Guidelines for building crypto-agility and migration for quantum-safe DLT systems

Fuwen Liu
China Mobile

Threats to distributed ledger technology (DLT) systems

- **Currently most popular DLT systems deploy the conventional crypto-graphic algorithms to enable secure transactions.**
  - Cryptographic hash algorithms for the integrity of a transaction.
  - Digital signature algorithms for the authorization of a transaction.
  - Optionly encryption algorithms for the confidentiality of a transaction.

- **CRQC puts most currently used cryptographic algorithms at risk**
  - The security strength of a symmetric cryptographic algorithm will be reduced to half due to Grover's quantum algorithm.
  - Many commonly used asymmetric cryptographic algorithms, such as RSA and elliptic curve based algorithms will be broken due to Shor's quantum algorithm.

➡ **There is a need to devise quantum-safe DLT systems, which employ quantum-safe cryptograhic algorithms**

Crypto-agility is desired for quantum-safe DLT systems

- **Currently a few DLT systems has deployed the quantum-safe cryptographic algorithms to defend agaisnt quantum computing attacks**
  - A set of quantum-safe cryptographic algorithms are fixed to be used
  - It is impossible to update the cryptographic algorithms

➡ **Once one deployed algorithm is broken, the whole system is compromised**

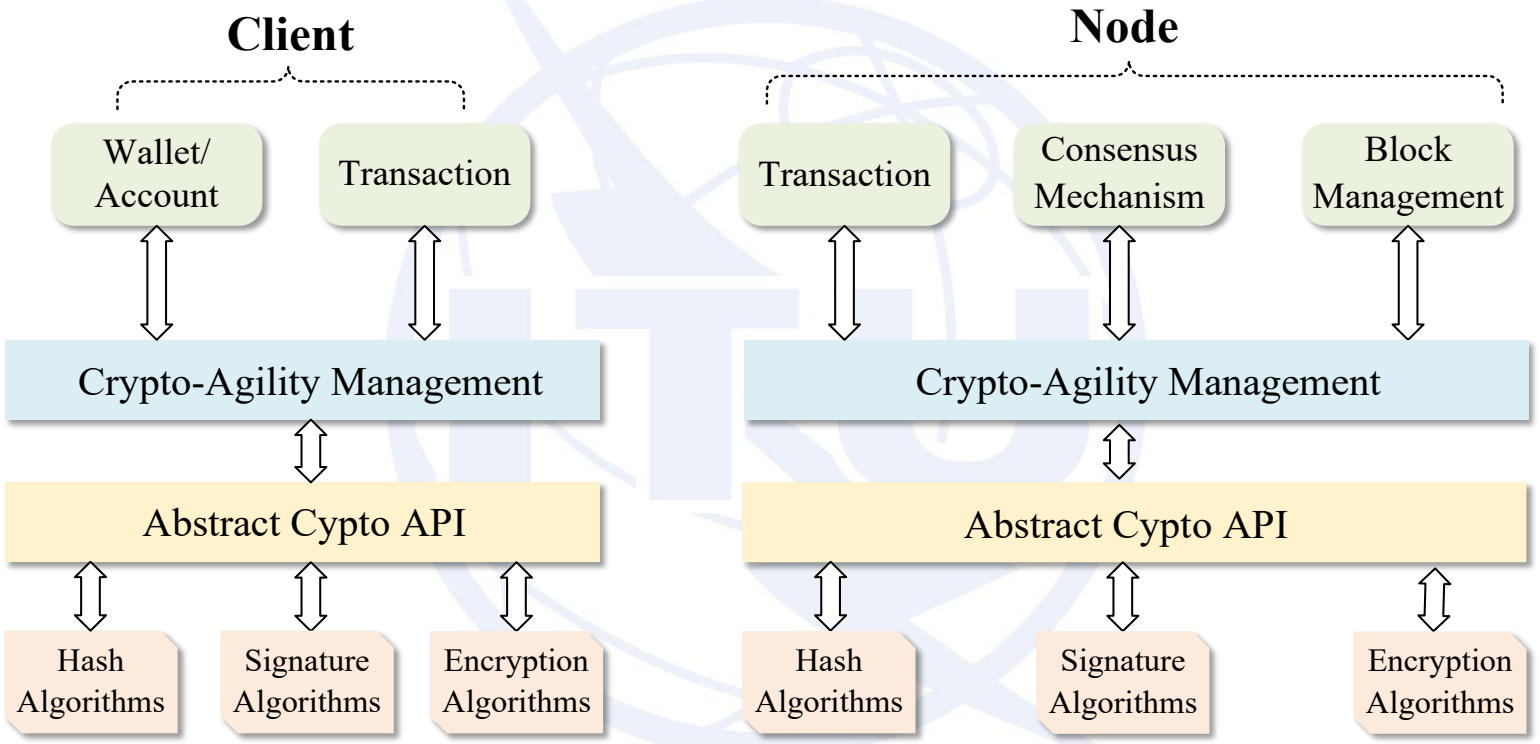
- **Reasons for the need of crypto-agility**
  - Weak confidence on PQC algorithms
  - Heterogeneous nodes and clients

