FINTECH ASSOCIATION

A closer look at the blockchain platforms

Masterchain - the first Russian legal blockchain platform and its capabilities

Anatoly Konkin
anatoly.konkin@fintechru.org

FINTECH ASSOCIATION

FINTECH ASSOCIATION

OUR MISSION

Technology

Designing and implementing new technological solutions to support the development of the Russian financial market

+

Digitalisation

Paving the way for the digitalisation of the Russian economy

WHAT WE DO

- Conducting research, analysing trends, and leveraging global best practices
- Coordinating the development of software, standards, platforms and protocols
- Representing and supporting our members
- Prioritising workstreams and focus areas
- Putting forth legislative initiatives
- Rolling out in-house projects and taking part in external ones
- Holding conferences and implementing educational projects and awareness campaigns

Masterchain - destributed ledger

Support smart contracts

Adjust role model

Based on Ethereum

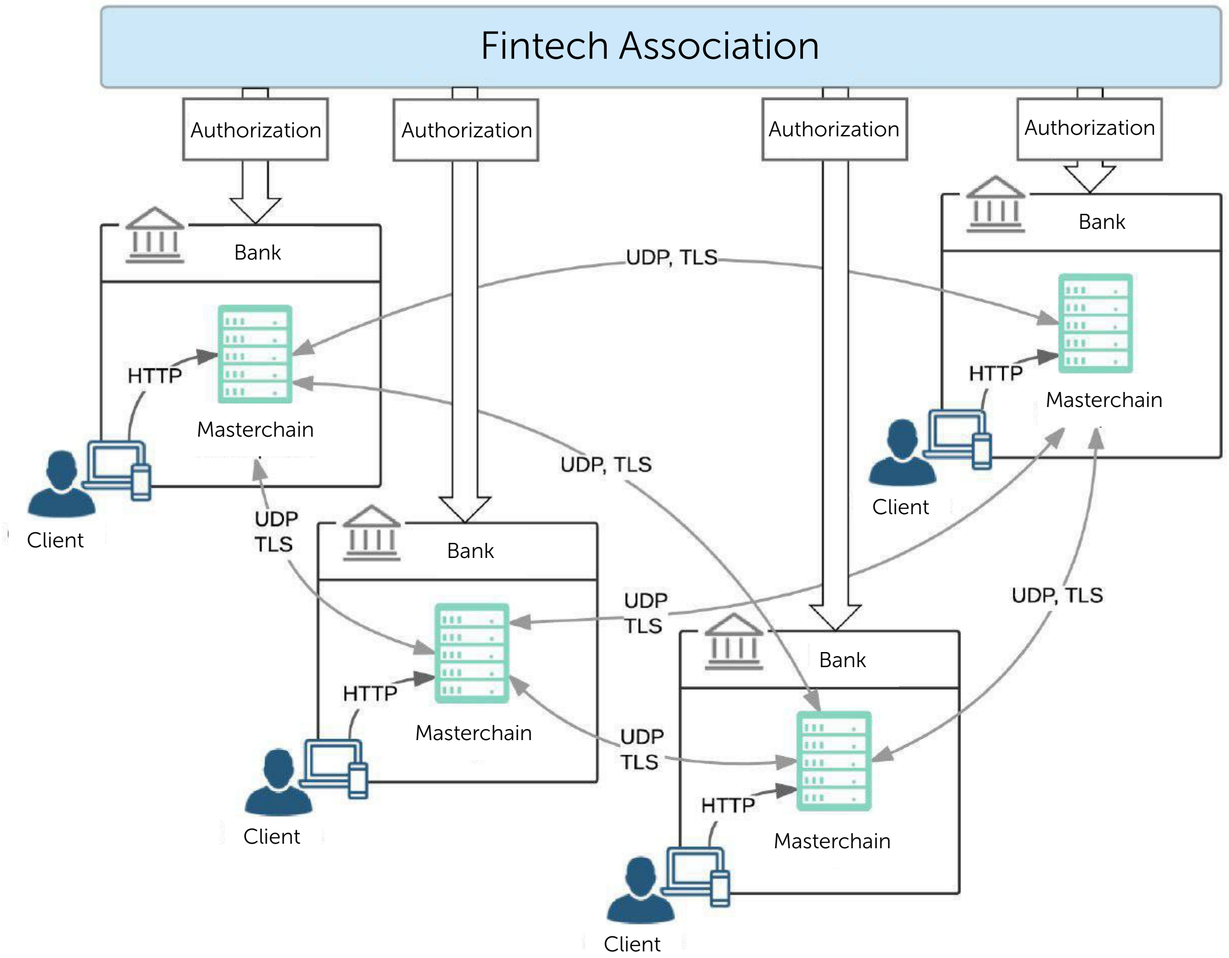
Core features:

