Q→NU

Proactively Quantum™

WHITEPAPER

Securing Blockchain Using Quantum Cryptography

Blockchain was born with the cryptocurrency Bitcoin. It has since evolved into a technology that provides a secure method for transactions between users who lack trust in each other.

Blockchain processes transactions with secure communication, privacy, resilience, non-repudiation and transparency—all necessary in a low-trust scenario. This has made the technology a popular choice in systems where the data needs to be securely transferred between different parties without letting the adversaries get their hands on it. Healthcare, IoT systems, logistics, banking systems, and other smart systems are increasingly opting for blockchain to prepare for a digital future.

Security is the backbone of Blockchain. Blockchain uses PKI (Public Key Infrastructure) to authenticate transactions between parties, and 'hashing' to generate digital certificates and link the blocks in a blockchain. Hashing makes the blocks tamper-resistant and only accessible to authenticated users.

That said, PKI and hashing are currently susceptible to attacks only with high computational resources. However, with quantum computers becoming a reality, they can't be deemed secure for long.

The tipping point for the breakdown of blockchain technology will be the day quantum computers are able to break a single block, after which there will be no turning back. Hence, it is important that we start securing the blocks now and generate the value blockchain intends to provide. In this paper, we will dig deeper into the security vulnerability of blockchain and how quantum encryption is the ideal solution that should be adopted.

Main security features of Blockchain

Decentralization

The control and decision-making are transferred from a centralized entity to a distributed network. This reduces the points of weakness in the system without degrading the functionality.

Privacy and data integrity

Blockchain uses the latest security techniques like PKI and hashing to secure the integrity and privacy of information being shared within the network

Data immutability

Once a transaction is stored in a blockchain, it cannot be modified or altered. All the steps of the transactions are also recorded and cannot be changed later.

Security backbone of blockchain

Before we understand the vulnerabilities, it is important that we understand the security method largely used in the present scenario. There are mainly two technologies used for secure a blockchain:

- PKI (Public Key Infrastructure)
- Hashing

Public Key Infrastructure

Blockchain uses PKI to secure information exchanges between parties through digital signatures. The message is signed using a private key and verified using a public key. For example, Bitcoin uses ECDSA signatures for the authentication purpose.

PKI is also important in crypto wallets, which are private-key containers, to store the files and data. In a blockchain system, the user has a wallet that is associated with a public address (hash of public key) and a private key that the user uses to sign the message or transaction.

Hashing

Hashing is mainly used for authenticating signatures and linking blocks. The PKI keys (public key) are mostly hashed when stored and used to authenticate the right user. Hashes link blocks in chronological order, with each block containing hash of the previous block. This linking can be restricted to a mathematical condition, like in the case of Bitcoin. Hashing is also used to generate user address or to shorten the size of an address.

The security problem

The security in use today at the key generation and distribution level is generally based on mathematics. This makes it vulnerable due to increase in computation power. Even though the same applies to blockchain security, it is safe till now because it is hard to achieve computational power required to break the security in a blockchain. This, too, will change with the advent of quantum computing.

A commercial-grade quantum computer won't be necessary to crack blockchain security as the combination of quantum simulators and classical computing will exponentially increase the computational power. This will break the security backbone that blockchain is based on and render the technology useless.

Let's see how quantum computers might be used to break the security on a higher level.

Public Key Infrastructure

Today, the cost of breaking 80-bit security cryptosystems (equivalent to RSA 1024 or ECDSA 192) is estimated to be hundreds of millions of dollars. It is not possible for everyone to own the costly hardware except state agencies willing to crack the cryptography. Therefore, researchers once believed it was safe to use PKI algorithms to secure blockchain, which is no longer true. Quantum computing has changed the perspective as it not only effects the present PKI systems, but also any future system with increased key lengths. The complexity on which PKI algorithms are based are hard to crack for classical computers but easy for quantum computers due to Shor's algorithm.

Shor's algorithm provides an unparalleled improvement in factoring large numbers. Its polynomial input length makes the gain in speed exponential. This could crack any key length of PKI given the time. The only variable saving us till today is quantum computers, and with them becoming a reality, it is just a matter of time before the whole PKI infrastructure goes for a toss. Quantum computing makes it possible to solve problems such as the discrete logarithm problem, which in turn makes cryptographic algorithms (like ElGamal encryption, Diffie Hellman key exchange, the Digital Signature Algorithm, and elliptic curve cryptography) insecure. The existence of Shor's algorithm demonstrates that a quantum computer opens vulnerabilities beyond that of the commonly seen attacks today.

Hashing

Hashing is a very complex problem to solve with classical computers. However, with the exponential increase in computational power brought in by quantum computers in combination with Grover's algorithm, hashing has become an insecure way to link the blocks. There are mainly two kinds of attacks on hashing that are possible with Grover's algorithm.

Full collision

When two different data have the same hash value, the situation is called a "collision". Even though collisions do occur, they are very difficult to find. If we are able to generate full collisions (all the possible combinations of hashes in a chain), then we can modify the whole blockchain, which will negate the security provided by blockchain. This involves a brute-force which is difficult to compute. Known vulnerabilities can reduce the time taken to crack the collisions, but to a minimal extent.

