DECENTRALIZED NETWORK FOR DATA EXCHANGE AND STORAGE

"MASTERCHAIN"

Version 1.1

WHITEPAPER

Association for Financial Technologies Development Moscow, 2017

A. Arkhipov alexey.arkhipov@fintechru.org
T. Bilyk bta2@cbr.ru
A. Blagirev alex@open.ru
D. Bulychkov dabulychkov2@sberbank.ru
M. Grigoriev grigorievma@cbr.ru
K. Ivkushkin kvivkushkin@sberbank.ru
P. Kalambet p.kalambet@qiwitech.ru
E. Kirtsova e.kirtsova@qiwi.com
R. Sklyar roman.sklyar@open.ru
V. Sorokin sorokinve@cbr.ru
A. Troshichev alexey.troshichev@fintechru.org

Association for Financial Technologies Development Moscow, 2017

CONTENTS

1. DOCUMENT PURPOSE

The whitepaper in hand declares basic working principles of the distributed system **Masterchain** created on the basis of distributed ledger technologies and *blockchain* data structure, as well as its applications. The document is designed for trained users familiar with general terms of distributed ledgers, technical terms and definitions used to describe and formalize the protocols of decentralized networks.

The document was prepared by the working party of the Association for Financial Technologies Development (hereinafter named "the AFT") and is the property of the AFT. The document may be expanded and amended due to changes in the legislation of the Russian Federation, regulatory acts of the Bank of Russia or further development of existing technologies of distributed ledgers.

The whitepaper provides:

1. Prerequisites and goals of creation of **Masterchain**.

2. Established technological requirements.

3. Overview of the existing products (presented by the AFT members), which may be optimized by implementing the technology of distributed ledgers, i.e. **Masterchain**.

The whitepaper was developed by studying and analyzing the existing operating protocols for the distributed ledgers and their best operating practices.

2. MAJOR ISSUES AND PREREQUISITES

At present, there are no standard and regulated distributed ledgers in the Russian market, which makes the legal usage of this technology difficult. At the same time the AFT members are interested in the development of this technology and its implementation in their own products.

Thus, the main prerequisite for the creation of **Masterchain** is a need for a solution for the financial market, which would allow the members to deliver their projects based on distributed ledgers in an environment, compliant with the Russian legislation. Such a solution should use innovative technologies compatible with the most common infrastructures of existing distributed ledgers.

3. DEFINITION

Masterchain is a P2P-network with access control. The communications between the nodes of this network are based on the modified Ethereum protocol. **Masterchain** provides for safe record of information in a distributed ledger. The copies of this ledger are kept at each node of the network.

4. GLOSSARY

Distributed ledger is a type of data structure, the non-fixed number of copies of which may reach eventual consistency with the use of a set consensus algorithm.

Access control network is a network with a centralized control of network access for nodes.

5. PREREQUISITES

The prerequisites for creation of **Masterchain** are established in the following limitations inherent to financial ecosystems, including those on a nationwide scale:

1. The existing system of financial intermediaries lending credibility to the financial transactions does not provide for significant improvement of the speed of operations or reduction of transaction costs.

2. The audit procedures and risk management are complicated, because the data about the completed financial transactions is fragmented.

3. The lack of technical specifications related to the application of the distributed ledger technology hinders the integration of business processes and data of financial organizations.

These factors severely limit the opportunities of implementation of new financial technologies by the financial market participants and lead to an uneven distribution of access to these technologies among stakeholders. In particular, the identified limitations decrease the opportunity of obtaining relevant information, essential for making business decisions, which in turn contributes to the emergence of unscrupulous practices and increases the overall risk of fraudulent operations in the financial market.

In order to address the above-described issues, we propose to create a unified national network for the exchange and storage of financial information based on the distributed ledger technology (hereinafter referred to as **Masterchain**). This would allow to automate the financial transaction process for the network members by the aid of the built-in decision logic (hereinafter - *smart contract*).

6. SYSTEM PRINCIPLES

The key system principles of **Masterchain** are:

1. The distributed ledger of **Masterchain** does not store data requiring special storage mode (commercially sensitive data, personal data, classified data, etc.).

