

# Future applications for a Quantum Internet

*VeriQloud: building trust in the quantum era*



# Applications of quantum communications

## Collect, list, benchmark

Not logged in [Talk](#) [Contributions](#) [Log in](#)

wiki.veriqloud.com

Page [Discussion](#) [Read](#) [Edit](#) [View history](#)

### Protocol Library

Functionality	Protocols
Anonymus Transmission	<a href="#">GHZ-based Quantum Anonymous Transmission</a>
	<a href="#">Verifiable Quantum Anonymous Transmission</a>
Authentication of Quantum Messages	<a href="#">Clifford based Quantum Authentication</a>
	<a href="#">Polynomial Code based Quantum Authentication</a>
Byzantine Agreement	<a href="#">Fast Quantum Byzantine Agreement</a>
<a href="#">Bit Commitment</a>	<a href="#">Quantum Bit Commitment</a>
<a href="#">Coin Flipping</a>	<a href="#">Quantum Coin Flipping</a>
(Quantum) Digital Signature	<a href="#">Gottesman and Chuang Quantum Digital Signature</a>
	<a href="#">Prepare and Measure Quantum Digital Signature</a>
	<a href="#">Measurement Device Independent Quantum Digital Signature (MDI-QDS)</a>
	<a href="#">Arbitrated Quantum Digital Signature</a>
	<a href="#">Blind Delegation of Quantum Digital Signature</a>
	<a href="#">Designated Verifiable Quantum Signature</a>
	<a href="#">Limited Delegation of Quantum Digital Signature</a>
	<a href="#">Quantum Proxy Signature</a>
	<a href="#">Multipartite Entanglement Verification</a>
	<a href="#">Quantum Fingerprinting</a>
<a href="#">Entanglement Verification</a>	<a href="#">Multipartite Entanglement Verification</a>
<a href="#">Fingerprinting</a>	<a href="#">Quantum Fingerprinting</a>



# Matching tasks with end-users

Selected tasks for quantum networks

- Quantum Digital signature
- Quantum Anonymous Transmission
- Quantum Money
- Delegated quantum computing

Potential end-user applications

- Secure e-payment
- Cryptocurrencies
- Distributed tasks (e-voting, auctions, etc...)
- Security of IoT, sensitive data
- Secure Long term storage
- Distributed QML

?

