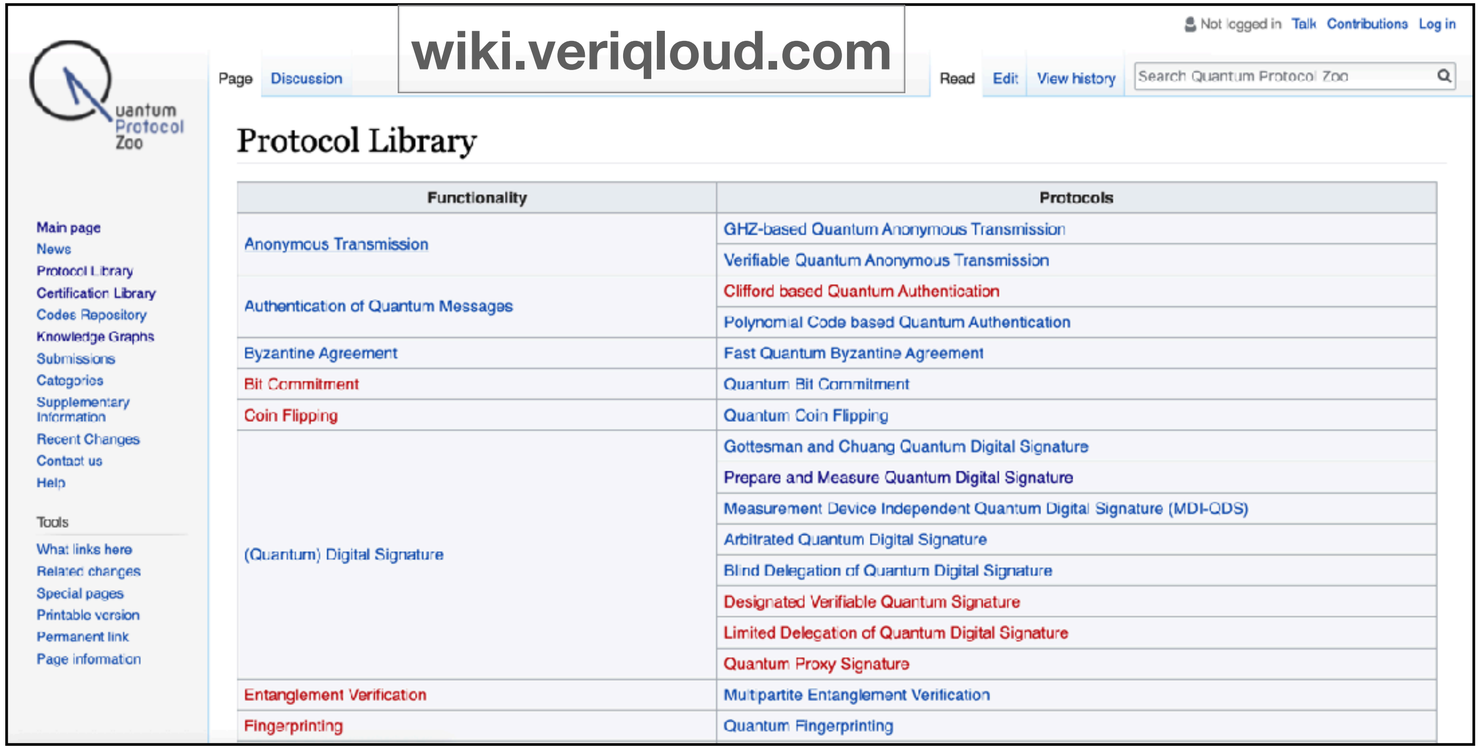
Future applications for a Quantum Internet