- ✓ Custom Crypto algorithm.
- ✓ Managed access that allow private networks.

White paper:

http://fintechru.org/en/Masterchain_whitepaper_v1.1_en.pdf

Target Masterchain architecture



Administration (Fintech Association):

1. Coding and technical support.
2. Dispute resolution.
3. Licening of validating nodes.

Validating nodes:

1. Store and support.
2. Handle and spread transactions.
3. Add new blocks.
4. Create keys for new nodes.

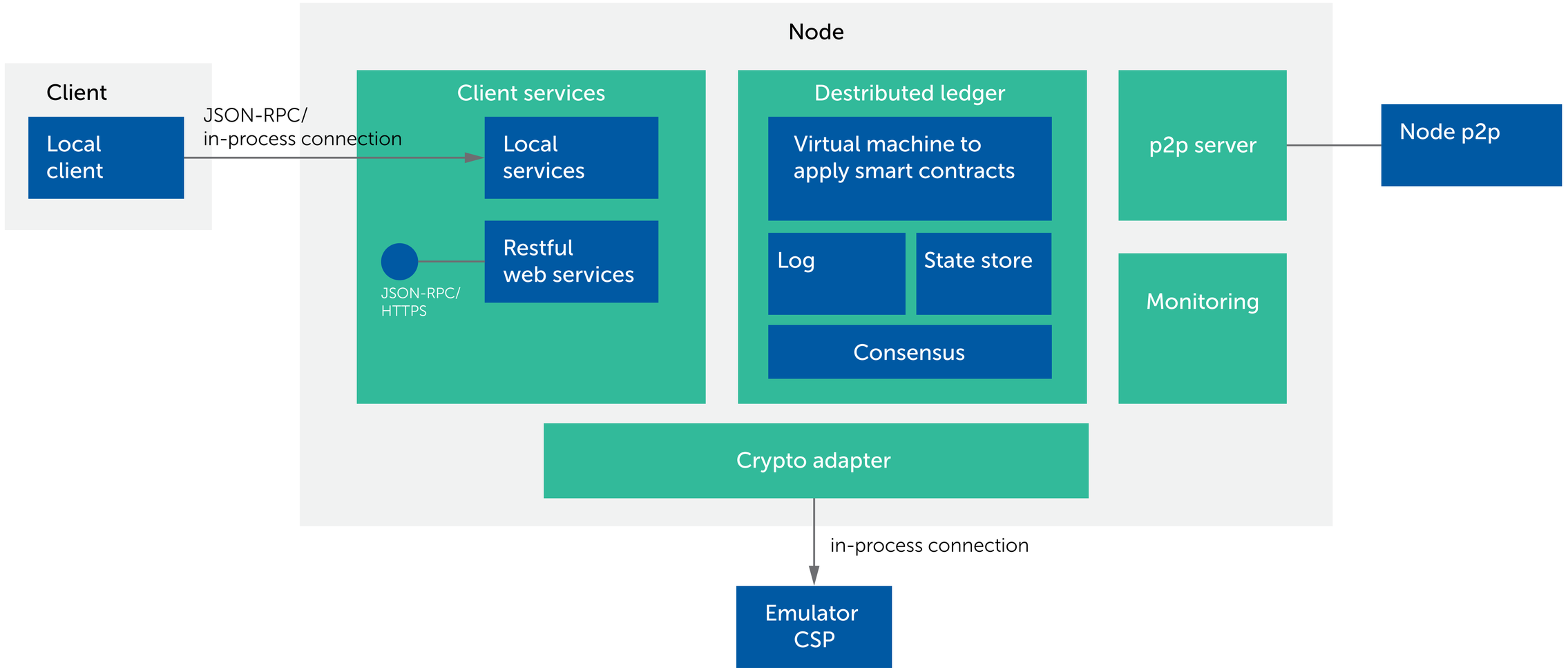
Non-validating nodes:

1. Store and support.
2. Handle and spread transactions.

Client:

1. Add new transactions.

Node: store and support, provide external API, implement Crypto adapter



Why custom crypto?

- **Only GOST crypto algorithms have legal power**
- **Only certified Crypto Service Providers have to be used**
- **Only few vendors of CSP. We used CryptoPRO CSP 4.0**

Masterchain certified cryptography

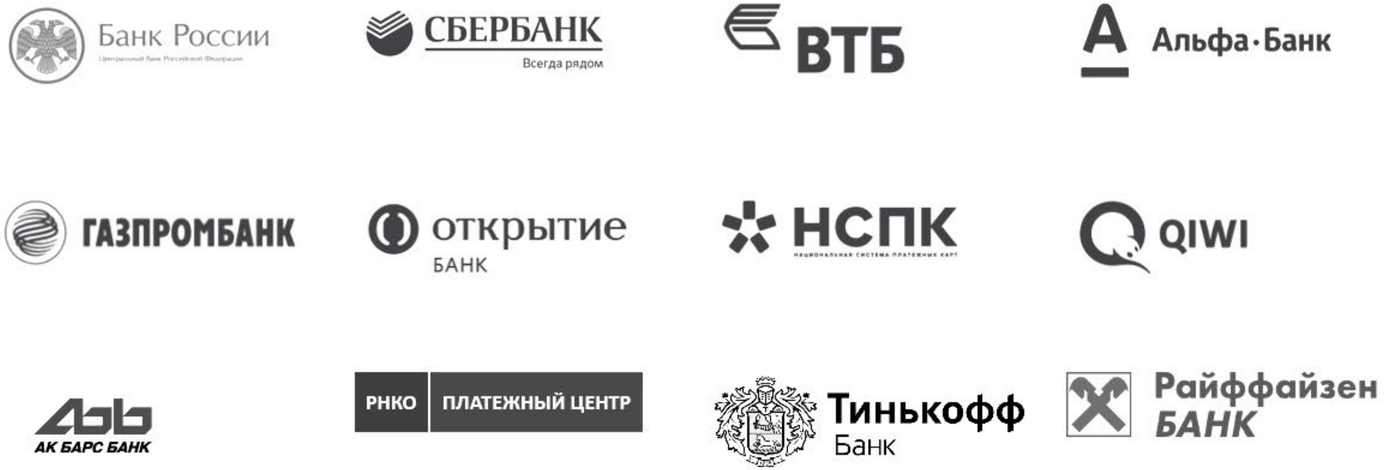
Ethereum	Masterchain	Mode
SHA256, SHA3	GOST R 34.11-2012 (Streebog)	256 bit
SHA3	GOST R 34.11-2012 (Streebog)	512 bit
ECDSA, secp256k1	GOST R 34.10-2012	256 bit curve, paramset A
Ecrecover	Ecrecover (Compressed signature) + Verify (GOST R 34.10-2012)	256 bit curve, paramset A
AES	GOST 28147-89 (Magma)	Key 256 bit, block size 128/64
RLPx-Encryption	Certified TLS	–