*Not providing the solution!*

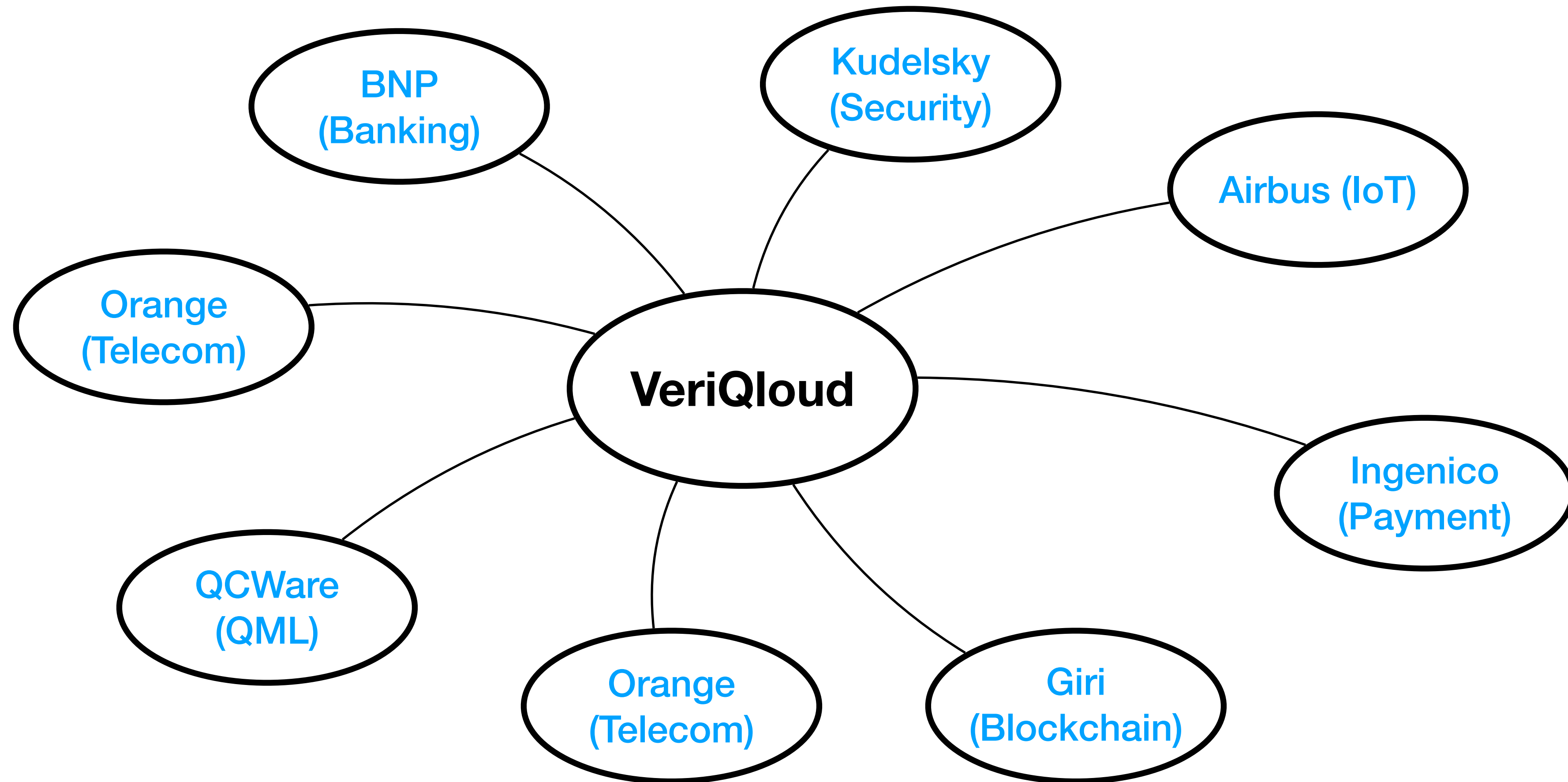


# Selected tasks for quantum networks

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 authentication

Secure data aggregation

Cross-platform finance

Toward regulation of  
security and privacy

Quantum machine  
learning



# Secure identifications

## Security, IoT, Payment

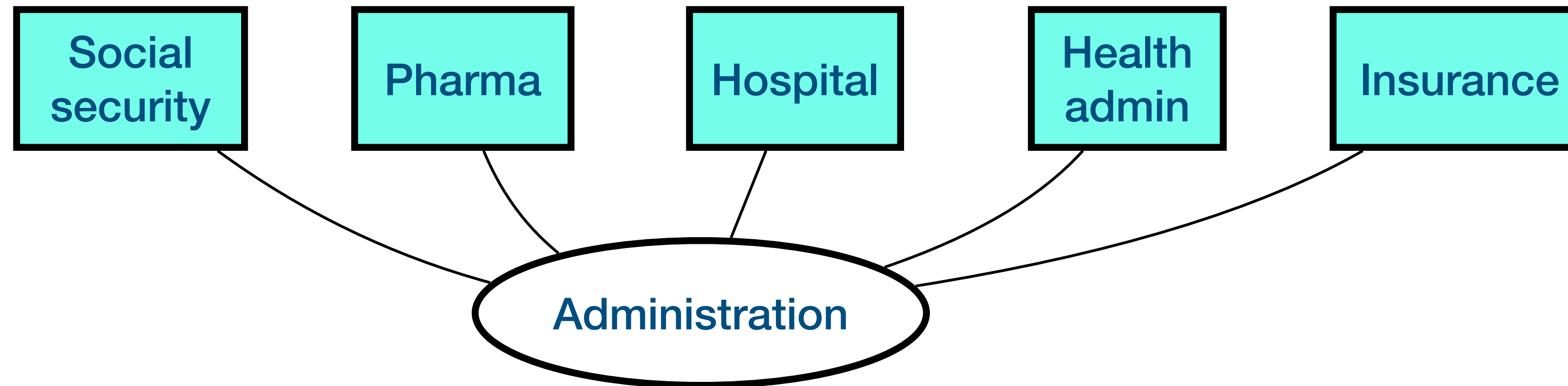
Identified issues
More and more connected systems
Dynamic environment
Identity management in these environment
New threats: credentials get copied, stolen, etc...