Design principle of crypto-agility in DLT systems

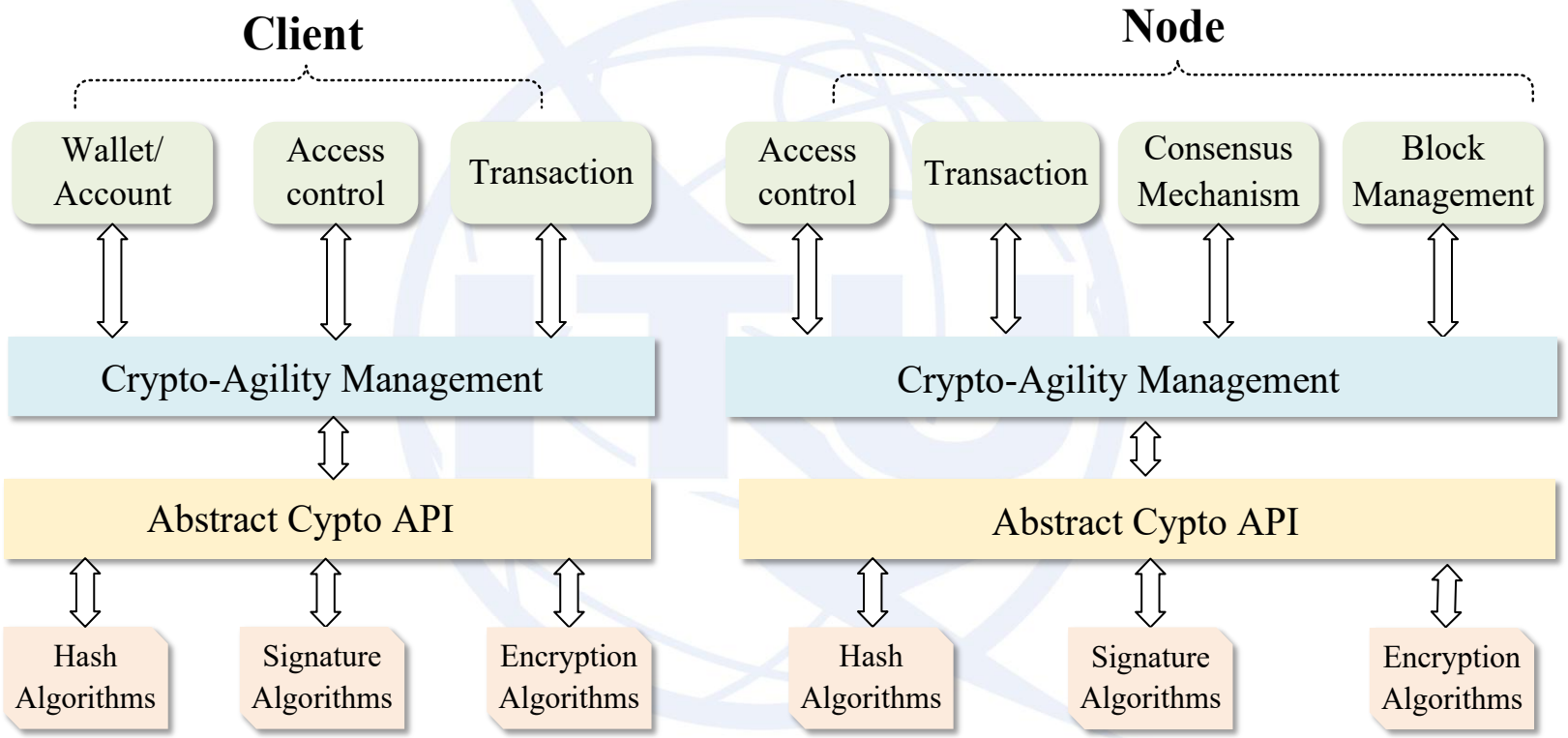
- **Crypto-agility refers to the capabilities needed to replace and adapt cryptographic algorithms while preserving security and ongoing operations**