VeriQloud: building trust in the quantum era

Marc Kaplan - ITU - 26/05/2021

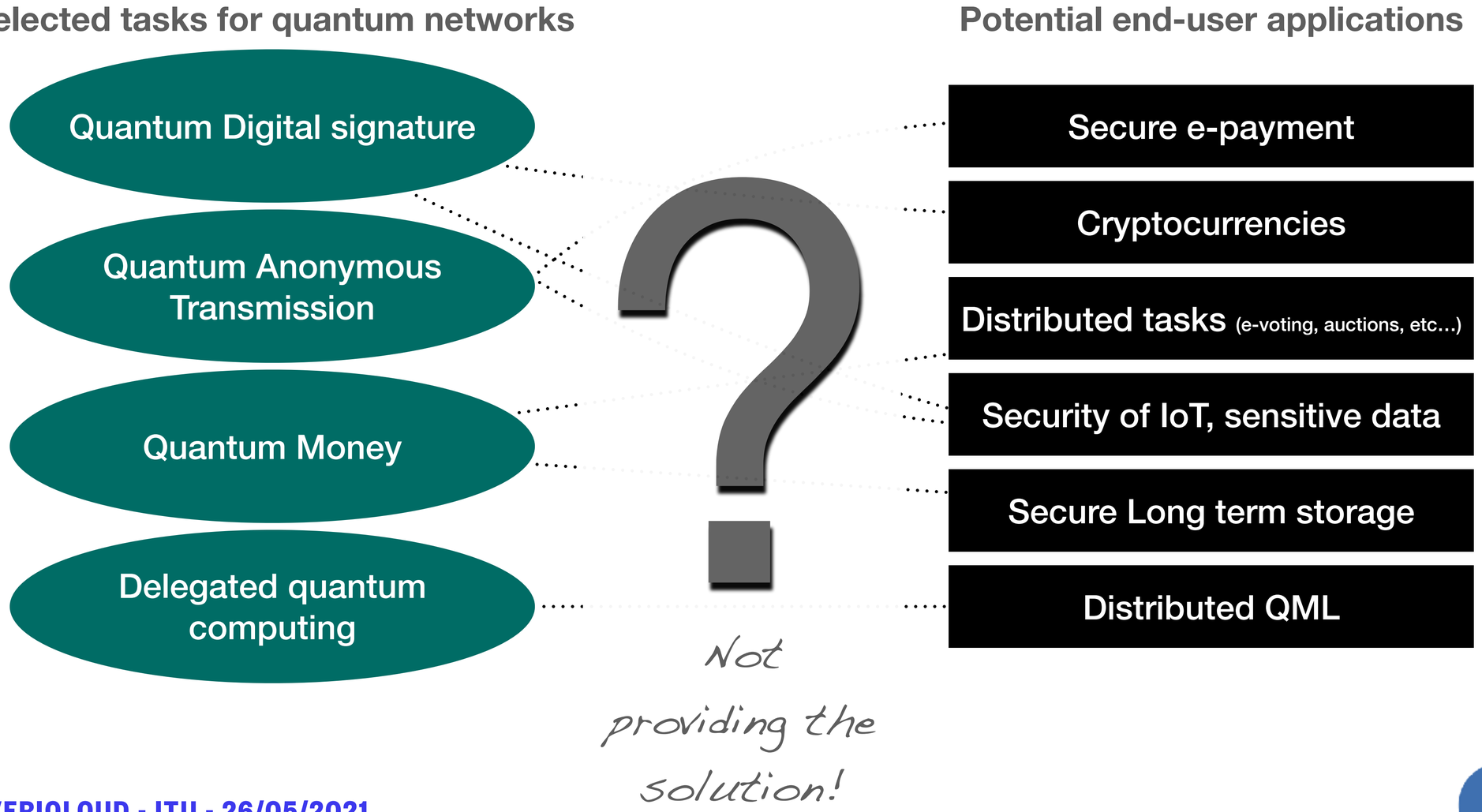
Applications of quantum communications

Collect, list, benchmark



QUANTUM INTERNET ALLIANCE

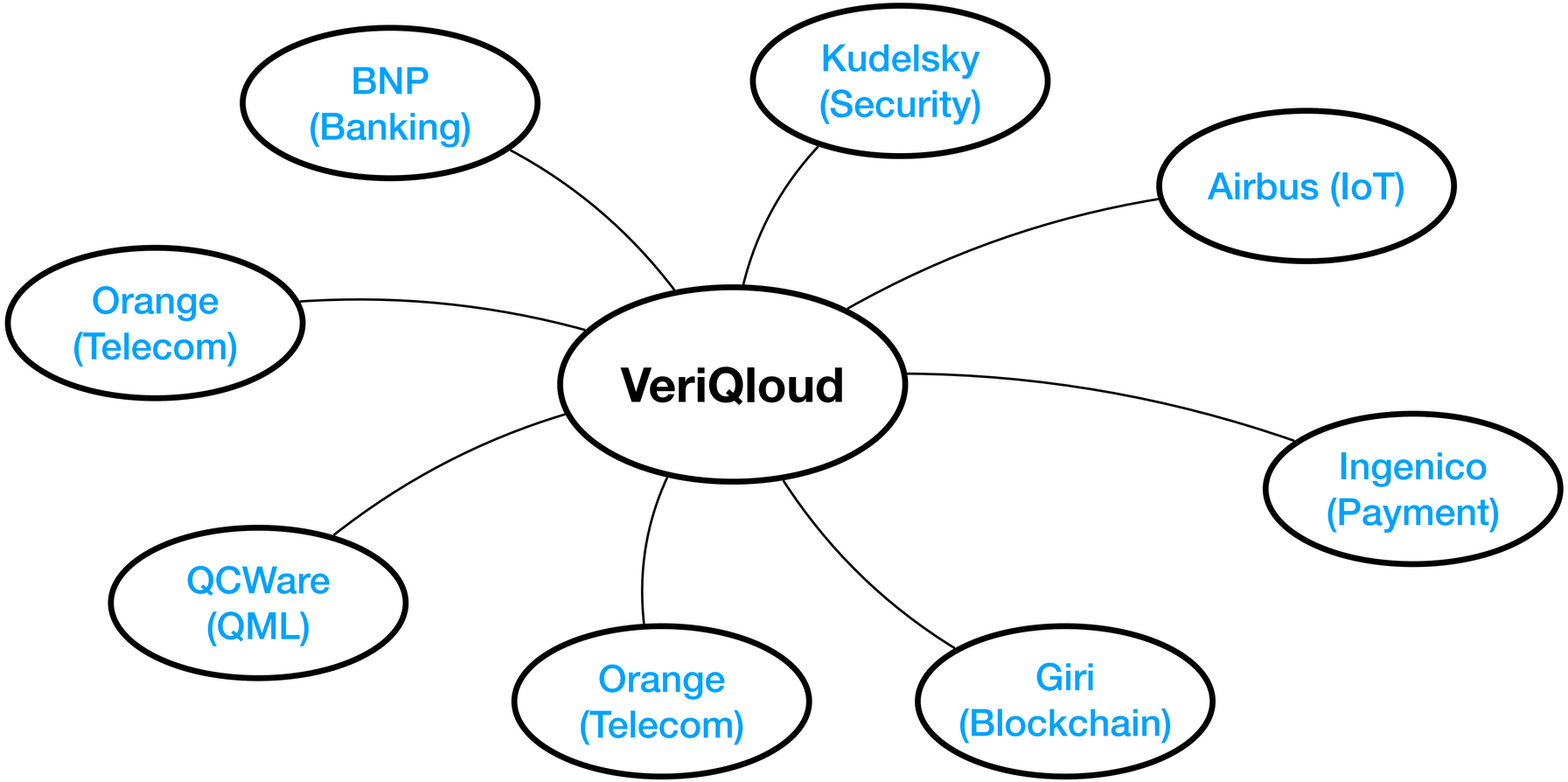
Matching tasks with end-users



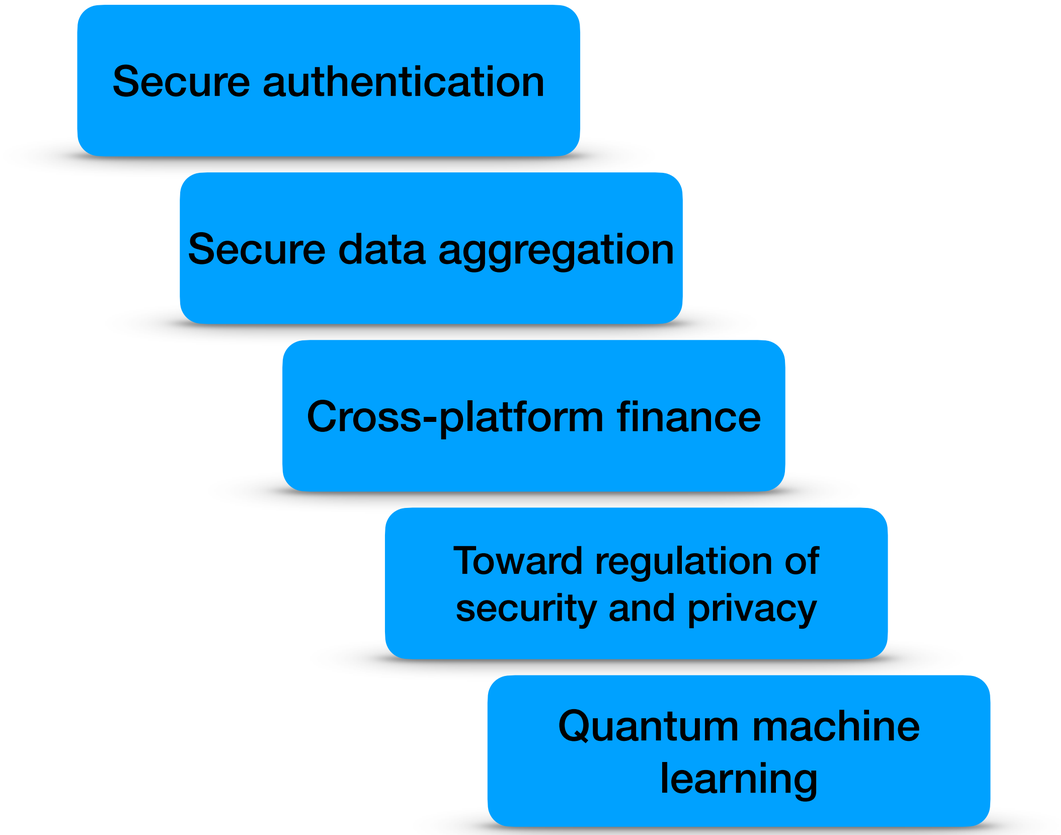
Selected tasks for quantum networks