We expect the order of O(n) to perform the attack of full collision. Grover's algorithm reduces the run time to O(√n), which decreases the time to brute-force polynomial time. This makes it possible to insert blocks without disturbing the sequence of the blockchain. Even though we can mitigate the attack by increasing the hash lengths, the computational effort to calculate the long hashes will limit the ability to generate the chains, rendering the blockchain non-viable.

Mining time

Mining a blockchain, creating new blockchains, adding it to the current chains to enable new transactions and increasing the value of the cryptocurrency using computational power—all of this is possible today due to the exponential increase in variable function of computational cost to generate each chain.

With the advent of quantum computing, it has become easy to construct the chains and generate new blockchains. This means only the fastest miners will be able to get more value out of the cryptocurrencies. This tips the scales of value generated by the blockchain against those dependent on classical transactions. This undermines the integrity on which the blockchain technology is built.

However, these are only some effects we can proactively see through. There can be many possible attack vectors that will mushroom due to quantum computers that will totally change the security landscape. We need to secure the chains and blocks in the blockchain now and shift them to secure levels of cryptography for future usage and security.

Ideal features of blockchain for post-quantum world

For a efficient, trustworthy, and secure technology, we need to have the following main features in the post-quantum blockchain:

Small key sizes

The keys that would effectively replace PKI should be of less key sizes but more secure. This is important when a blockchain is interacting with digital systems like IoT, AI and ML which cannot work on large and complex key systems.

Small signature & hash length

As discussed earlier, increasing the hash length is not a viable solution. It is important that the hashes are replaced by small tokens which cannot be predicted and can be used at a very high rate to create the chains in a blockchain.

Fast execution

When integrated with the digital system, blockchain would work at a very high TPS (transactions per second). The new schemes of cryptography should be able to function at such high rates without introducing any latency into the system.

Low energy consumption

The cryptocurrency implementation of blockchain especially requires high energy to execute the protocol. This is due to the complex hardware, communications, security schemes, and transactions involved. New security should aim at reducing the energy consumption.

The QNu solution

Years ago, NIST observed the problems that quantum computing will cause and, hence, is evaluating algorithms that can replace the PKI systems. These are called Post-Quantum Cryptographic (PQC) Algorithms. At QNu, we have adopted a way in which PQC can be integrated into quantum encryption, which uses quantum physics principles to repel the attacks by quantum computers.

Below are the QNu products which will help in securing the blockchain infrastructure and increase its scope of applications

QUANTUM RANDOM NUMBER GENERATOR

- Generates 100% random numbers using quantum source
- Entropy is of the highest level possible
- Also comes in the form of chip or PCIe card

Explore Tropos (QRNG)

QUANTUM KEY DISTRIBUTION

- Secure key distribution and generation using quantum physics principles
- Intrusion detection allows to identify adversary tapping into the network

Explore Armos (QKD)

POST QUANTUM CRYPTOGRAPHY

- Algorithm based key generation which are quantum resistant
- Approved by NIST
- To be used as hybrid with QKD for better security

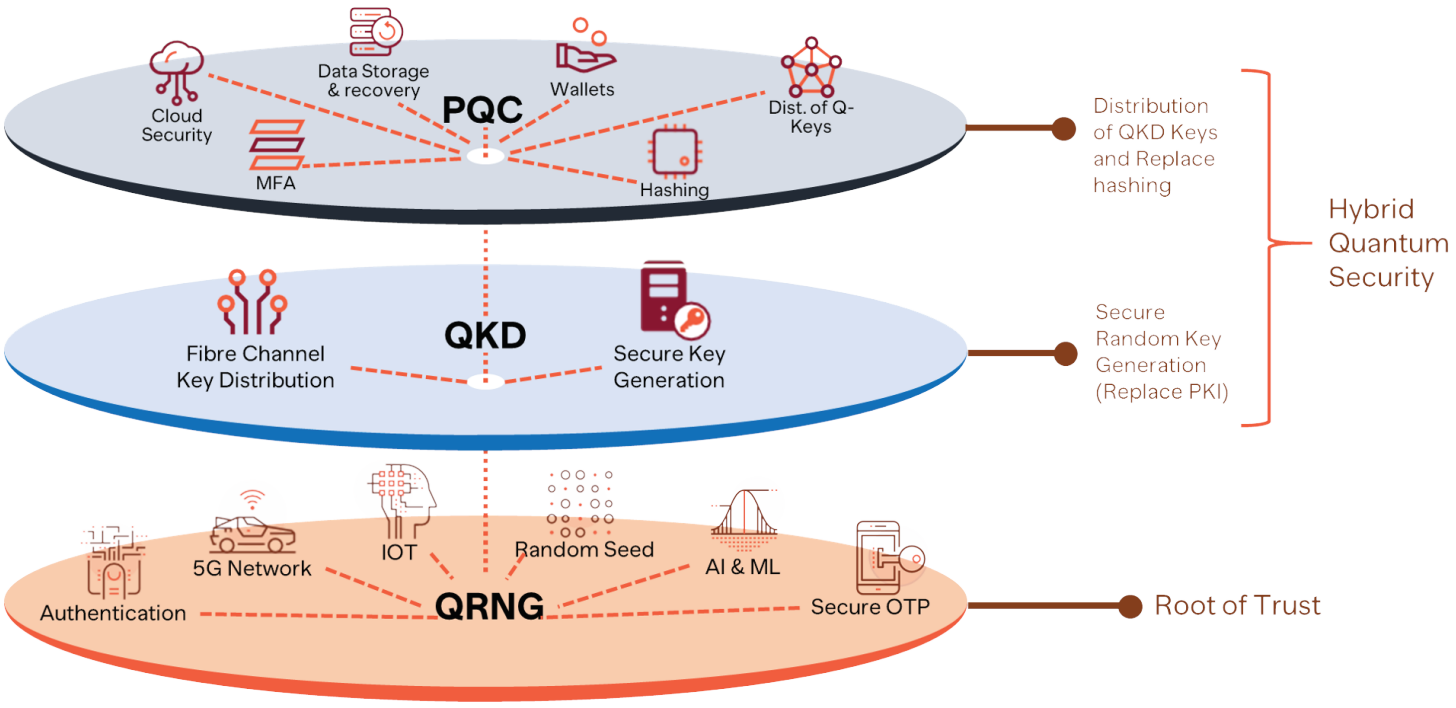
Explore Hodos (PQC)