- **Design principle**
  - Modular and agile architecture
  - Cryptographic abstraction and interoperability
  - Algorithm and parameter negotiation
  - Secure update and verification
  - Performance and resource adaptation
  - Cryptographic governance

Arichtecture of permissionless quantum-safe DLT system

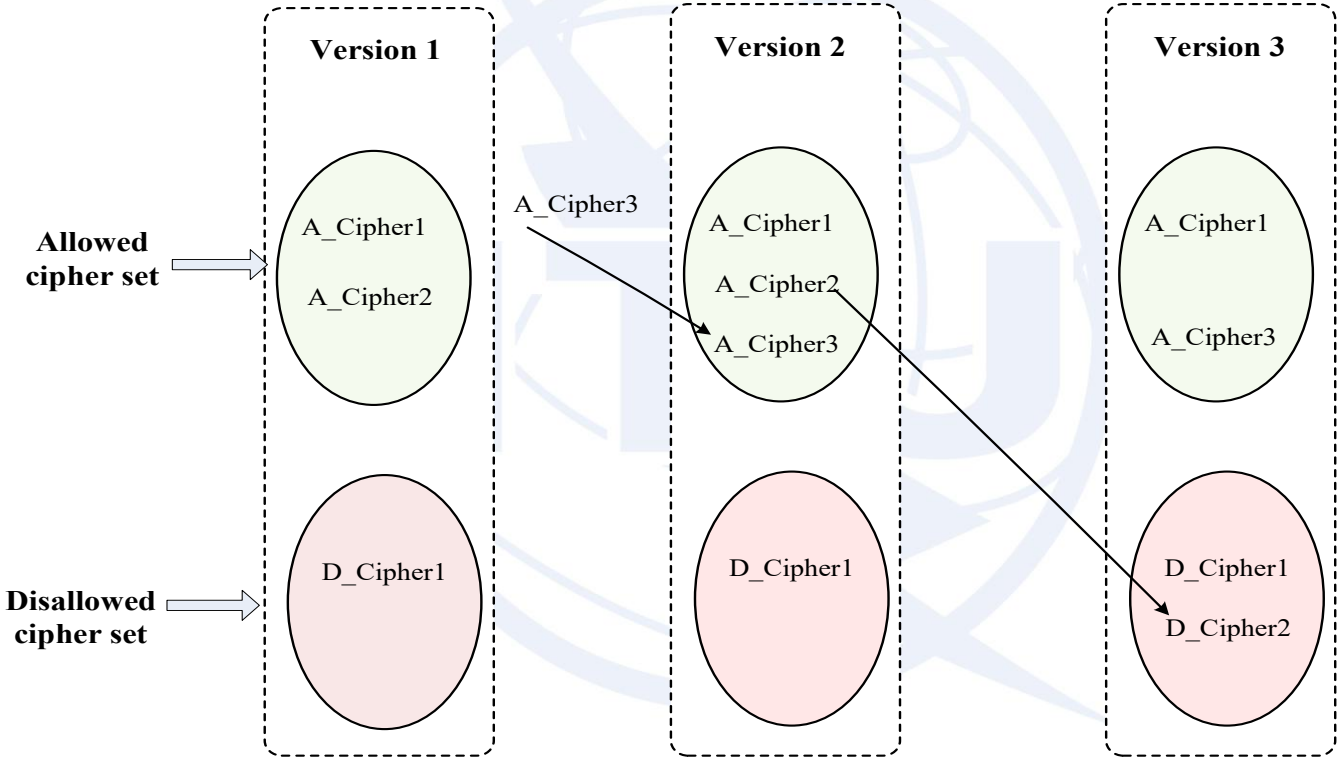


