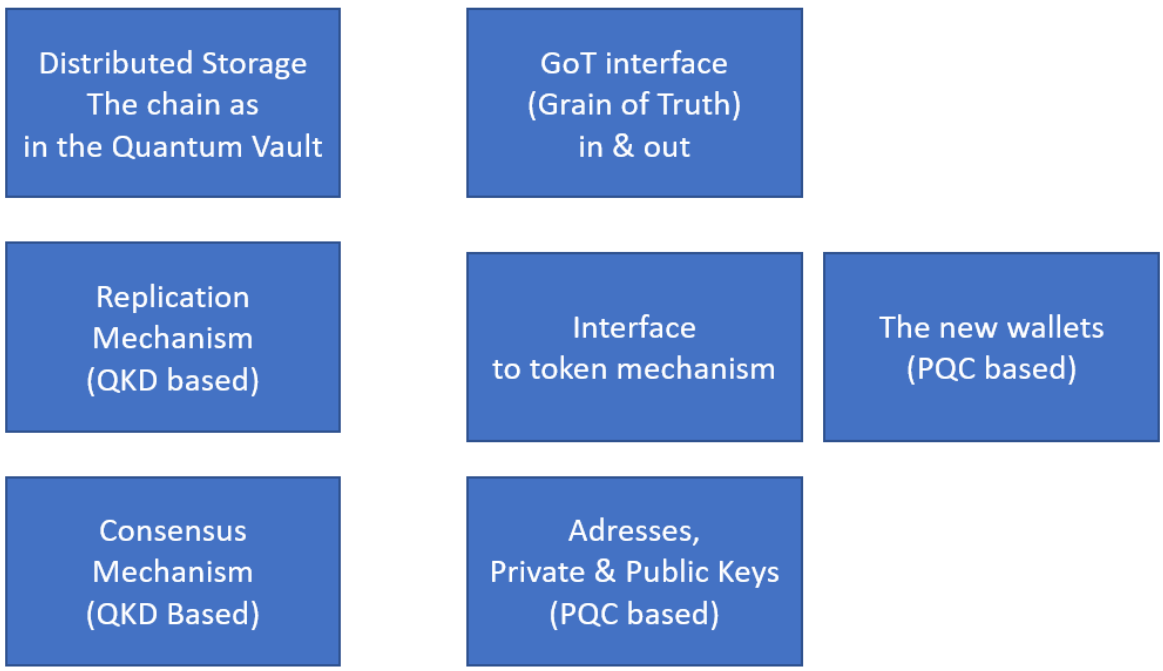
Possible tokenization

We do not exclude the creation of a new token/coin to help in the QMC economy side. However, to do so, we shall use an external, third-party blockchain, like Ethereum.

<tbc>

Top-level depiction of QMC system components

<tbc>



Conclusion

<tbc>

[15] https://www.quantumblockchains.io/current-services/