Post-Quantum

Cryptography Conference

Vulnerabilities of Blockchain Security in the World of Quantum Computing

Andrew Cheung
President & CEO at 01 Communique Laboratory Inc.

ENTRUST HID PKI Consortium

Vulnerability of Blockchain in the Post-Quantum World

PKI Conference
(November 8, 2023)

Tomorrow's Cyber Security, Today
IRONCAP

HNDL Attack
(Harvest Now, Decrypt Later)

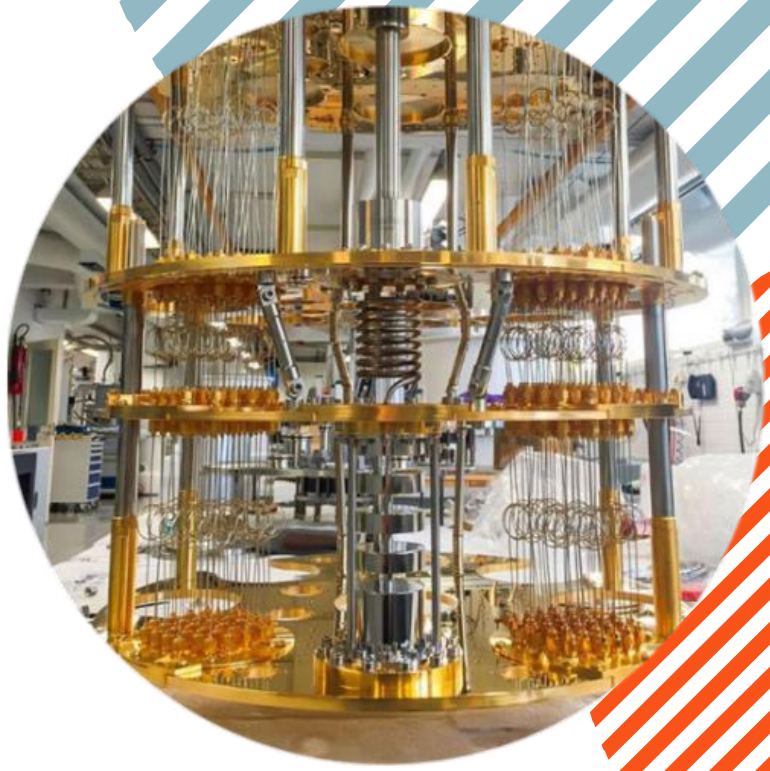
If X + Y > Z then *Checkmate!*

X	Y	Z
How long do you need your encrypted data to be secure?	How long will it take to implement a quantum secure solution into your current infrastructure?	How long will it take to develop a sufficiently strong enough scale quantum computer?

Q-Day has Arrived!

2019 – 27 Qubits
2022 – Osprey with 433 Qubits
2023 – Condor with 1121 Qubits
2024 – Flamingo with 1386 Qubits
2025 – Kookaburra with 4158+ Qubits
2026 – 100,000+ Qubits

- IBM's quantum computers roadmap (May 2022)



Researchers in China claimed to have reached a breakthrough in quantum computing, figuring out how they can break the RSA public-key encryption system using a quantum computer of 372 qubits
https://therecord.media/chinese-researchers-claim-to-have-broken-rsa-with-a-quantum-computer-experts-arent-so-sure/

- January 4, 2023

Who will Suffer on Q-Day?

Financial World

- ❑ Financial transactions: Cryptocurrencies, CBDC, etc.
- ❑ Smart card infrastructure