2. The data processed by Masterchain has legal value (in the Russian legal framework).

3. There is no technical need in trusted intermediaries.

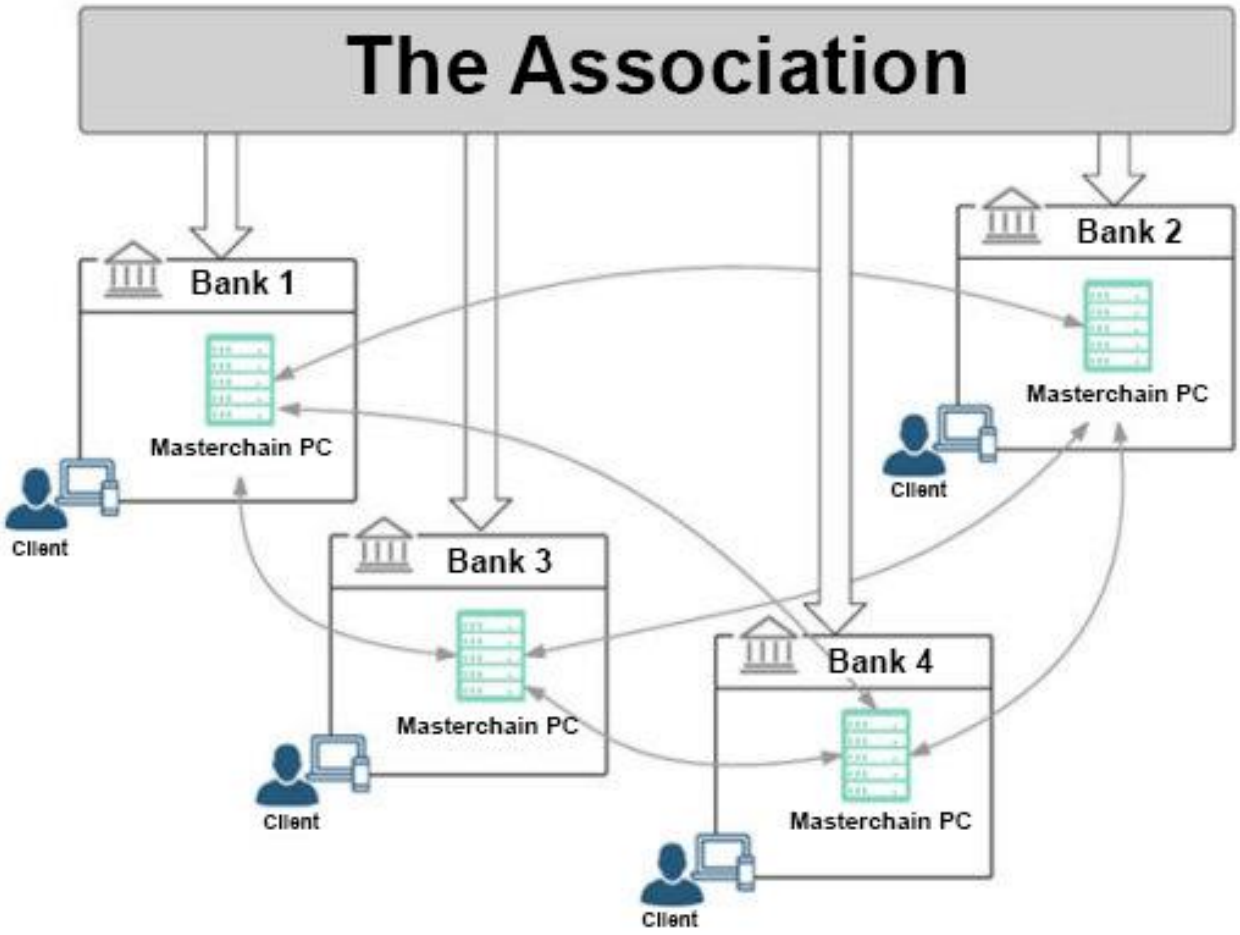
4. The network supports the programmable contracts (smart contracts).

5. The system hasn't a single point of failure.

6. The resources invested by the members to support the operation of the system are accounted for independently.

7. The system is scalable (according to the number of members and transactions).

6.1. COMMUNICATION PATTERN



The financial organizations, which are members of the Association, use **Masterchain** to support their business processes.

