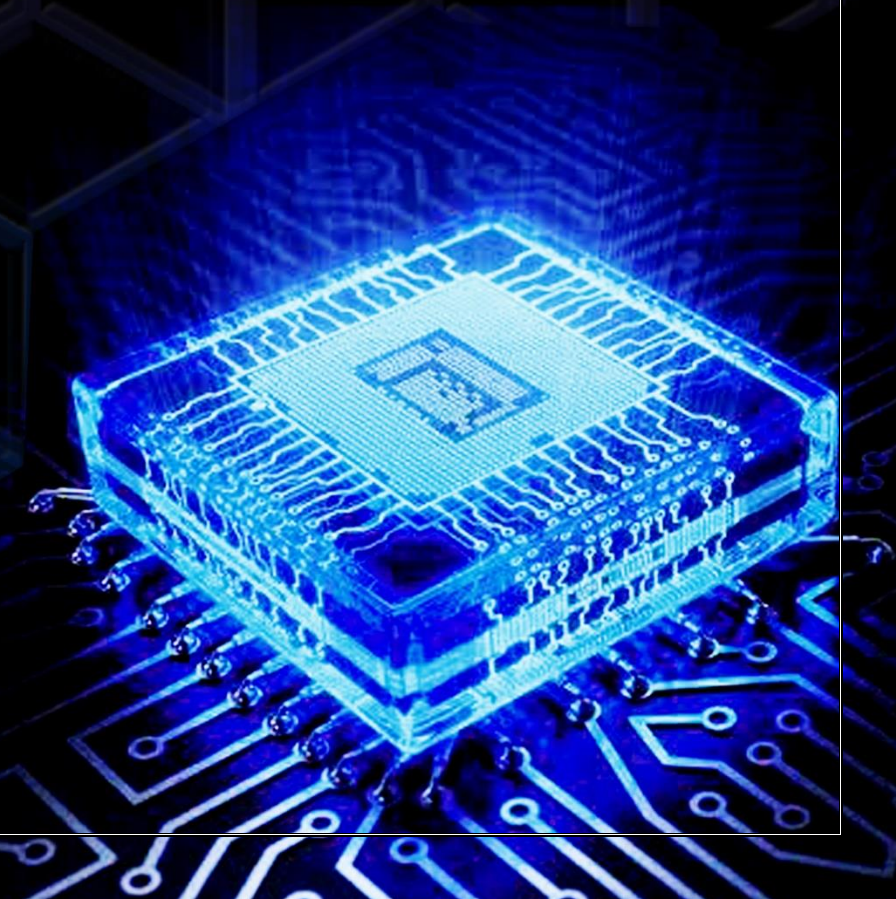
Hashcash Consultants®

HashCash Consultants Quantum Venture



Private Key Security with Quantum Encryption:

HashCash Consultants uses quantum computing to provide enterprises with enhanced and unbreakable private key security. Our work is focused on strengthening the existing security protocols of our Blockchain Network HC Net with quantum encryption.

A Brief on Quantum Computing & Quantum Encryption:

Quantum computing is cutting-edge compared to the existing digital version and involves an array of complex mathematical equations. The working of these devices revolves around the mechanics of quantum physics.

While a regular computer processes data as binary bits of 1 or 0, quantum computing uses quantum bits or qubits for the same. These qubits can exist in both the states of 0 and 1 simultaneously.

This unique feature allows multiple computations to happen at the same time. The concurrent state of both 0 and 1 creates a blend of probabilities known as a superposition, making it possible to store and manipulate a vast amount of information with a considerably small amount of particles.

While many fear that owing to this feature, quantum computing can be a threat to the existing advanced security encryptions in place, we beg to differ as the solution lies in the problem itself.

The state of superposition is what makes it very hard for cybercriminals to crack the code and steal the information. The laws of quantum have emboldened us with an advanced version of cryptography or encryption technique, which will revolutionize cybersecurity.

Quantum cryptography or quantum encryption uses the exact mechanics to encrypt and decrypt messages enabling only the intended sender and receiver to access it.

The Concept and Procedure of Quantum Cryptography:

Quantum Cryptography influences the photons or light particles to communicate or transmit any kind of data from the sender to the receiver. The characteristics of a fraction of the photons are measured and compared between the two endpoints to conclude the safety of the private key.

Here's A Breakdown of The Process:

- The photons are transmitted through a polarizer or filter. It provides with any one of the four possibilities in polarizations and bit i.e., vertical (1 bit), horizontal (0 bit), 45 degrees left (0 bit) or 45 degrees right (1 bit)

- The receiver of the photons utilizes two beam splitters which are either horizontal or vertical and diagonal to decipher the polarization per photon. One has to guess which splitter to use for this.

- After sending the photons, the receiver communicates the kind of beam splitter used for each photon in the series to the sender. It is followed by the sender comparing the information with the series of polarizers used for sending the key. The ones read using the wrong beam get deleted and the ones remaining create the key for decryption of data or message.

If there is any attempt to read or copy the key by someone unintended then the state changes automatically, making it virtually unbreakable.

Hashcash’s Use of Quantum Encryption:

Quantum encryption or quantum cryptography, harness laws of quantum physics to transmit a secret key most safely and securely. The current methods of transmitting secret keys are backed by complex mathematical equations. This might work in the present day scenario but from the future perspective, there is a high chance of the encryption getting compromised. So for long term security quantum cryptography is the best option.

Quantum Encryption in HC Net:

All of HashCash's applications are backed by Blockchain which uses public-key cryptography. A combination of the public and the private key is used to process transactions, and ensure security and privacy-preserving protocols.

The public key is the address of the wallet that network participants can see and send coins to and the private key is the one with which one can access their wallet. HashCash's Blockchain network HC Net is where all transactions take place and it is fortified with the most advanced encryption.

However, keeping the long term security in mind we are working on quantum computing to strengthen the private key using quantum encryption or cryptography.

Quantum Key Distribution:

HashCash uses QKD or Quantum Key Distribution as a subset of quantum cryptography to enhance private key security. It is being used to create private keys to send encrypted messages from one location to another. Because of complexities and multiple probabilities in quantum mechanics, the hackers cannot secretly copy the key. It requires extensive computation and breaking the laws of quantum physics to decode the key, making the process of encryption unbreakable. This ultimately provides the users with the safest passage to communicate and conduct transactions with one another through HC Net.

Thank You!

Hashcash Consultants

Contact us

Address: 2100 Geng Road, Palo Alto, CA, 94303, USA

Email: contact@hashcashconsultants.com

Phone: (888) 893-0588

Website: www.hashcashconsultants.com

Social Connection