General Cybersecurity

- ❑ Healthcare system, Energy system
- ❑ National defence

World of Internet

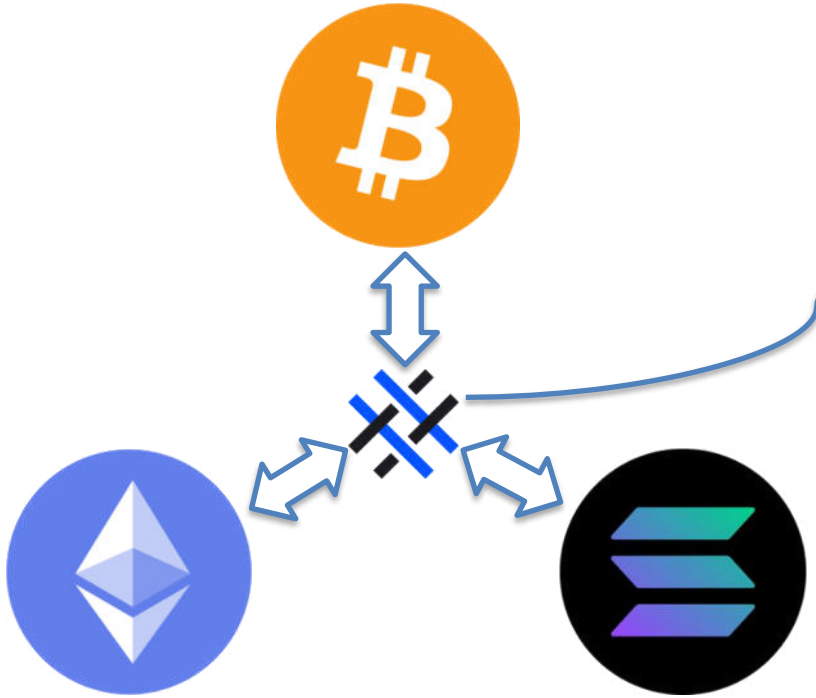
- ❑ AI Privacy
- ❑ Email security
- ❑ IoT
- ❑ Website authenticity

Crypto Theft 2022 - Record High

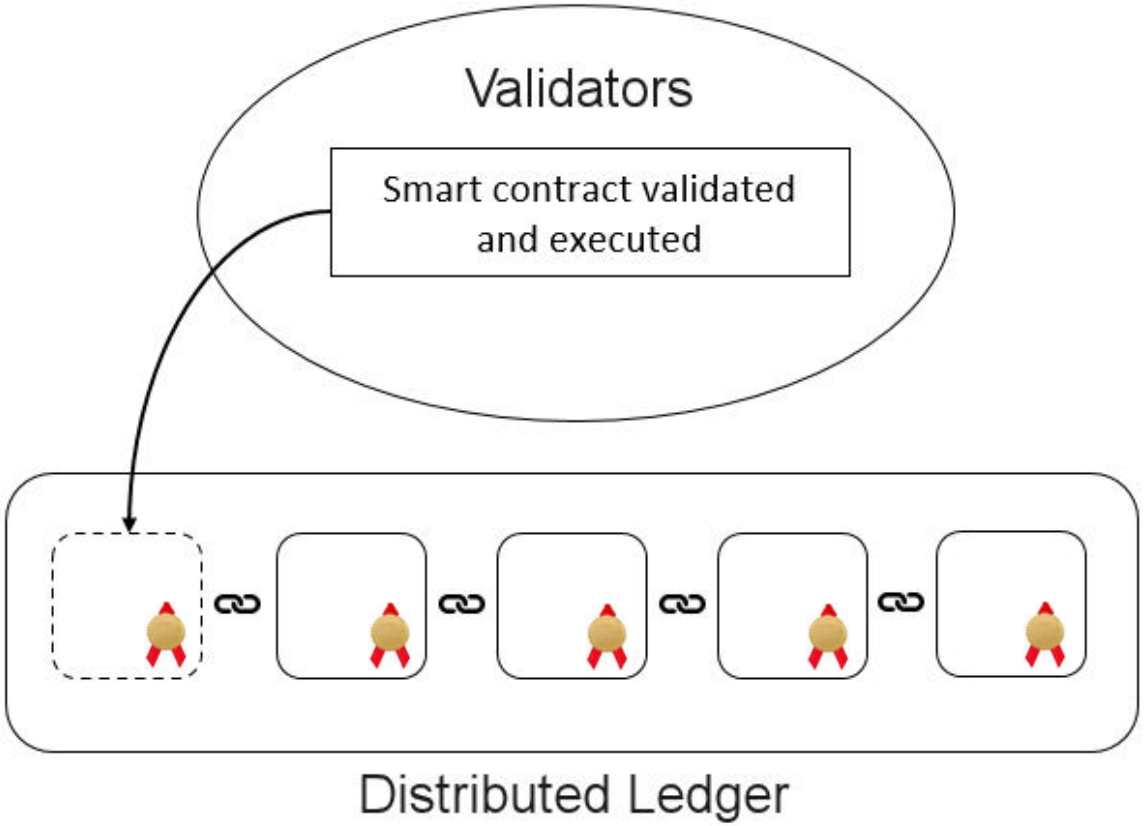
- $3.8B of crypto stolen by hackers in 2022
- October alone had $775m crypto stolen