Current Masterchain goals

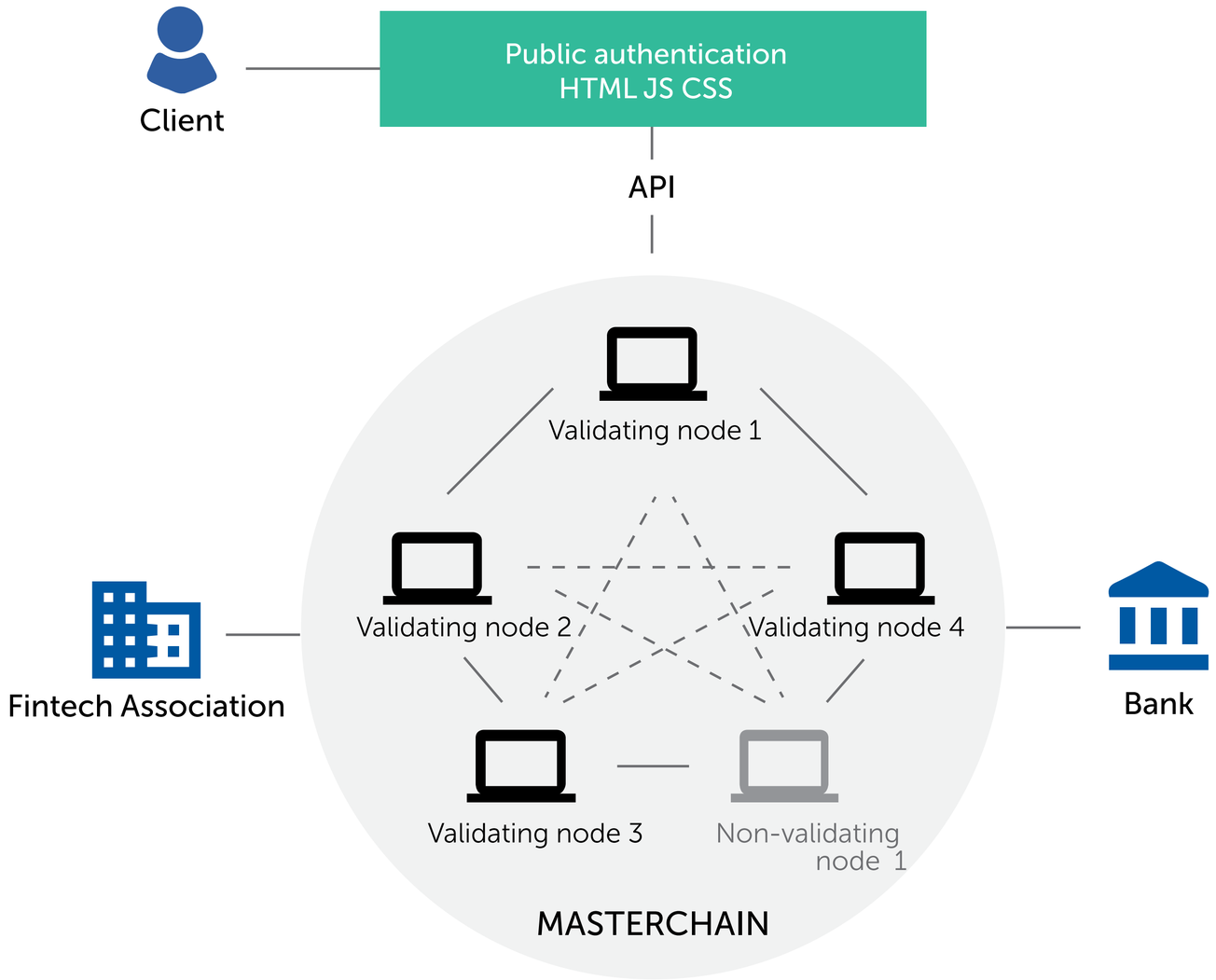
- Roll out financial scenarious (use cases) with members of Fintech Association.
- Improve scalability and reliability.
- Reduce costs and risks for financial transactions, accounting of securities ownership, and trading operations.
- Propose according legal regulations for destributed ledger technology.
- Develop new standarts for destributed ledger technology using embedded Russian cryptography.