6.2. PLATFORM

In order to determine the requirements for the platform, we studied the existing distributed ledgers and their best operating practices. The requirements that are relevant to the task in hand are divided into three categories:

1. Operational requirements.

2. Security requirements.

3. Functional requirements.

6.2.1. OPERATIONAL REQUIREMENTS

1. Scalability according to the number of nodes. The increase in the number of nodes shall not add to the complexity of the consensus algorithm of the platform.

2. Support for a distributed system mode, under which all of the following requirements cannot be fulfilled simultaneously:

- trouble-free network connectivity,

- constant data transfer speed,
- secure network (the traffic cannot be modified by a third party),
- constant network topology,
- centralized network administration,
- all nodes and communication channels are identical,
- universal system clock.

3. The mainstream use of the platform in the Internet without the system access control and with the open source code.

The speed was not deemed an important operational requirement, as the effective control of speed in a decentralized distributed system with an unlimited number of members is virtually impossible.

6.2.2. SECURITY REQUIREMENTS

1. Chain authenticity verification. A single-valued algorithm for the only correct version of the distributed ledger.

2. The chain data cannot influence the logic of the consensus algorithm.

3. The opportunity for calculation of price of compromising the system with high accuracy.

4. Controlled access of nodes to the network.

5. The implementation of certified algorithms of cryptographic protection of information applicable in the Russian Federation.

6.2.3. FUNCTIONAL REQUIREMENTS

1. The opportunity for creation new code instances in the network, the execution of which results in events (smart contracts).

2. Accounting for the validation operations (mining).

3. Network access control.

6.2.4. DEFINITION OF COMPROMISE

The platform is deemed compromised, if any of the following events becomes possible:

1. The deliberate change of data in the distributed ledger, when the network has already reached consensus on this data.

2. The simultaneous existence of contradictory versions of the distributed ledger without an unambiguous marking allowing members to choose the right one.

6.3. LEGAL VALUE

The legal value is achieved via compliance with the Federal Law of the Russian Federation no. 63-FZ “On Electronic Signature” dated April 6, 2011. In particular, the certified CIPFs carry out the cryptographic transformations prescribed by the All Union State Standard (GOST).

6.4. TYPES OF ACCOUNTING UNITS

Technological units of account (TUA) are used to register the transaction processing operations (as technical commission). They are created by the validators during the block creation.

Specialized units of account are used for value operations. They are created within smart contacts managed by the regulator.

6.5. SUPPORTING SYSTEMS

The distributed ledger uses the supporting systems for performing the following categories of tasks:

1. Acceleration of transaction processing..
2. Processing of data requiring special treatment mode (personal data, payment information).
3. Monitoring and diagnostics of network status.
4. Integration with the third-party automation systems.
5. Integration with other distributed ledgers via Interiedger protocol.

6.6. SYSTEM OF REMUNERATION

Masterchain uses a mechanism of technical commissions for transactions and execution of smart contracts, similar to that implemented on the Ethereum platform.

The execution of each transaction (including those triggering the execution of smart contracts) detracts a technical commission stated in TUA. For the calculation of technical commission we use an abstract unit named *gas*. *Gas* is the unit of measure of the resources required to process a transaction and record it in the distributed ledger. A unit of gas corresponds to the number of TUAs specified by the administrator of the node. Accordingly, the minimum necessary transaction costs are calculated by multiplying the amount of required gas by the number of TUAs corresponding to the unit of gas (specified by the administrator).

The TUAs received by the validator for processing a transaction are used to account for the following costs:

- costs of calculations performed during the transaction,
- commission for the amount of data recorded in the distributed ledger.

In addition to cost accounting, the technical commission works as an adaptive protection against DDoS attacks by “garbage” transactions: the attacker (just like any other user) has to spend TUAs to use the resources, including calculations, the size of the transferred transactions, and data storage.

7. PROJECTS FOR THE PLATFORM

The following section contains the descriptions of projects that are expected to launch in the Masterchain network in the short term.

7.1. DECENTRALIZED DEPOSITORY SYSTEM FOR REGISTRATION OF MORTGAGES

7.1.1. GOALS

1. To put the DDS into operation in compliance with the effective date of the requirements for the accounting of mortgages in the electronic form.