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

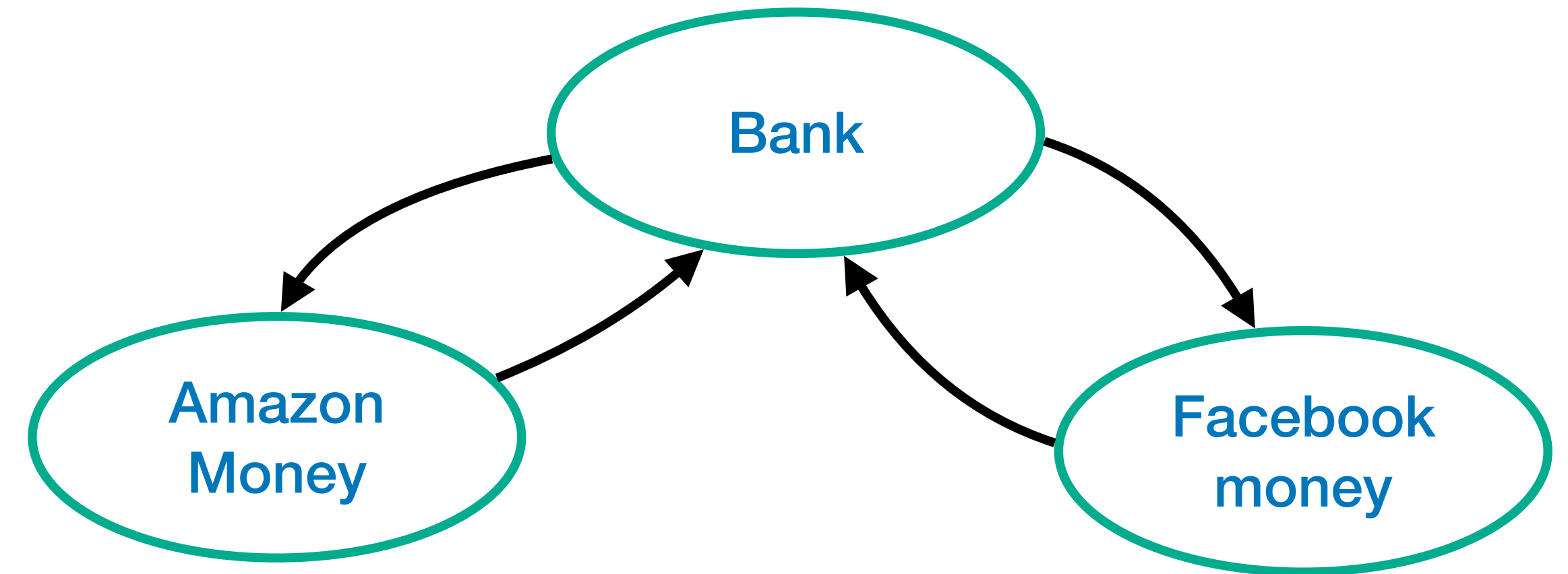
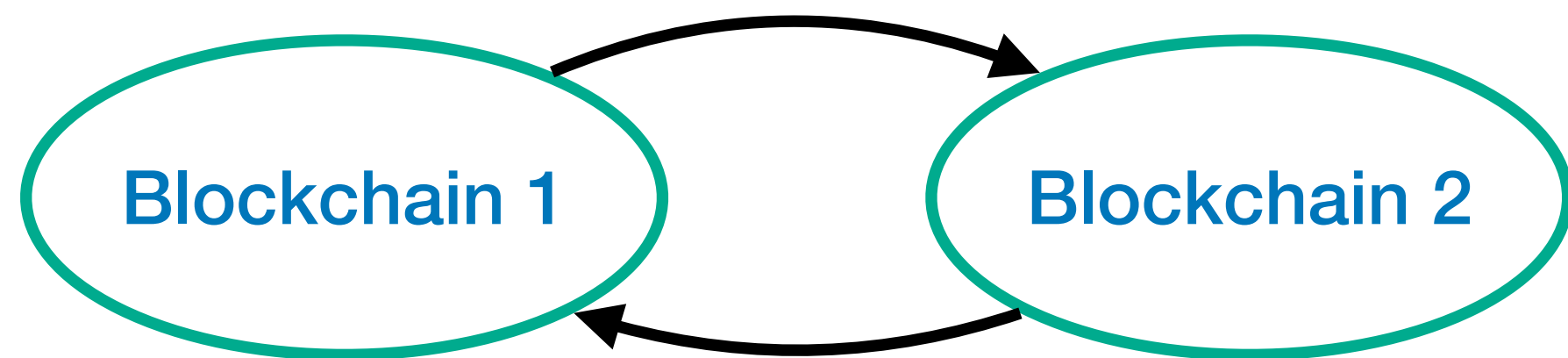
Potential solutions
Hiding sources with Anonymous transmission
Distributed protocols
Long-term secure storage





# 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

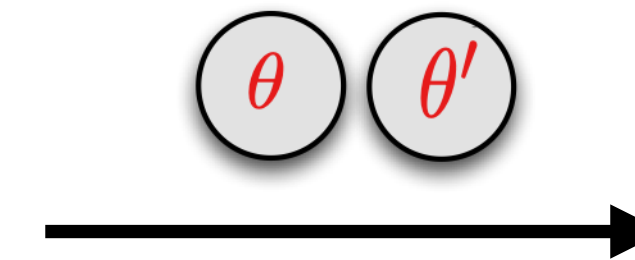
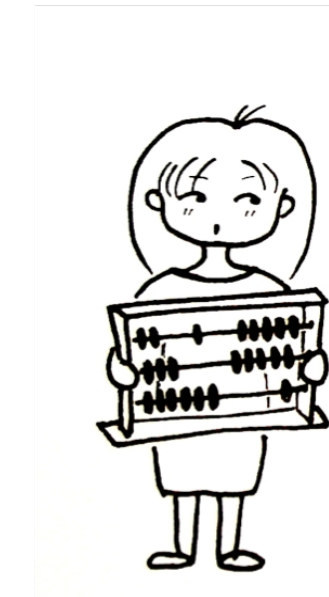
Potential solutions
Long-term secure storage
Anonymous transmission
Distributed protocols



# Quantum Machine Learning



Classical communication: No security



Quantum communication: Server 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@veriqcloud.com](mailto:kaplan@veriqcloud.com)

[www.linkedin.com/in/kapmarc/](https://www.linkedin.com/in/kapmarc/)