Selected use cases

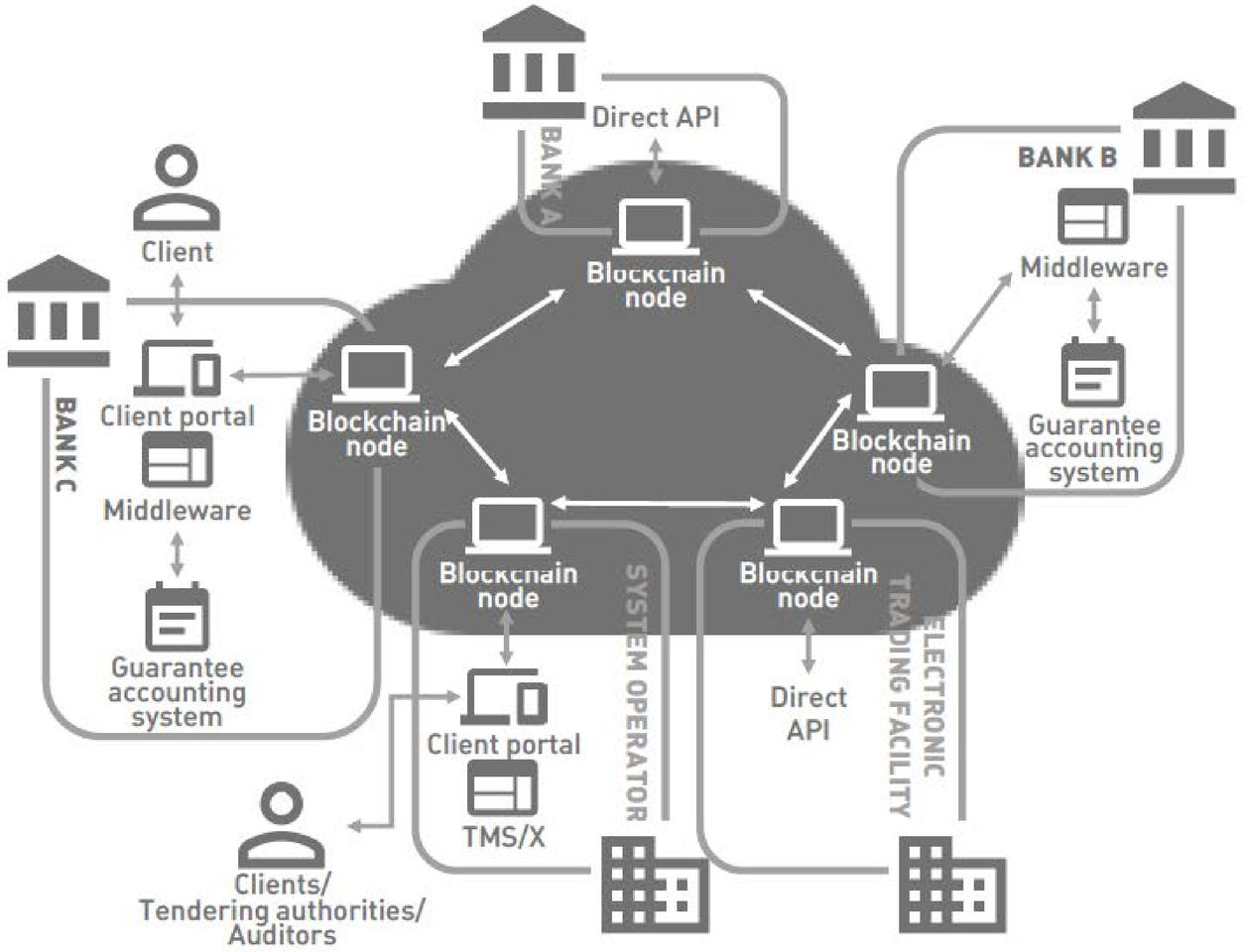
1. System for transfer of financial messages
2. Letter of credit
3. Bank guarantee
4. Mortgage
5. KYC (know your customer)