2. To involve a sufficient number of mortgage banks in implementation of this unified solution throughout the segment.

3. To reduce the costs and time of operations of storage, accounting and securitization of mortgages.

7.1.2. OBJECTIVES

1. To create an economic interest group formed by the key participants of the mortgage market and involve them in the operation of the DDS.

2. To design and implement the DDS as a fully open-source out-of-the-box solution.

3. To launch the commercial operation of the DDS as a mortgage electronic register by the middle of 2018.

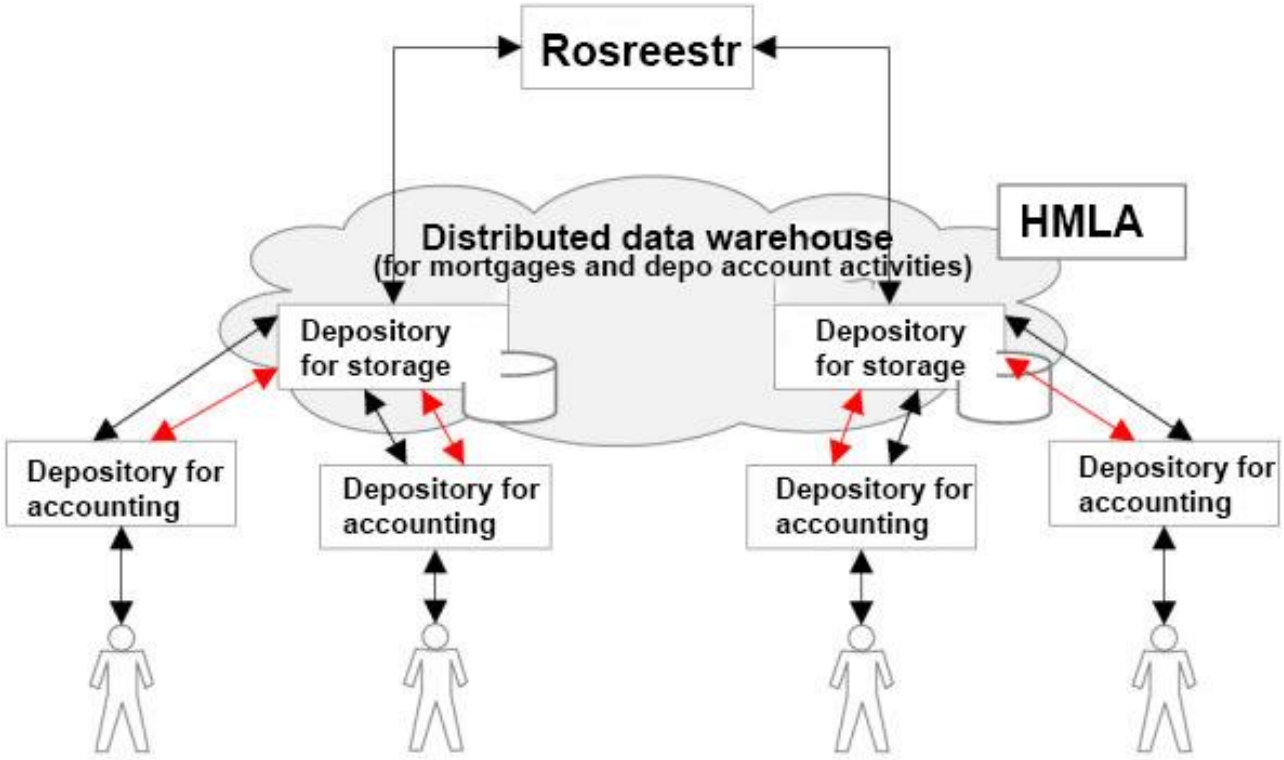
4. To establish a service company (SPV) for facilitating the contractual relationship between the members of the DDS.

7.1.3. PROJECT DESCRIPTION

- The project is in compliance with the current legal framework; it preserves the division of roles and functions of existing members.

- The storage depositories form "a cloud" for the distributed storage of electronic mortgages and depo account activities.

- The inter-member processes are automatized via smart contracts; they are compliant with the logic of the current legislation.