Arichtecture of permissioned quantum-safe DLT system



Realization of crypto-agility

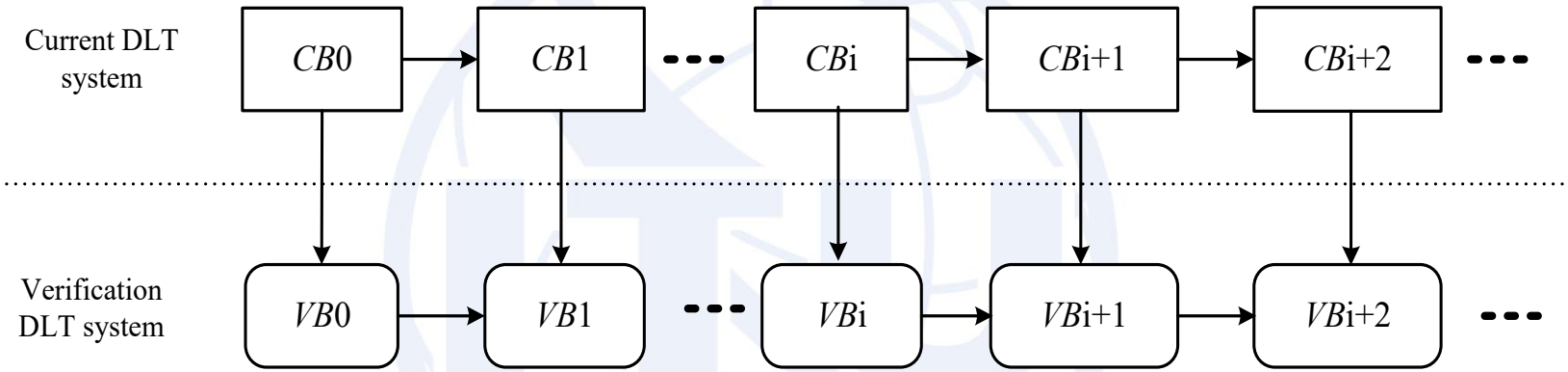
- Crypto-agility management module contains an allowed cipher set and an disallowed cipher set



- Interaction between the crypto-agility management module and various functional modules.