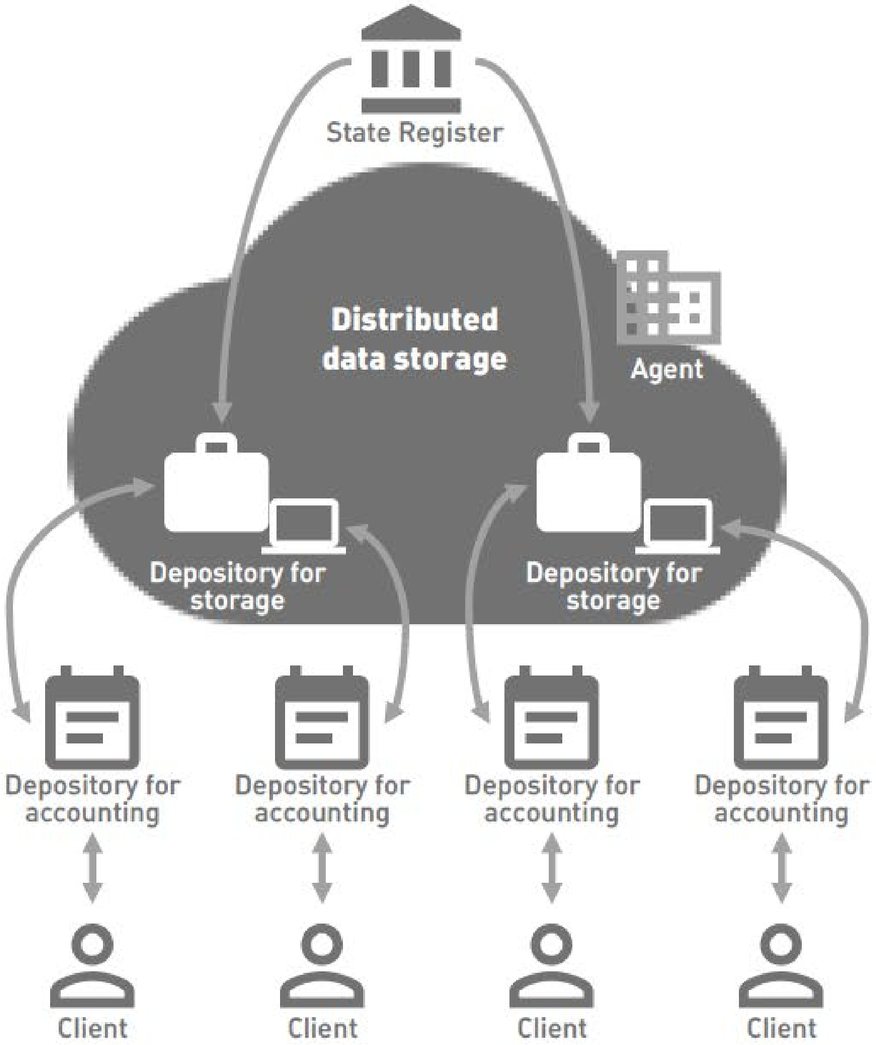
Masterchain provides public open authentication API methods



