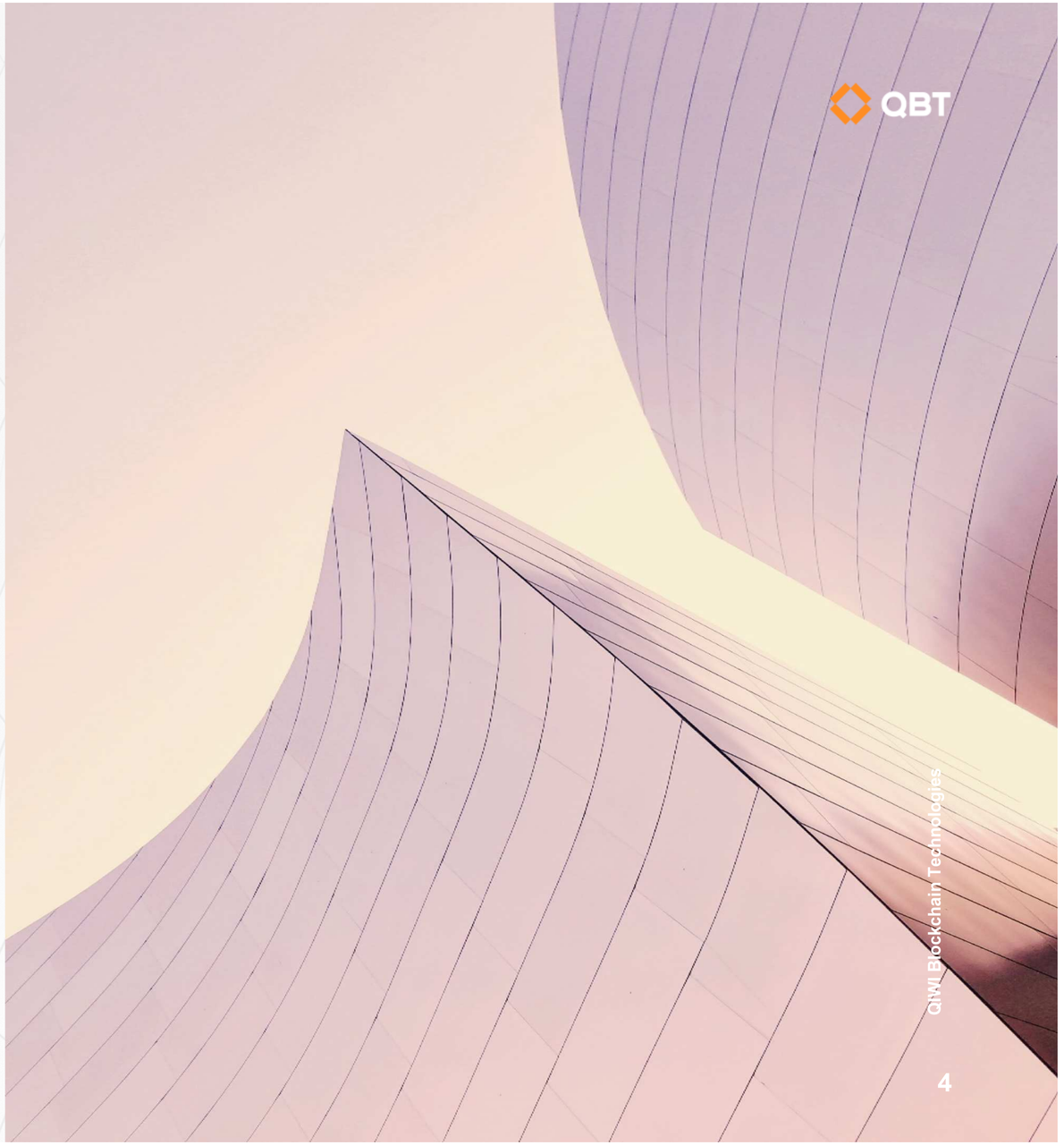

QIWI
BLOCKCHAIN
TECHNOLOGIES
Topic: “Architectural principles in the context of the national regulatory framework and confidence building on the example of the consortium blockchain platform "Masterchain"
2019