7.1.4. PROJECT MEMBERS

- banks providing mortgages and depositories,
- housing mortgage lending agencies,
- (optional) Rosreestr (Federal Service for State Registration, Cadaster and Cartography).

7.1.5. ECONOMIC FORECAST

- Significant (2 to 5 times) reduction in the costs of storage, accounting and preparation / conduct of securitization.
- Reduction in the time of operations from days to minutes.
- Secure storage of mortgages and depo account activities.
- After the first year of operation the DDS is to become the world's largest system for storing fully electronic mortgages (eMortgage).

7.2. KYC

7.2.1. GOALS

1. Elimination of the risk of lacking information necessary to prevent fraudulent transactions.

2. Exchange of information about physical persons (data structure "KYC Attributes") between the members of the **Masterchain** decentralized network, not involving the disclosure of information covered by bank secrecy or clients' personal data.

3. Providing the ability to scale the solution in the following areas:

- simplified identification - the implementation of the Digital Identity concept,

- exchange of information about legal entities,

- exchange of credit histories.

7.2.2. OBJECTIVES

1. Implementation of business scenarios using the "KYC concept".

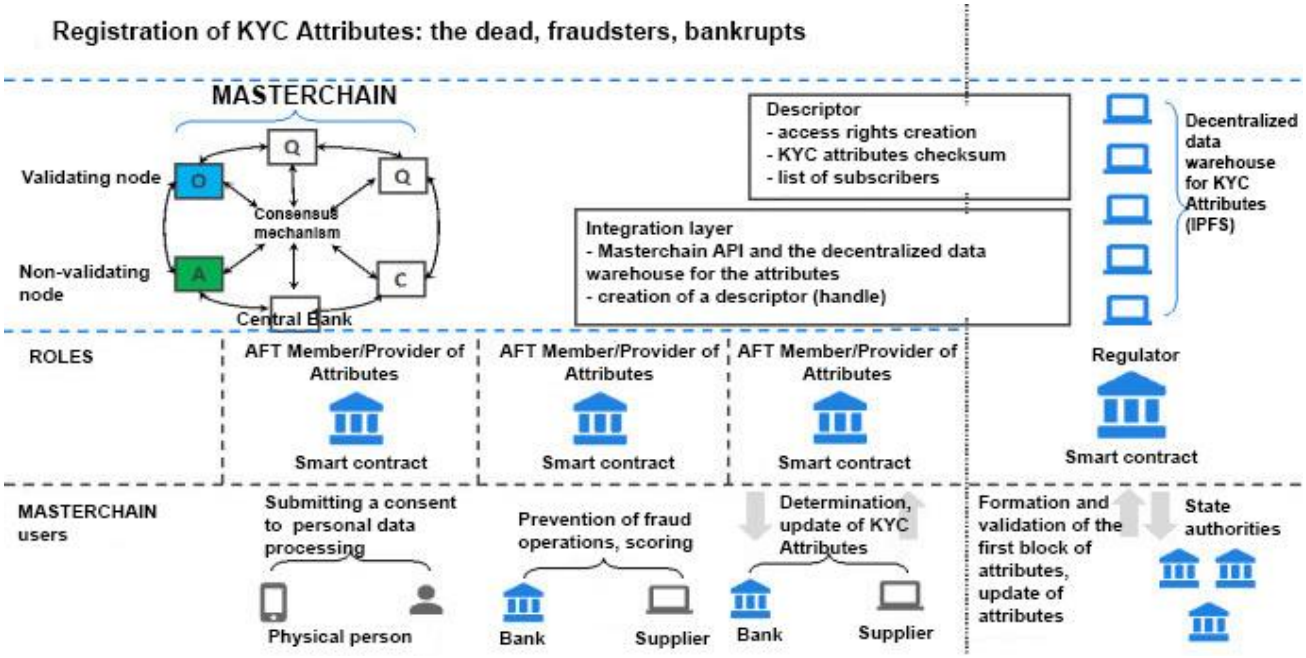
2. Interbank cooperation, not involving the disclosure of the client base, on a commercial basis.

3. Compliance with the Federal Law no. 13-FZ (as in force on July 2, 2017) to the extent concerning the following requirements: depersonalization, destruction of personal data, fulfilling all requests from the owners of PD.

