Tomorrow's Cyber Security, Today

IRONCAP

IronCAP Use Case

The World's First Quantum-Safe Bitcoin ATM

01 Communique

01 COMMUNIQUE

Digital Asset Exchange Machine (DAEM)

Cryptocurrency and blockchains are widely accepted today. Cryptocurrency is redefining the conventional finance industry, and blockchain technology is changing the face of how businesses and governments operate.

Once considered "unhackable", blockchain end-points are now being targeted and hacked – the digital signature of the end-points used to be secure are actually vulnerable to attacks from quantum computers which have excessive computing power! According to an article on Nasdaq, blockchain end-points targeting reached new heights in May 2019 when hackers stole $40 million worth of Bitcoin from Binance, one of the world's biggest cryptocurrency exchanges. Most crypto wallets in today's market are connected to the internet and therefore VULNERABLE.

"The cyber security industry must become quantum-safe NOW. Quantum hacking is a matter of when, NOT "IF".

The patent-pending IronCAP technology developed by 01 Communique is to safeguard against quantum hacks. In December 2020, its partner ixFintech launched the world's first quantum-safe DAEM (Digital Asset Exchange Machine) at Cyberport, Hong Kong, allowing its customers to purchase and sell digital assets using cash and digital wallets. Utilising IronCAP's cryptographic technology for its key generation, encryption, decryption, digital signature, verification and other quantum-safe crypto functions, DAEM adopts 2 layers of authentication to ensure end-to-end security between:

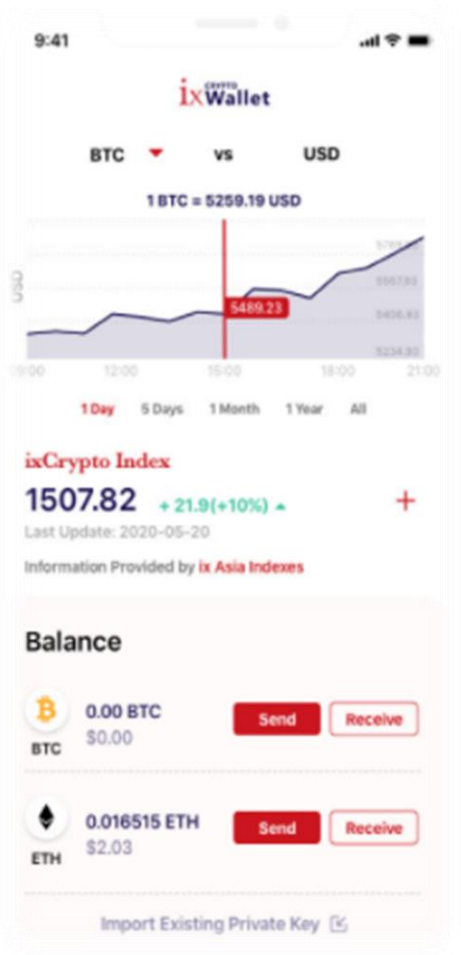
1. user's device and DAEM;
2. DAEM and the host application. The next phase of DAEM will include IronCAP in its e-wallets to further protect users' end-points and their digital assets.

DAEM has 3 levels security protection with post-quantum computing security being the most unique; making DAEM the world's first quantum-safe cryptocurrency machine.

Now you may wonder why post-quantum computing security today? Well, quantum advancements skyrocketed in 2020 and many experts believe cryptographic algorithms are quantum vulnerable. In fact, NSA in 2016 said that agencies and companies must become quantum-safe immediately. Difference between being quantum-safe 2-years-too early vs 2-years-too-late is EVERYTHING.

But why IronCAP?

End-points are secured today but vulnerable to attacks in the post-quantum era.



IronCAP is the first commercially available quantum-safe solution. Based on Goppa code-based theory; a 40-year time-tested with no mathematical cracking theory. It's a patent-pending cryptography system designed to operate on conventional computer systems and safeguard against the quantum future. Examples of vertical applications are email/file encryption, digital signatures, blockchain security, remote access/VPN, password management, credit card security, cloud storage, artificial intelligence, IoT (5G), and website security.

The security industry must become quantum-safe NOW. Quantum hacking is a matter of when, NOT IF. **Q-Day** (The day quantum computers can render all current encryption methods meaningless) is a lot closer than most people believe it to be.