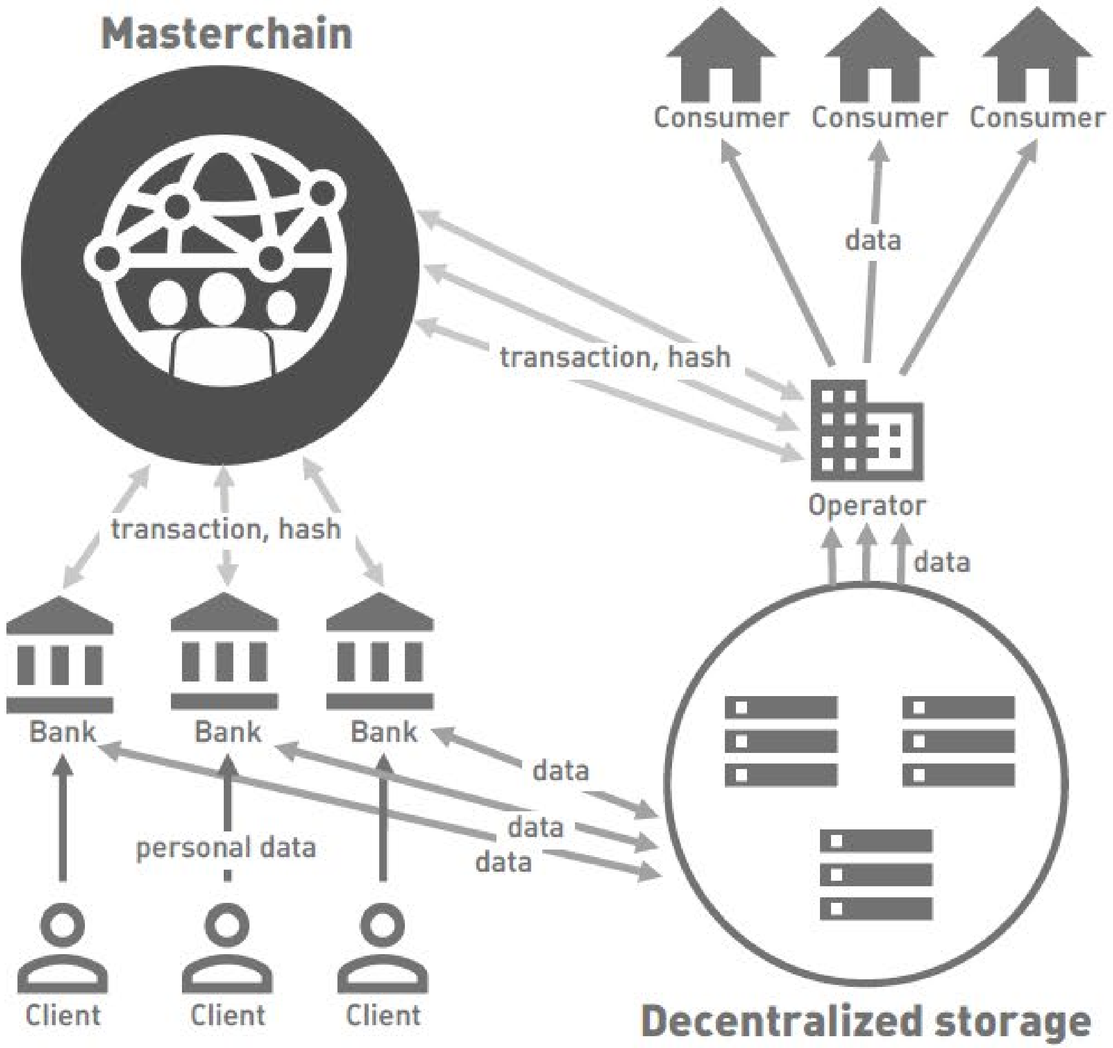
Use case example 1: Bank guarantee



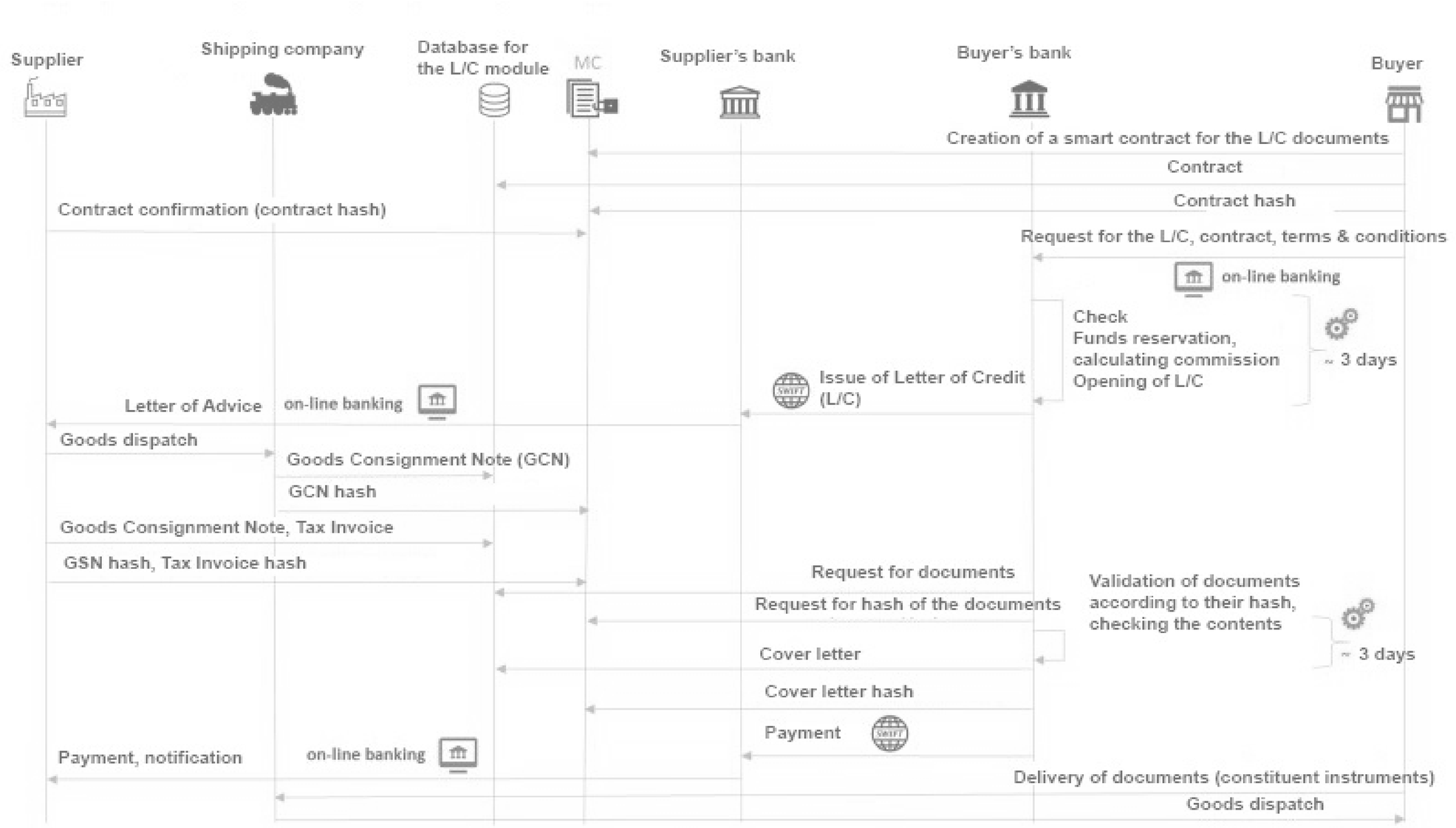
Use case example 2: Mortgage



Use case example 3: KYC



Use case example 4: Letter of credit



Questions?

Anatoly Konkin
anatoly.konkin@fintechru.org

FINTECH
ASSOCIATION