Blockchain Vulnerability Today

- Vulnerabilities in DeFi applications
- Vulnerabilities in cross-chain bridges



Blockchain in Post-Quantum era



Blockchain PQ Conversion

Main Goals

- Replace the quantum-vulnerable signature algorithm (e.g. ECC) by a quantum-safe signature algorithm (e.g. Crystal Dilithium)
- Sandbox: Existing Solana chain

Challenges

- Data structure of the Solana smart contract is hard-coded to the size of ECC's signature and wallet address (public key size)

Blockchain PQ Solution

Off-the-chain PQ Validation

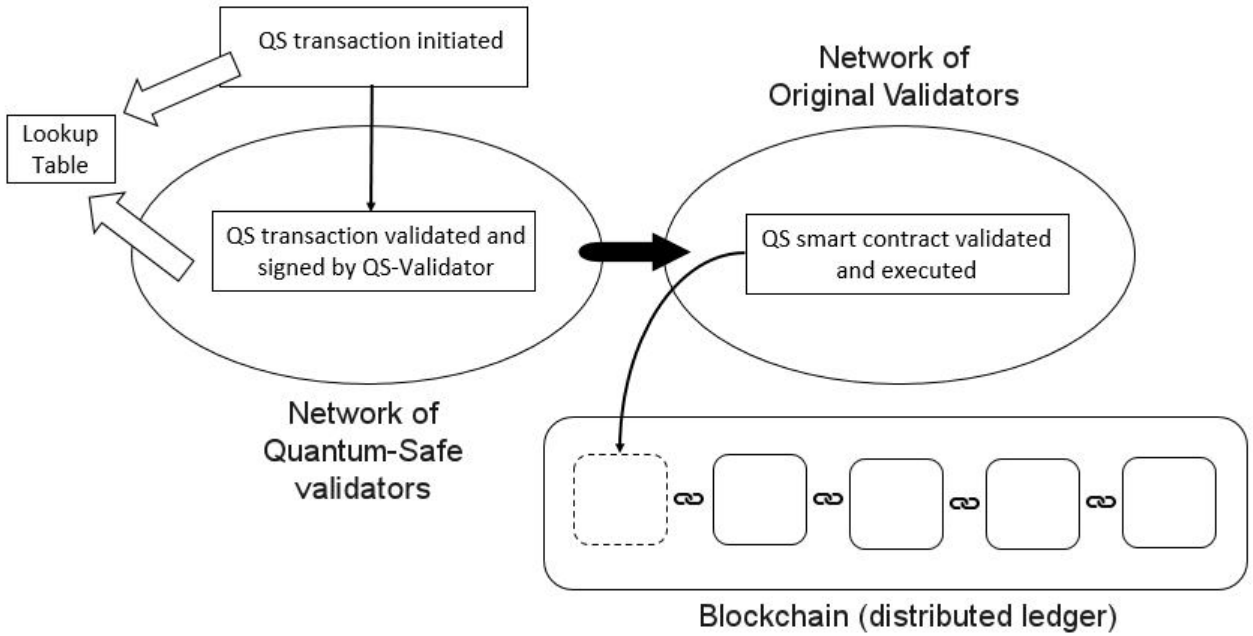
- Storing the hash (32-byte) of the PQ signature, payer's address, and payee's address rather than the actual data to avoid the data size limitation
- Resolving the hash to their original data via a look-up table