Alexander Chuburkov

Legal consultant

Expert on international standardization (GOST-R)



CONTENTS:

- Key regulatory requirements for DLT & the impact of regulatory requirements on technology architecture
- The need for a private layer
- KYC and access control
- The use of non-recoverable hardware keys for all cryptographic operations in the blockchain
- Managed access. Role-based model of access to confidential data, which is controlled through the blockchain

KEY REGULATORY REQUIREMENTS FOR THE MASTERCHAIN SYSTEM

1. Integration of the platform with the cryptographic key storage system and the use of an enhanced electronic signature (GOST R 34.10-2012)

2. Data exchange between participants with TLS secure channel

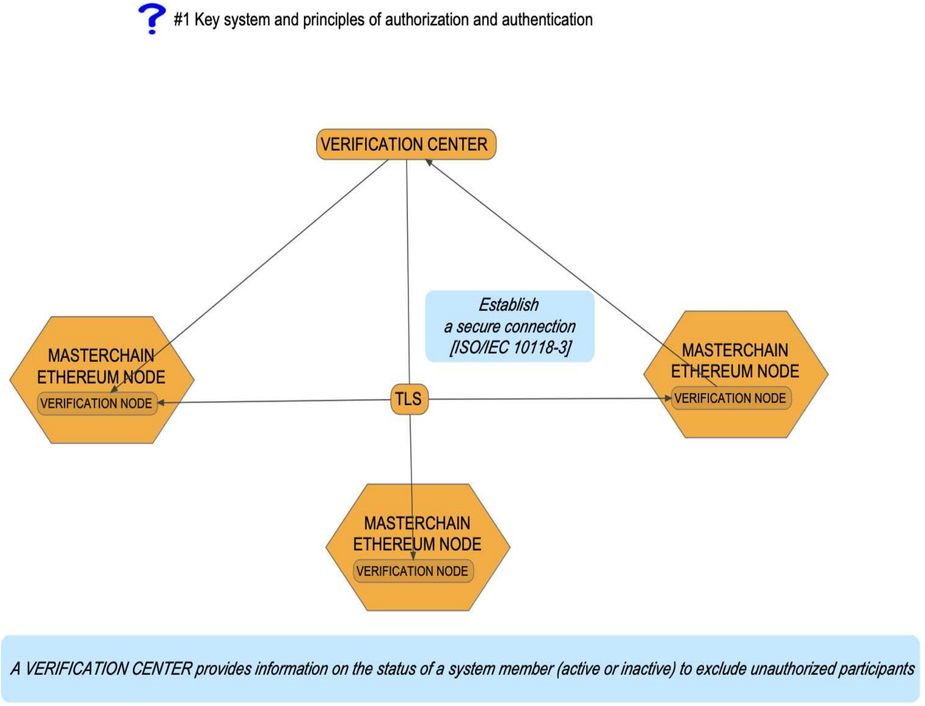
3. Integrity of a distributed ledger

IMPACT OF REGULATORY REQUIREMENTS ON TECHNOLOGICAL ARCHITECTURE

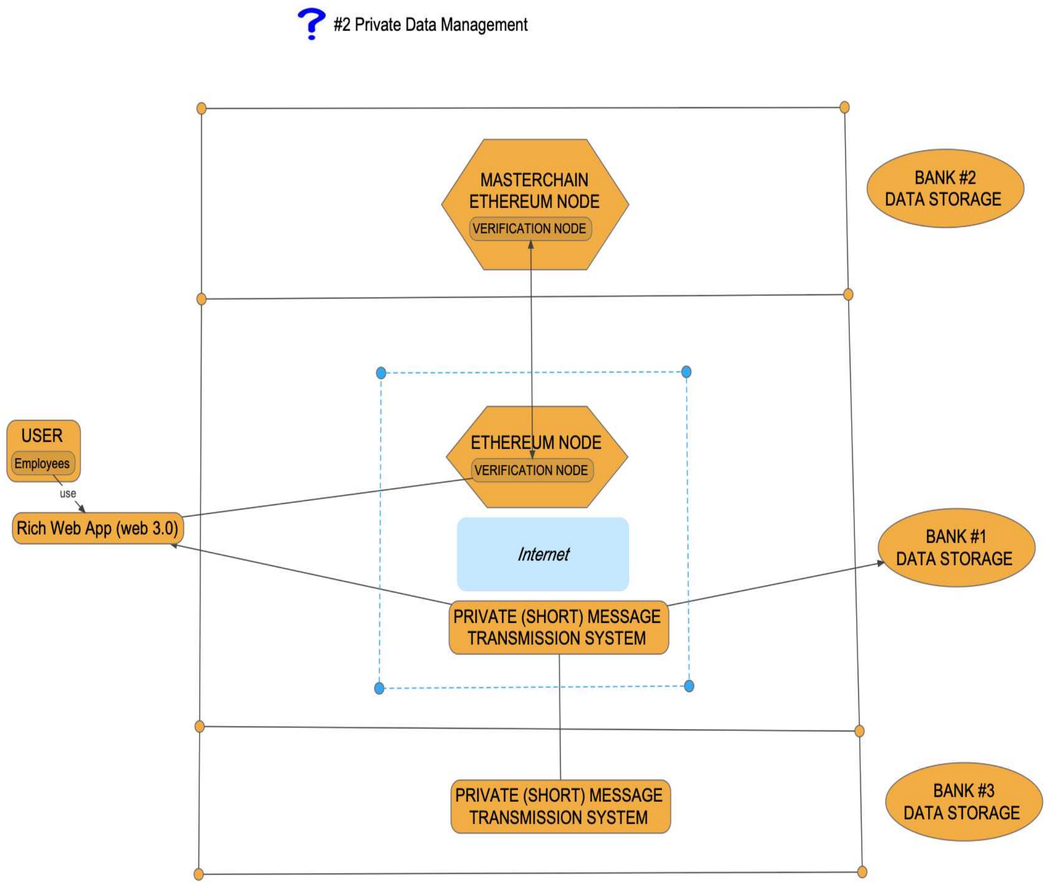
Implementing cryptographic mechanisms that meets Russian state standards (directing all cryptographic calls to this module).

Modification of the Ethereum protocol In order to provide the required information security level
(See Figure1):

New role-based access model, New cryptographic key system
New protocols for establishing secure connections,
New principles of authentication and authorization



Modified protocols for interfacing with subsystems for processing confidential data (See Figure 2)



Data integrity control is ensured in accordance with the Russian state standard (the algorithm is part of the international standard ISO / IEC 10118-3),

In order to exclude unauthorized access to functions, keys and processed information, user identification / authentication procedures have been modified

when accessing transaction signatures and turning on blocks, authentication of nodes upon access, integrity control of software and key information.

