The Quantum Vault
Custody of Digital Assets

Bruno Huttner
ID Quantique

Seattle; November 2019
Agenda:

- Why?
  Need custody of digital assets
- How?
  The principle of the quantum vault
- When?
  Implementation with OpenQKD project
- Conclusion
Why?
Are we talking about real money?

First real transaction in 2010: 10’000 ᶾ’s =

Today (2019): 1 ᶾ = 1’000 X
New ecosystem: the Exchanges: 🏷 ↔ $ and others

→ Crypto is now real money

### Top 100 Cryptocurrencies by Market Capitalization

<table>
<thead>
<tr>
<th>Cryptocurrencies</th>
<th>Exchanges</th>
<th>Watchlist</th>
<th>Market Cap</th>
<th>Price</th>
<th>Volume (24h)</th>
<th>Circulating Supply</th>
<th>Change (24h)</th>
<th>Price Graph (7d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td></td>
<td>$144,541,514,031</td>
<td>$8,048.50</td>
<td>$17,521,563,553</td>
<td>17,958,812 BTC</td>
<td>-4.16%</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td></td>
<td>$17,518,746,755</td>
<td>$162.36</td>
<td>$7,213,479,184</td>
<td>107,902,324 ETH</td>
<td>-3.89%</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>XRP</td>
<td></td>
<td>$10,293,774,365</td>
<td>$0.238945</td>
<td>$1,317,159,671</td>
<td>43,080,011,224 XRP</td>
<td>-2.84%</td>
<td></td>
</tr>
</tbody>
</table>

© 2019 ID Quantique SA, Switzerland | page 5
The bitcoin blockchain is built from:

• A network of computers
• A set of rules (Opensource SW)
• **Transactions**
• A blockchain linking blocks of transactions
• A distributed ledger: each PC in the network contains the same blockchain
• A network of miners, bookkeepers and regulators
A simple transaction: Alice sends 1 ₿ to Bob

**Alice**: generates key pair:
- \( \text{Pri}(A) \) (for signing)
- \( \text{Pub}(A) \) (for verification)

and calculates: \( \text{Add}(A) = \text{Hash} [\text{Pub}(A)] \)

<table>
<thead>
<tr>
<th>Initial BC:</th>
<th>( \text{Add}(A): 1 , \text{₿} )</th>
</tr>
</thead>
</table>
| Transaction: | • Text: [ send 1 ₿ from \( \text{Add}(A) \) to \( \text{Add}(B) \)]  
• \( \text{Pub}(A) \)  
• Signs with \( \text{Pri}(A) \) |
| Final BC: | \( \text{Add}(A): 0 \)  
\( \text{Add}(B): 1 \, \text{₿} \) |

Note: red = top secret; blue = keep secret until transaction; green = publish on the BC
Current storage solutions

- Major pain point of blockchain technology: **Storage of Private Keys**
  
  Private keys need to be stored in tamper proof, reliable and protected systems and yet be available upon request;

- Current solutions (with some issues...):
  - On-line wallet (ownership, trust)
  - Dedicated HW wallet (loss, destruction)
  - Vault – HSM (trust, backup)

  ➔ Need new solutions for high-value private keys
How?
The technology behind the quantum vault

- **Generation of the keys**
  - Real randomness: Use Quantum RNG

- **Storage**
  - Keys split in several elements with Shamir Secret Sharing
  - Distribution these elements to distant locations with QKD
  - Information Theoretical Security: no future computational attack possible

- **Access**
  - Complete separation between access & storage
  - Can use banking-grade access control
The technology behind the quantum vault

Key Management Node

QRNG

HSM

KEYS

KEY SPLIT

QKD LINK

QKD LINK

QKD LINK

Key Storage Node 1

Key Storage Node 2

Key Storage Node 3

The Quantum Vault
Main advantages

- **Unconditional security** thanks to the joint use of QRNG and two Information Theoretic Secure protocols:
  - Keys split with Shamir secret sharing protocol
  - and QKD;
- **Backup without duplication:** Keys are never in their complete form in the HSMs (Key storage or backup nodes);
- **High availability** of the keys for future transactions.
When?
The OpenQKD project started in September.

“Our vision is that classical and quantum communications will jointly ensure the ICT needs of European governments, service industries (e.g. health, finance), businesses and citizens.”

- 38 partners from academia and industry
- Funding: 15 M€
- Includes testbeds in Geneva
The OpenQKD testbed in Geneva

Partners for the quantum vault in Geneva:

- Services Industriels de Genève (SIG) for the fiber infrastructure
- Mt Pelerin (new bank on blockchain, based in Geneva) for the SW layer
- IDQ for the QKD systems
- Several partners for the endpoints: (CERN, Equinix, Safehost, SIG)

PoC deployment will start in December, and last over 2020

Final goal: full deployment of the technology!
Potential customers of the Quantum Vault:

- Global custodians (banking industry);
- Central banks;
- Government agencies;
- Crypto currencies exchanges and vaults;
- Utilities and critical infrastructure providers;
- Large corporations.
Conclusion: the value of the Quantum Vault

- Practical application mixing QKD with algorithms
- QKD used in a novel way for secure storage
- Solves a significant issue in Blockchain
- Real-world implementation in progress