4. Provision of control over the process by the regulator.

7.2.3. PROJECT DESCRIPTION

The project involves an implementation of shared access to a decentralized data warehouse (the data structure "KYC Attributes") with the use distributed ledger technology on a commercial basis.



The database "KYC Attributes" is stored in anonymized form in a decentralized storage (IPFS) integrated with the **Masterchain** decentralized network, but not in the network itself.

The operations performed within the project:

1. Trusted exchange of client-related information involving physical persons on a commercial basis.

2. Collection and processing of data for the creation of the "KYC Attributes" data structure:

- Objective attributes are not defined by a behavioral pattern or a relationship guaranteed by the state.

- Accumulated attributes are facts that can change during the life cycle of a physical person or legal entity.

- Acquired attributes are prone to change; they act as identifiers of the relationship with the trusted data domain.

3. Formation of a decentralized data warehouse, provision of access in accordance with the accepted concept of roles and rights within the Masterchain decentralized network.

4. Implementation of business scenarios:

- Verification of whether a physical person is included in the register of fraudsters compiled by the members of the decentralized messaging system through scoring of personal data forms.

- Verification of whether the physical person has got a death record.

5. The possibilities of scaling the solution in the future:

- implementation of the process of exchanging customer credit histories (equivalent of credit bureau);

- implementation of the process of exchanging information about legal entities;

- implementation of the process of simplified / remote customer identification;

- expansion of the system's functionality to implement a full-fledged KYC script.

7.2.4. PROJECT MEMBERS

• Provider - a member of the decentralized network responsible for collection, processing and transfer of the "KYC Attributes" database.

• Consumer - a member of the decentralized network with an access to the "KYC Attributes" database using its data to prevent fraudulent operations.

• Physical person - a person who grants or revokes consent to the processing and use of their personal data for the "KYC Attributes" database.

• Regulator - a person performing control / audit of the selected scenario / process for integrity, compliance with the legislation, and proper execution of inquiries of physical persons.

7.2.5. ECONOMIC FORECAST

• Formation of a trusted operating environment for the members.

• Reducing the risk of fraudulent operations.

• Simplified / remote customer identification.

7.3. PROJECT "DISTRIBUTED REGISTER OF DIGITAL BANK GUARANTEES"

7.3.1. GOALS

1. To reduce labor costs for obtaining / verifying the guarantee for all members in the chain: bank, obligor, beneficiary.

2. To improve the security of bank guarantees and reduce the number of printed counterfeits.

3. To expand the application of bank guarantees through the use of smart contracts.

7.3.2. OBJECTIVES

1. To design and implement an operating prototype product based on Masterchain with an Open API to connect with other members.