Issues have to be addressed for Migration (1/2)

- Integrity verification of data on the current DLT system

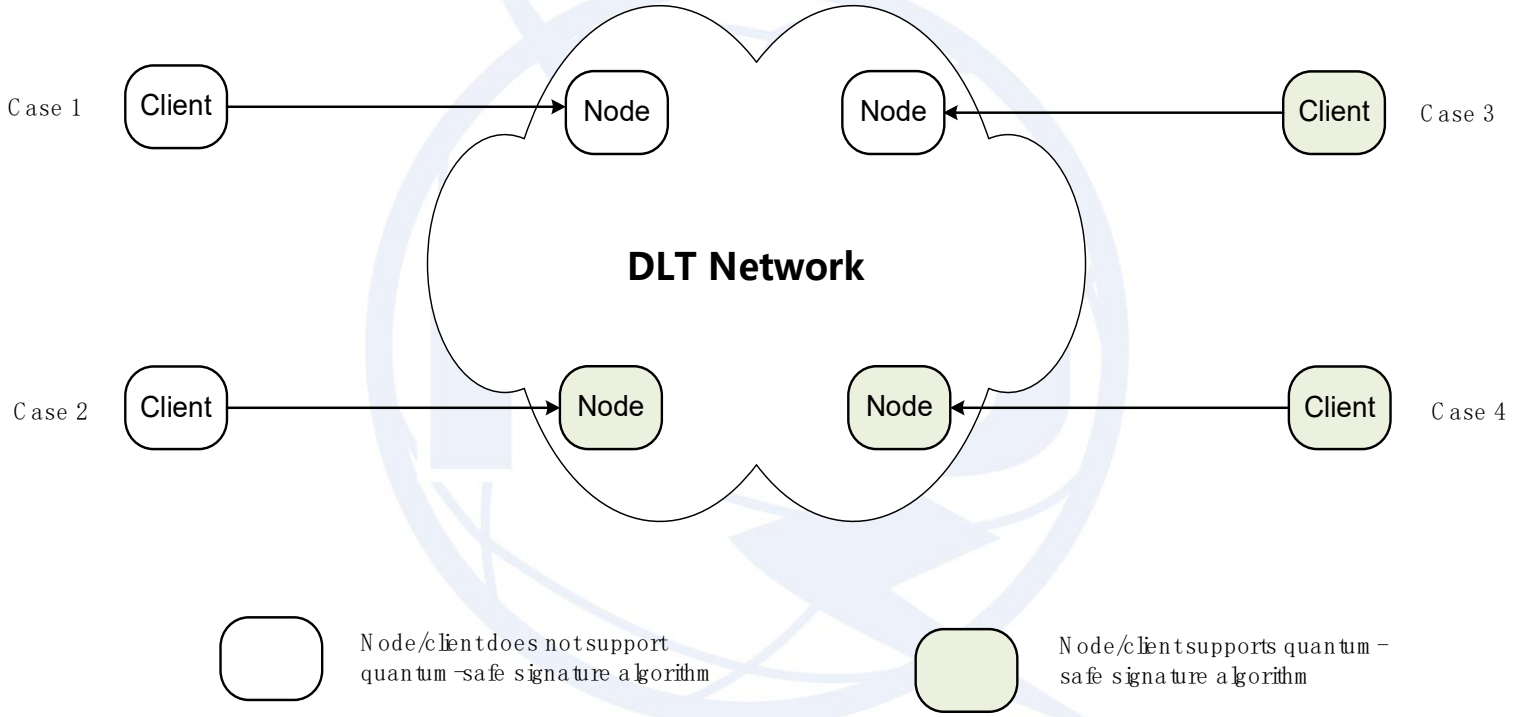


CB: Current block in current DLT system
VB: Verification block in verification DLT system

- The block body of the genesis block contains a description of NHF (nested hash function) to indicate which hash functions are used to form the NHF
- The body of each block is generated by using the NHF to hash the block header, the previous block and the block associated with this block on the current DLT system.

Issues have to be addressed for Migration(2/2)

- Asynchronous software update



- The client that does not support quantum-safe signature algorithms signs all information in a transaction by using the conventional signature algorithm.
- The client that supports quantum-safe signature algorithms signs all information in a transaction by using the hybrid signature method.

Overall migration plan

- Monitoring international PQC standards
- Inventory and risk assessment
- PQC algorithm and protocol choices
- Protocol and ledger upgrades
- Migration phasing
- Operational controls

Thank you