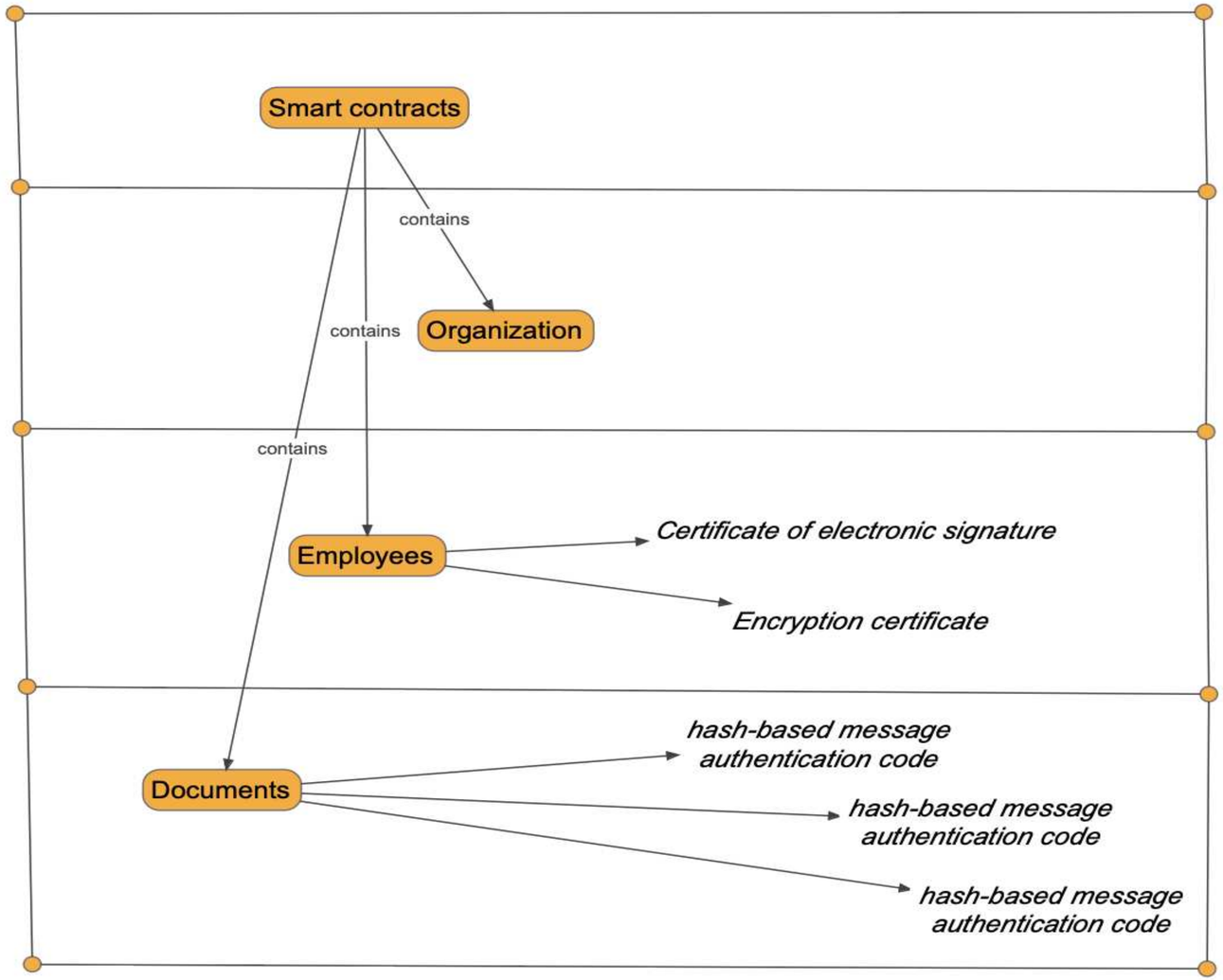
Authentication of subjects when accessing nodes is provided using the TLS protocol using additional roles specified in the certificates.

Certificates (separately for each of the protocols running within the framework of the work of the system functioning) are issued by an authorized certification center using templates with additional identifiers — during operations, they allow you to determine if the key holder has the appropriate permissions.