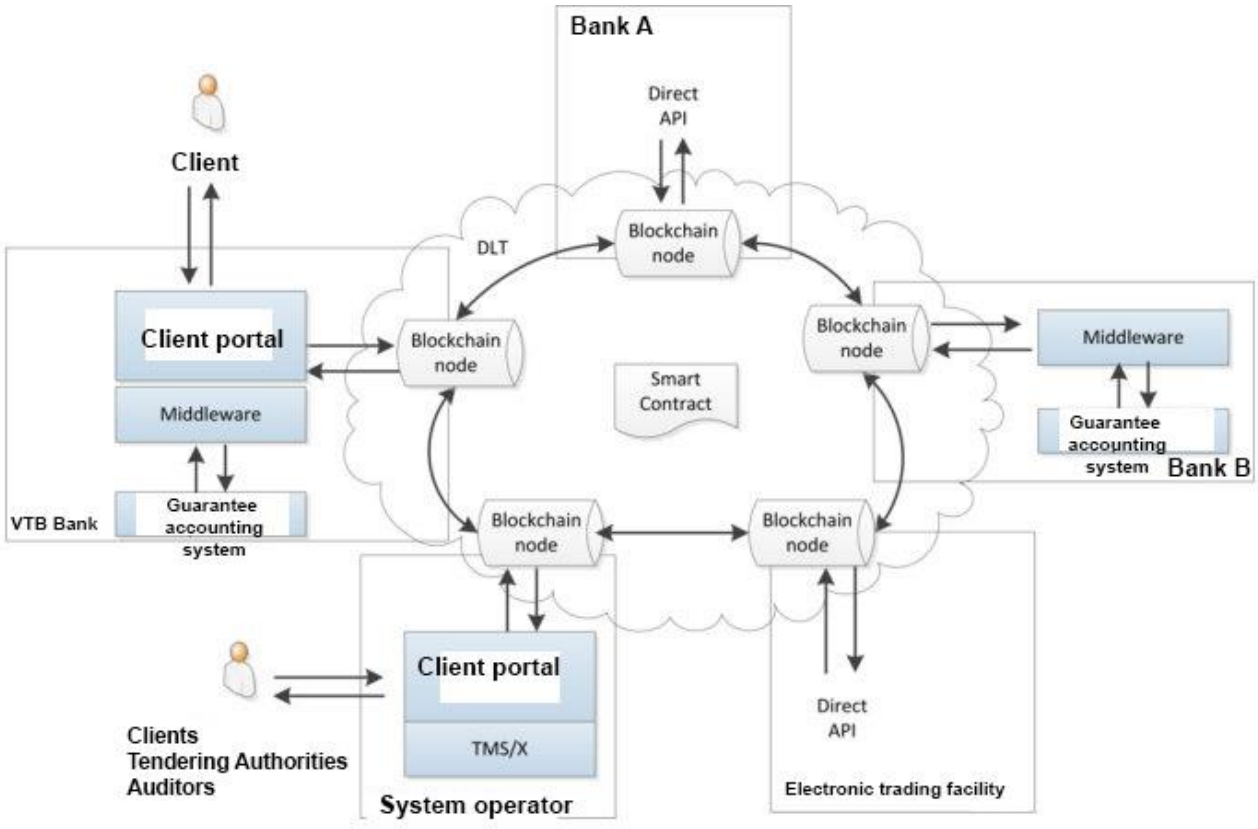
2. To carry out beta-testing of the prototype product together with the interested AFT members and (if necessary) make changes in Open API (the goal is to minimize the costs of connecting the internal bank systems to the network).

3. To identify and develop changes (drafts) in the legislation necessary for launching the commercial operation of the product.

7.3.3. PROJECT DESCRIPTION

The final goal of the project is the creation of a distributed ledger of digital bank guarantees issued by the banks operating in the Russian Federation, as well as moving away from guarantees on paper.

It is expected that a digital guarantee will act as a primary digital document, which will be reproduced on paper only if necessary, for the purpose of reference.



1. The system will be powered by the Masterchain platform.

2. The direct members of the system (banks) will have their own nodes in the network "Masterchain-Guarantees", as well as client portals for conveying information to their customers.

3. Being major consumers of information about the guarantees, electronic trading facilities will be provided by a special gateway interface for working with "Masterchain-Guarantees", as well as special rights.

7.3.4. PROJECT MEMBERS

• Banks operating in the territory of the Russian Federation and entitled to issue bank guarantees. Issuing of digital bank guaranties and publishing the information about each guarantee in the ledger.

• Trading facilities. The opportunity to receive ledger information about the guarantees related to the transactions on the trade platform.

• Representatives of legal entities. The opportunity to receive ledger information about the guarantees related to legal entities.

• Natural persons. The opportunity to receive ledger information about the guarantees with a right of public access (for instance, the guarantees listed in the Federal Law 44-FZ).

• Representatives of public authorities. The opportunity to receive ledger information as pertaining to their authority and areas of responsibility.

7.3.5. ECONOMIC FORECAST

Increased security of bank guarantees.

A digital guarantee stored in a trusted distributed digital ledger is more difficult to counterfeit than a printed document.

The opportunity to expand the functions of the guarantees via the use of smart contracts.

Reduction of costs and acceleration of issue of bank guarantees.

This is especially important for small and medium businesses, as well as for banks issuing guaranties for them. The larger the number of guaranties, the more significant reduction of costs and acceleration effect will be.

The expansion of the base of the registered bank guarantees.

At present, there is a centralized register of guarantees issued in connection with contracts under the Federal Law no. 44-FZ - http: //zakupki.gov.ru.