Results

- No change in the original smart contract
- 100% efficiency (TPS) retained

Quantum-Safe Blockchain

US Patent: #11,698,833

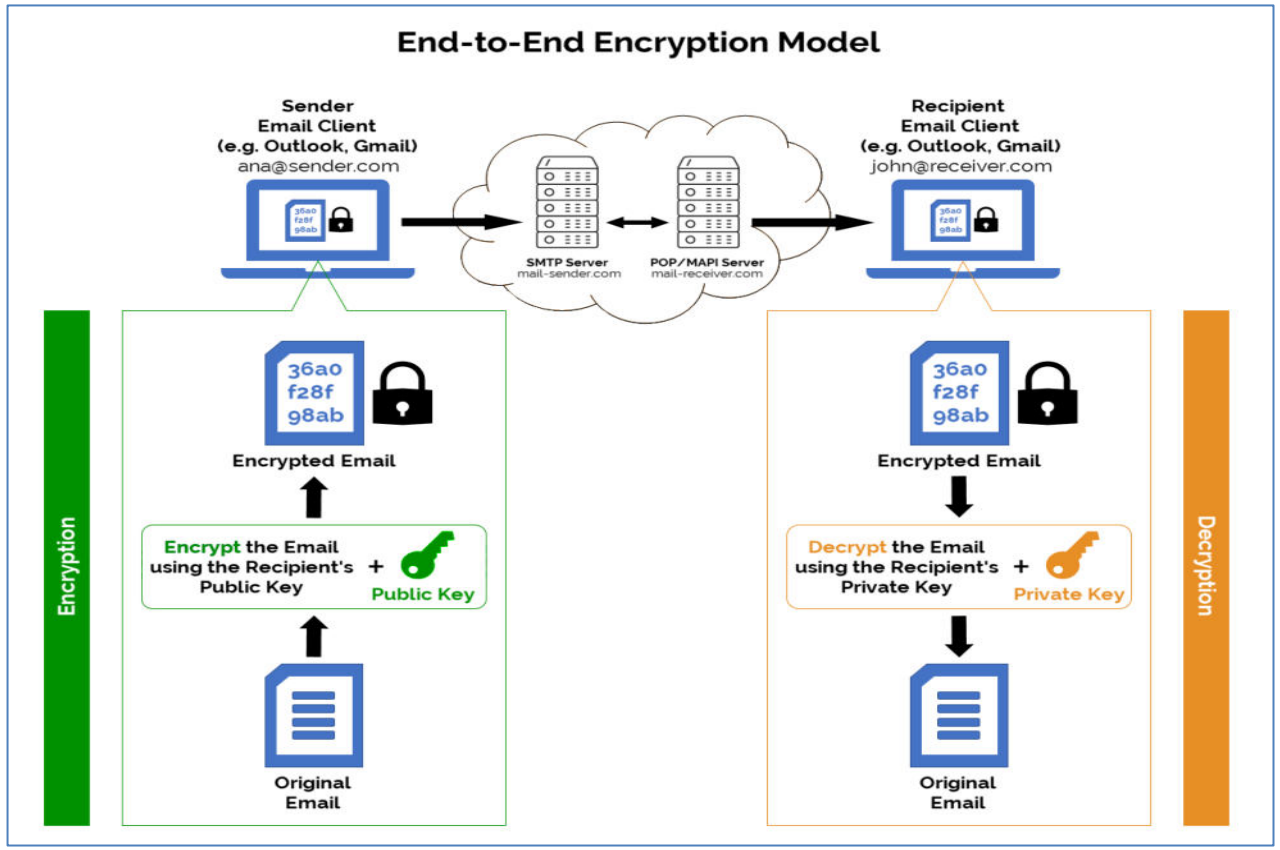


IRONCAP

Blockchain with Quantum-Safe HSM

THALES
Building a future we can all trust

Other Use Cases: Email Security



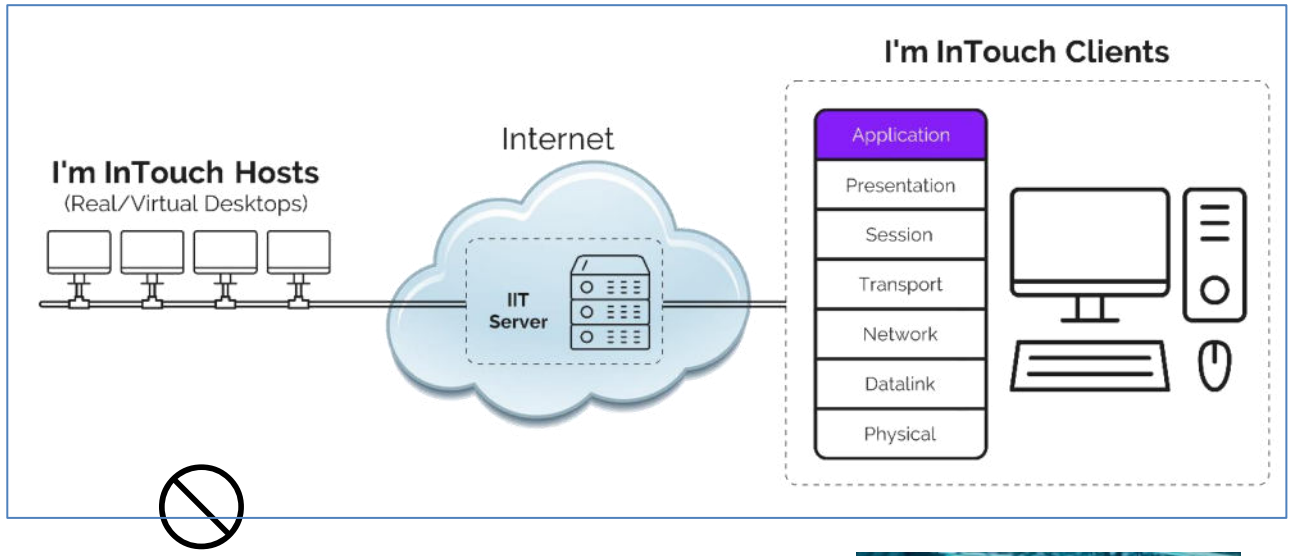
IRONCAP

Other Use Cases: Steganography

- Watermark steganography – **18th Century**
- Quantum-safe Steganography – **21st Century**
- IronCAP Goppa-code error vectors – **proven**
- International Patent Application – **filed**
- Applications: e-wallets recovery, NFTs, etc.

Other Use Cases: Remote Access

Quantum-Safe + Zero Trust



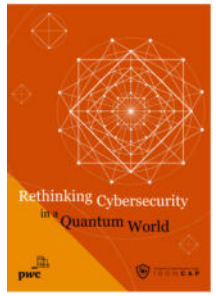
No access to corporate LAN

IRONCAP

Thought Leadership: Papers

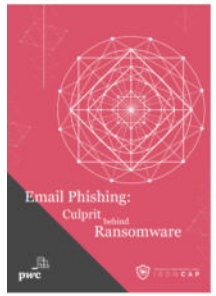
pwc

Tomorrow's Cyber Security, Today
IRONCAP



Rethinking Cybersecurity in a Quantum World

https://www.pwccn.com/en/issues/cybersecurity-and-privacy/rethinking-cybersecurity-in-a-quantum-world-jul2021.html



Email Phishing Culprit behind Ransomware

https://www.pwccn.com/en/issues/cybersecurity-and-privacy/email-phishing-culprit-behind-ransomware-apr2022.html

Tomorrow's Cyber Security, Today
IRONCAP

Summary

- ❑ Q-Day has arrived – no time to wait
- ❑ Everything needs to be quantum-safe (e.g. financial transactions, health care, IoT, general cybersecurity, email, remote access, etc.)
- ❑ Some pioneer Post-quantum end-user products can be found in the market already (e.g. email security, blockchain, remote access, etc.)

For more information: Visit Our Booth for live-Demo

www.ironcap.ca | www.01com.com
+1 905-795-2888 (tel)
+1 800-668-2185 (toll-free)
Sales@ironcap.ca

Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTAsia