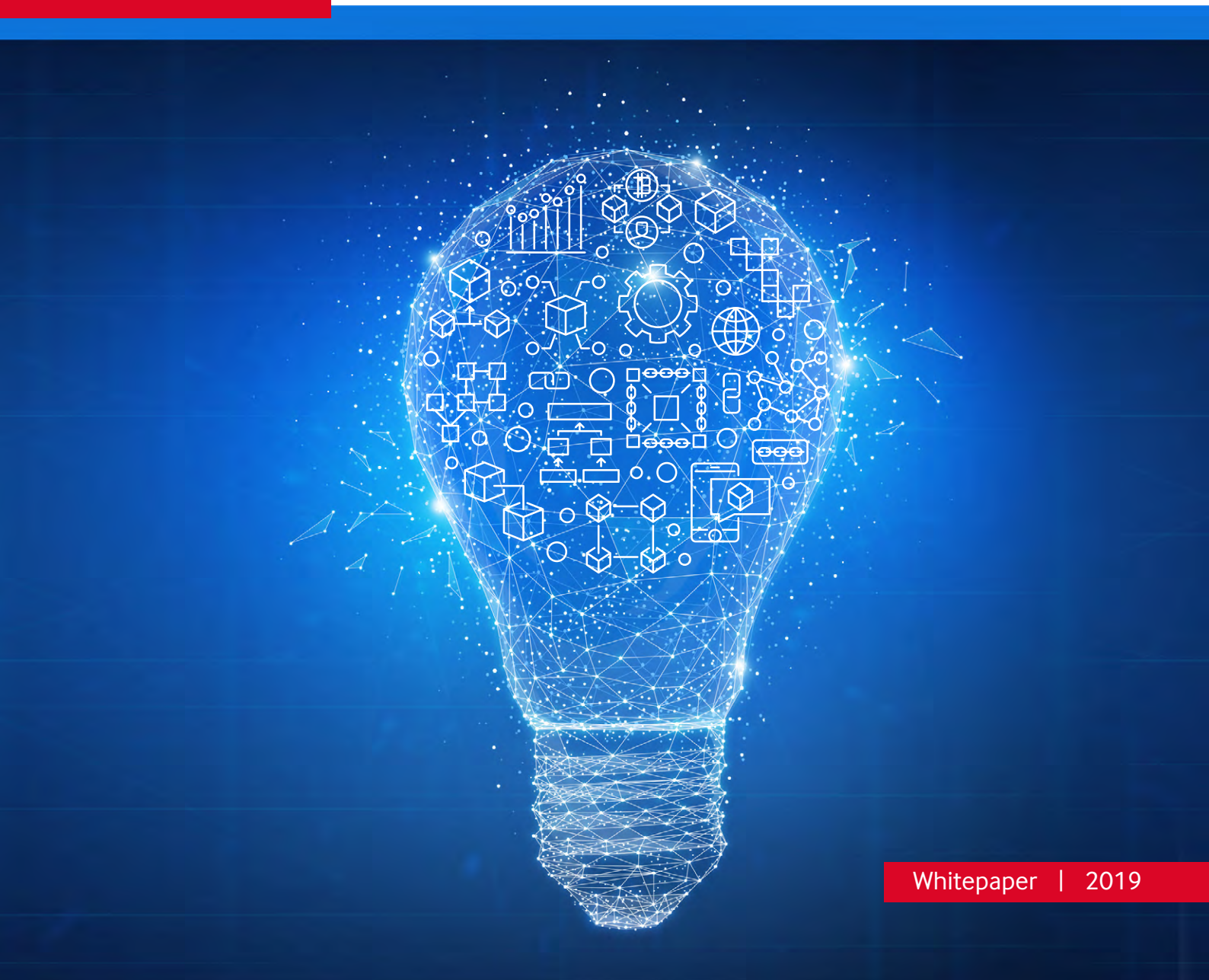
NATIONAL SETTLEMENT DEPOSITORY
MOSCOW EXCHANGE GROUP

BLOCKCHAIN IN FINANCIAL INFRASTRUCTURE: RISKS AND OPPORTUNITIES



Whitepaper | 2019

INTRODUCTION

National Settlement Depository (NSD) opened a blockchain lab in 2015. Since then, considerable experience in applying distributed ledger technology, including practical application in current business processes within the Russian financial infrastructure, has been gained. The lab has implemented multiple commercial solutions, such as bond issuances, a distributed digital depository, and tri-party repo transactions. Today, NSD's blockchain lab analyzes technological capabilities: stress testing various configurations of a distributed ledger, utilizing zero-knowledge proof, and applying various tokenization schemes. The working group established by NSD within the International Securities Services Association (ISSA) and involving major international central securities depositories issued a series of recommendations and blockchain-related reports to harmonize the requirements that contribute to addressing the challenges faced by the sector.