Quantum Digital signature	Signing classical messages with quantum bits
Quantum Anonymous Transmission	Sending messages on a quantum network without revealing the sender
Quantum Money	Unforgeable and unclonable tokens object that could be circulated among parties
Delegated quantum computing	Encrypting programs and executing them remotely on a quantum computer

Selected end-users interviews



Identified use cases



Secure identifications

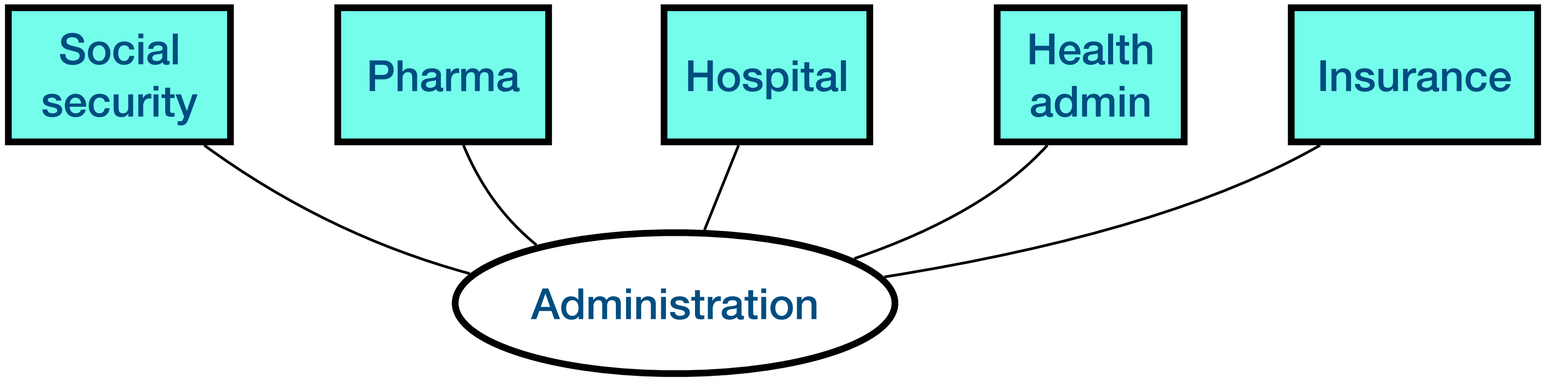
Security, IoT, Payment

Identified issues
More and more connected systems
Dynamic environment
Identity management in these environment
New threats: credentials get copied, stolen, etc…

Potential solutions
Long-term security of Quantum Digital Signatures
Unforgeability, revocability with Quantum tokens

Data Aggregation

Distributed computing, blockchain

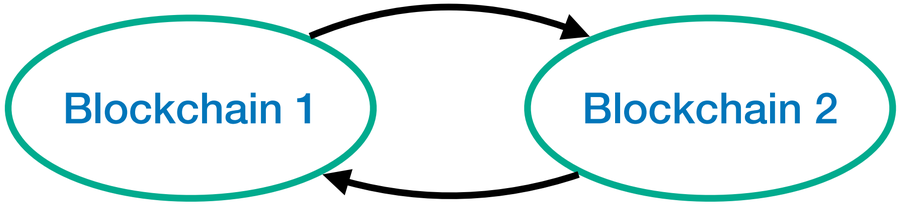


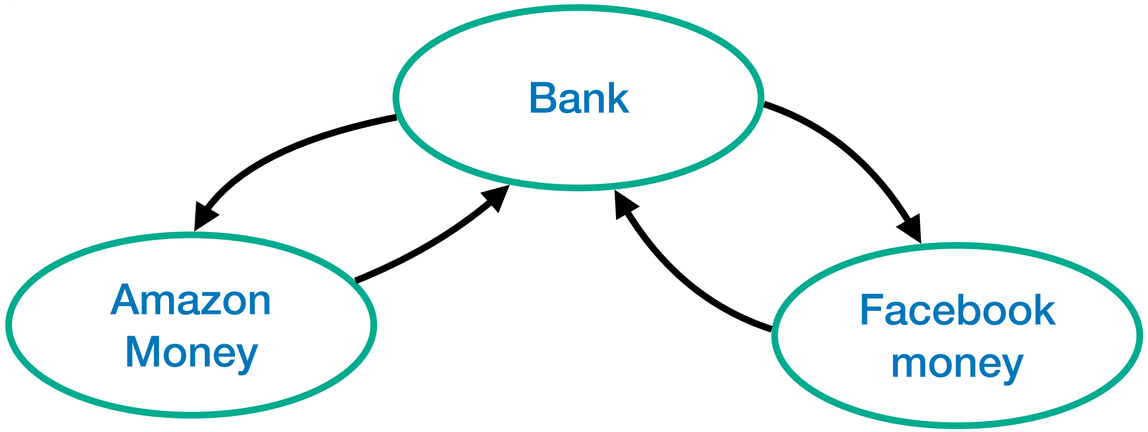
Identified issues
More data, more responsibility, more needs for security
Participants don’t trust each other
Eavesdropping

Potential solutions
Hiding sources with Anonymous transmission
Distributed protocols
Long-term secure storage

Cross platform operations

Blockchain, Banking, Payment, DeFi





Identified issues
Ensuring asset's liquidity and security without 3rd parties
Banking always requires more security
Identity management for platform money systems

Potential solutions
QSwift system based on quantum money
Unforgeable tokens for cross-chain operations avoiding double-spending

Security through Regulation

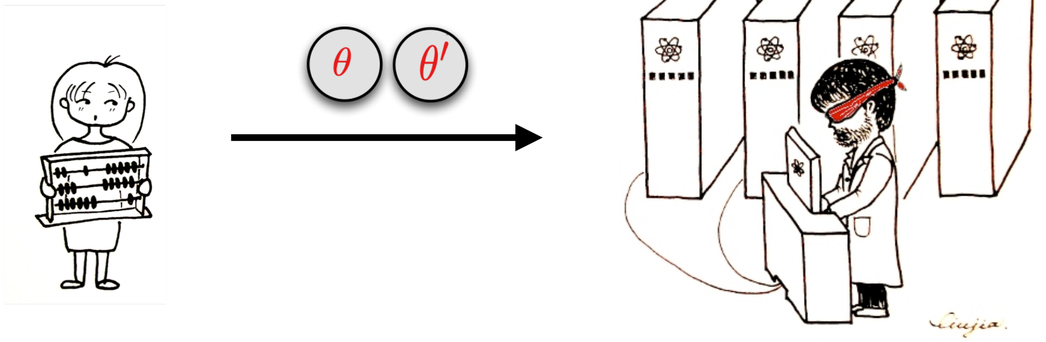
Transverse

Identified issues
Data protection
RGDP Compliance
Enforcing human rights

Potential solutions
Long-term secure storage
Anonymous transmission
Distributed protocols

Quantum Machine Learning

Classical communication: No security



Quantum communication: Sever does not learn anything about algorithms, inputs or outputs

Identified issues
Insecurity of quantum cloud computing
No trust in quantum operators
Data sharing is highly regulated

Potential solutions
Blind quantum computing
Verifiable quantum computing

Challenges for future applications

- **Secure authentication** — Challenge n°1: Design an authentication system using unclonable quantum tokens
- **Secure data aggregation** — Challenge n°2: Make privacy by-design long-term secure with the help of quantum resources
- **Cross-platform finance** — Challenge n°3: Design a Quantum SWIFT system
- **Toward regulation of security and privacy** — Challenge n°4: Design secure cross-chain operations using unforgeable quantum tokens
- **Quantum machine learning** — Challenge n°5: Use the noise of quantum networks to make quantum machine learning algorithms private by-design

Conclusion

- More data means more opportunities, but also more responsibilities
- Quantum era consists in challenges and opportunities
- Designing applications of quantum communication requires research

Reach me:
kaplan@veriqloud.com
www.linkedin.com/in/kapmarc/