In this case, local access is only possible for the tasks of configuration and maintenance of the node by security administrators

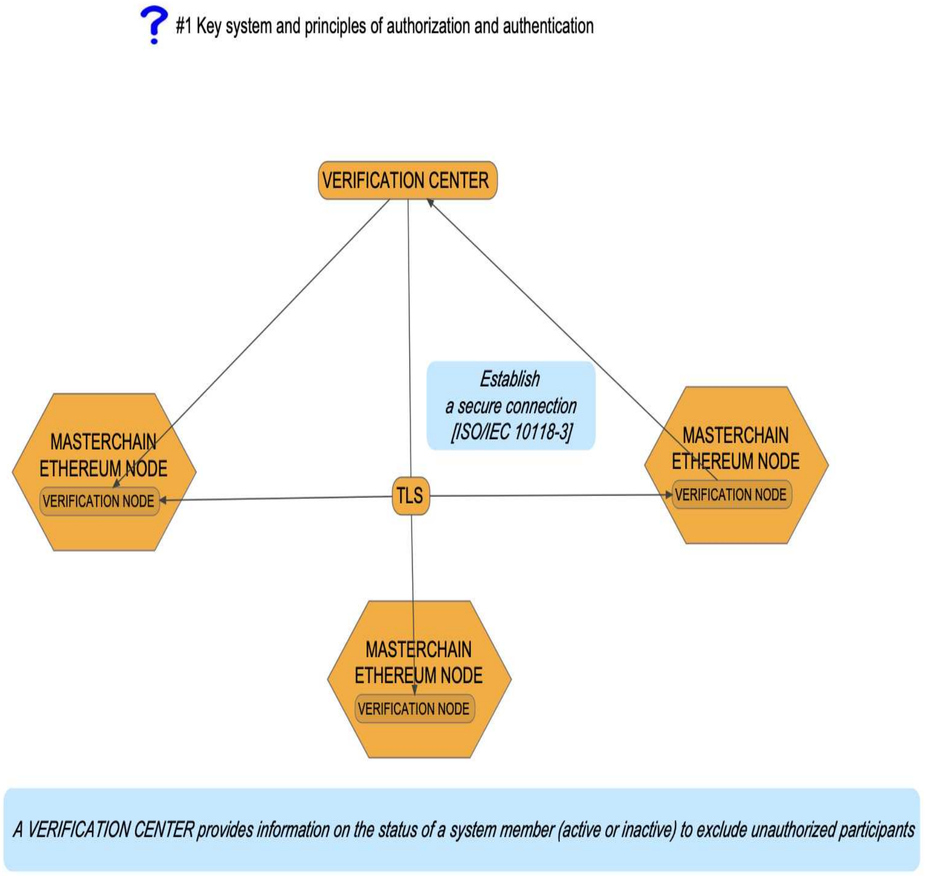
(See the next slide: Figure 3)

3 Access Rights Management Role Model
(Each node contains a smart contract, with the following logical structure)



Additional authorization is based on a special smart contract stored in the blockchain — it contains a white list of users and determines the role of each subject and the operations available to him. This list can be changed by the information security administrator when adding / excluding users from the system

A special Certification Authority has been implemented and is being used, thanks to which the requirements for integrity control, verification of key validity periods, work with certificate usage, random number generators, audit and implementation of all cryptographic protocols are fulfilled (See Figure 1)



CONFIDENTIAL DATA SECURITY

Implemented:

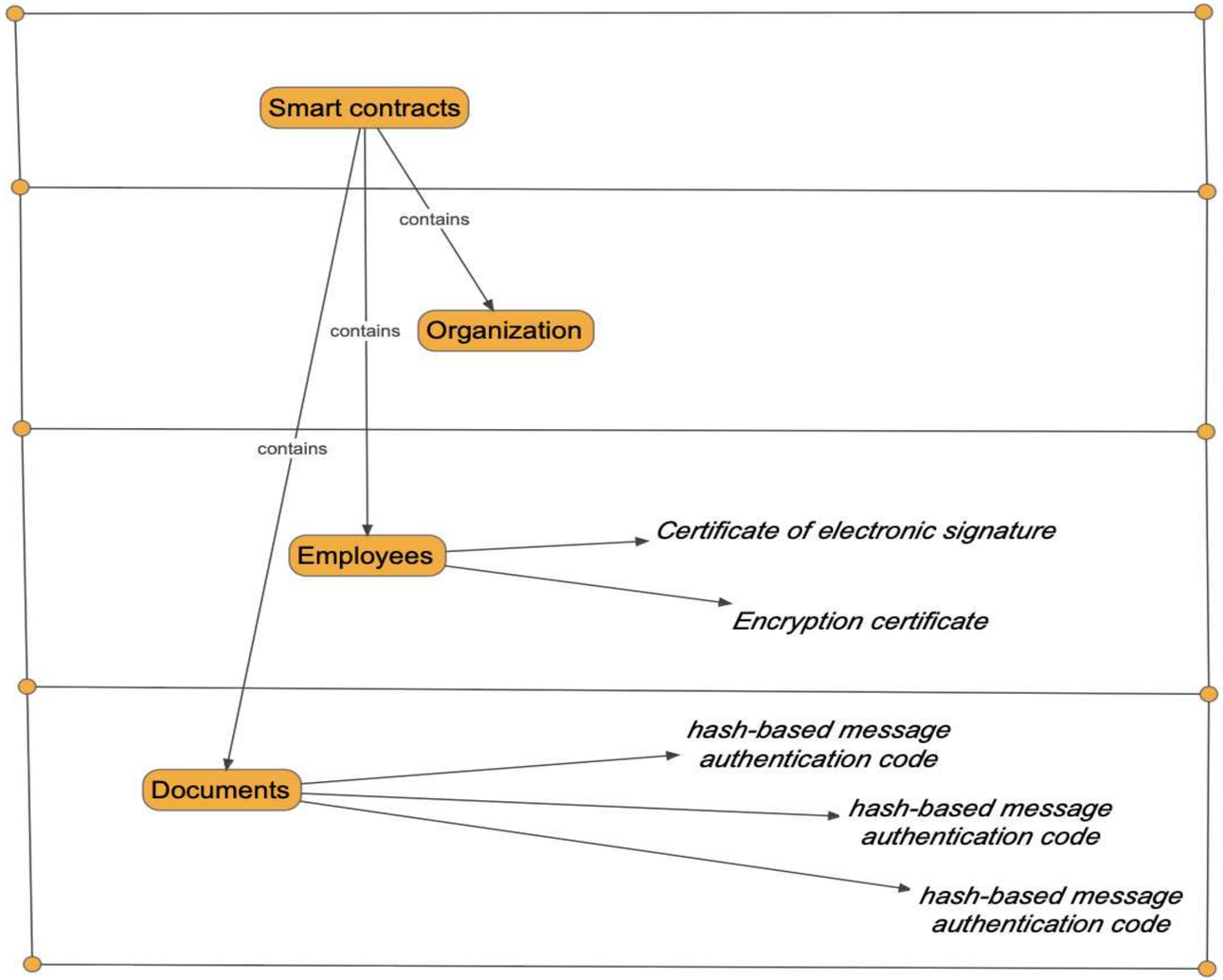
•role-based access control to data;

•management and storage of access rights directly on the blockchain.

The document is stored in a special dedicated storage, and the “fingerprint” of this document is stored on the blockchain; not a hash value, but a message authentication code (hash-based message authentication code) is used as such a fingerprint.

It provides integrity check and immutability like a hash function, and due to the random 256-bit vector stored in secret, it prevents the ability to restore a document from its fingerprint” by brute force attack (See the next slide: Figure 3)

3 Access Rights Management Role Model
(Each node contains a smart contract, with the following logical structure)



CONCLUSION

Masterchain simultaneously provides confidentiality and reliable data storage with safe authentication of each subject, legal significance, and therefore the ability to implement on the same platform all those projects that would previously require the manual combination of technology with a separate security audit

QIWI
BLOCKCHAIN
TECHNOLOGIES

Thank you

+7 495 009-0009

Info@qiwi.tech

4 Shlyuzovaya Embankment 115114 Moscow, Russia

2019