Simplification of the process of verification of bank guarantees by third parties.

The opportunity to differentiate between the access rights of various categories of users both to the bank guarantees in the register and to their separate sections.

Depending on the user category, the system will regulate which guarantees are visible to them in the database, and which sections of each guarantee they are allowed to read. For instance, special privileges may be granted only to the bank, the obligor, the beneficiary and the regulator.

7.4. ELECTRONIC LETTER OF CREDIT

7.4.1. GOALS

1. Reduction in the term of execution of transactions on paid letters of credit.

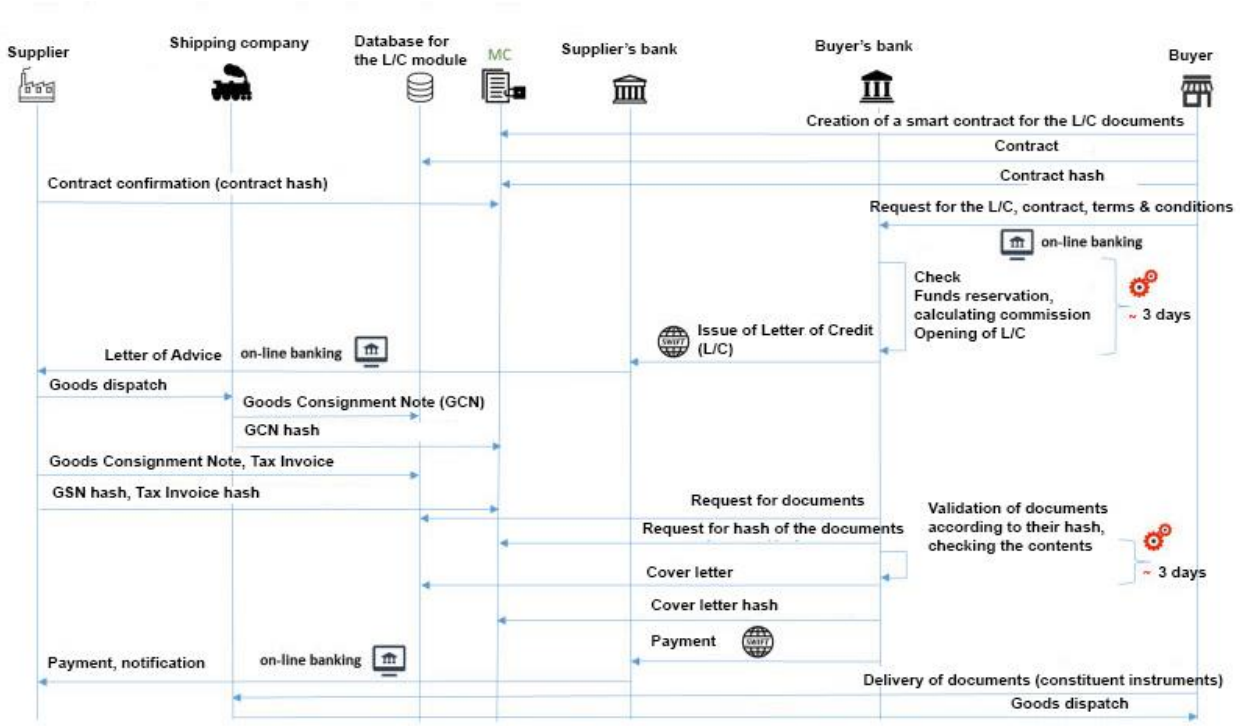
7.4.2. OBJECTIVES

1. To eliminate paperwork and related time delays in the execution of transactions (stage 1).

2. To automatize financial transactions (stage 2).

7.4.3. PROJECT DESCRIPTION

The implementation of Masterchain in transactions involving paid letters of credit to eliminate paperwork and shorten the time of transaction.



7.4.4. PROJECT MEMBERS

- Seller;
- Seller's bank;
- Buyer;
- Buyer's bank;
- Shipping company.

7.4.5. ECONOMIC FORECAST

Reduction in the term of implementation of a letter of credit with a 15 days' cover.

- Stage 1: Reduction by 9 days.
- Stage 2: Further reduction up to 6 days.

Association for Financial Technologies Development Moscow, 2017