The diagram below illustrates how blockchain will evolve using post-quantum technologies. The basic problem today is randomness and this can be dealt with by using Tropos (Quantum Random Number Generator). Tropos uses a quantum source to generate random numbers that can be fed to hashing and key infrastructure to increase the security posture. The random numbers from Tropos can be distributed to IoT and other digital systems using Qosmos (Entropy as a Service) for a secure last-mile distribution of random numbers.

Tropos is connected to Armos (Quantum Key Distribution) to generate keys using quantum physics principles and cannot be broken with any computational power. Armos is restricted to fibre optic communication, which can be extended using our PQC product, Hodos. Hodos not only distributes quantum keys to encrypt the data flowing between the nodes, but also generates hashes which are quantum resistant.

The hashes generated will be a combination of random numbers from Tropos and keys from Hodos. Armos keys provide the replacement to PKI keys for security of wallets and use Hodos keys to encrypt, thereby providing security for longer periods. A Hodos hash combined with an Armos key is not based on any mathematics and at higher TPS, making it secure against the computational power of quantum computers. This can be use to generate chains which cannot be broken due to the complexity. This combination provides unconditional security, making it the perfect solution for blockchain.

Solution stack



Why QNu security is perfect for blockchain?

Resistant to Quantum Computing

The generation of keys and hashing is purely random and are not governed by any mathematical laws. It is quantum-resistant and unconditionally secure for the future.

Key size and synthesis

The key size is not large and can be easily integrated into IoT and other systems which cannot operate on large key sizes.

Low energy consumption

The generation of hashes and keys requires normal hardware systems which do not need high energy.

Future security and agility

The QNu stack provides security for anytime into the future; it can be integrated into present and future digital systems.

Conclusion

Quantum computing is already here. The examples we see of Google, IBM, or Honeywell is just the tip of the iceberg. There are many quantum companies working on different quantum techniques and the tipping point for security is expected to be from any of these areas. Instead of waiting for the breakdown after which there will be no turning back, it is important that blockchain adopts quantum-safe encryption today to be relevant in the future.

Google achieved Quantum Supremacy

It is faster than any conventional computer available today

IBM hosted its quantum computer on cloud

These examples are just tip of the iceberg. The impact will be due to something which we do not see

Here are **73** companies changing the landscape of quantum technologies across verticals. Some of these companies have been able to raise about $50M to $100M. This will change the future of the world, not just in data security, but also in the way we interact with each other.

Quantum Computing is Here

There are many changes expected in blockchain with respect to applications and integrations in the future, and it is important that the security backbone remains intact and agile. This is only possible with QNu.

The implementation of QNu products into blockchain will secure it now, while any improvements made in the future can also be integrated into the QNu layer. This will ensure that there's no scope for vulnerabilities to take advantage of the change in technology.

Contact us to know how you can implement our products in your applications.

References

- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8967098
- https://www.mitre.org/sites/default/files/publications/17-4039-blockchain-and-quantum-computing.pdf
- https://medium.com/abelian/from-post-quantum-cryptography-to-post-quantum-blockchains-and-cryptocurrencies-an-introduction-eb0b50ed129a
- https://www.eylpartners.com/wp-content/uploads/2016/12/EYL_Brochure_2018_HP.pdf?ckattempt=1

Get in touch

E: info@qnulabs.com
sales@qnulabs.com

W: qnulabs.com

A: QuNu Labs Pvt. Ltd.
2nd Floor, East Wing,
Centenary Building,
28 MG Road, Bangalore - 25

T: +91 80 4851 4013
+91 988 604 1133