Blockchain already was at its peak of popularity owing to a surge in demand for cryptocurrencies and numerous ICOs in a legal grey zone; the technology was tested by pilot transactions in a corporate environment and survived attempts to hack blockchain networks, wallets, and token exchange platforms, as well as investigations in various jurisdictions, and it seeks to take its place within the diversity of technologies that can be used in corporate and global systems. The use of this technology makes it possible to move from transferring data about asset movements to transferring assets themselves using cryptography, as well as to adapt the financial infrastructure to dealing with new asset types that require more flexible approaches and focus on the technological part of the service. Financial market participants develop their own solutions based on the distributed ledger technology, play an active role in various consortiums, and launch pilot solutions on different blockchain platforms to find out what opportunities the blockchain technology can offer in practice.

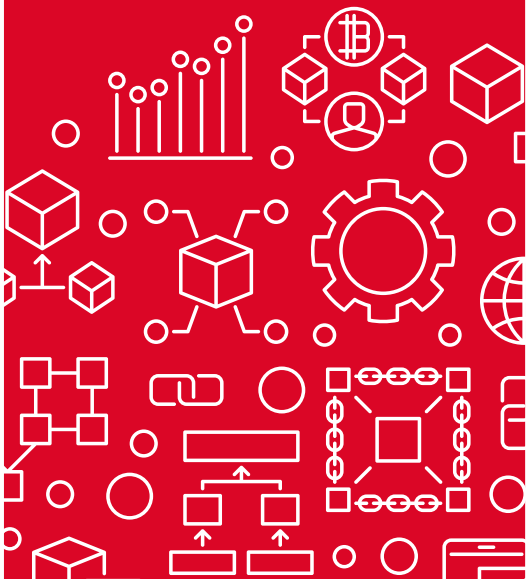
In this writing, we summarize the results of our work and describe the potential ways to successfully implement blockchain in the sector in the near term. Specific focus is placed on the methodology for choosing a distributed ledger as one of the architectural solutions, as well as on technical aspects: ensuring data privacy within the network, scalability of solutions, and blockchain governance issues.

What is blockchain?

Blockchain (originally block chain) is a continuous sequential chain of blocks that contain information built by certain rules and linked by cryptographic algorithms [1]. Each block consists of an identifier, a cryptographic link to the previous block, and a data set. The first steps to create a concept of chains of data blocks linked by cryptographic mechanisms in an electronic database were proposed in 1991 – it was a mechanism for creating certificates that protect time-stamps embedded in electronic documents against forgery [4]. The next year, this concept was enriched with Merkle trees [2, 3], which allowed bringing multiple document certificates together in a single block [6].

The first full-scale blockchain system concept was proposed in 2008 [8]. The system's architecture was enhanced by the use of a system designed to add blocks to a chain, based on the HashCash idea and not requiring signatures of an authorized person [7].

The first public blockchain was launched in 2009, and today Bitcoin, a native token issued on it, is the most popular native asset issued using cryptography and blockchain ideas.



CLASSIFICATION OF EXISTING CHALLENGES IN USING BLOCKCHAIN

IT SECURITY

For financial infrastructure, IT security is a critical issue. Any technology used must ensure the highest level of protection of assets themselves, and offer mechanisms to prevent unauthorized data access. Identification of a network participant is also crucial.

The history of financial infrastructure evolution has convincingly demonstrated the need to separate different functions when dealing with financial instruments: safekeeping, settlement, clearing, and trading. However, when launching trading platforms for native tokens (cryptocurrencies), that experience was ignored. This led to thefts of more than 6.5% of the total amount of the first global cryptocurrency – Bitcoin – directly from centralized platforms, since 2011 [25]. Trading platforms that have been launched with a certain level of decentralization do not currently demonstrate a large trading volume compared with centralized solutions and account for less than 1% of the total trading volume, which may be due to their operational instability and high risks of manipulation [26], as well as due to problems with identification of participants in a fully distributed open network architecture [27].

The analysis of security breaches of systems that handle assets stored and issued directly on a blockchain shows that the vast majority of successful attacks happen not through cryptographic schemes, and that they are aimed at gaining access to private keys for e-wallets and making quick withdrawals. Multi-signatures, Hardware Security Modules (HSM), and cryptography software designed to protect against unauthorized access to keys are used to mitigate this risk.

DATA PRIVACY

First blockchain platforms were created without having data privacy in mind. This resulted in the emergence of the term "pseudo-anonymity" in relation to some blockchain platforms, and also made it possible to identify owners of private keys and to put a pressure on them, gain control over these keys, and transfer assets controlled by them [28].

The use of various cryptographic anonymization tools (zero-knowledge proof, confidential transactions protocols, and transaction mixers) is constrained by the scalability trilemma [12, 36]: all implementations require substantial computing power and transmission and storage of large data volumes. Despite the evolution of basic and applied cryptography, there are still no blockchain technology solutions available that have the required set of properties for them to be successfully implemented in the financial infrastructure [29, 30]:

- transaction mixers are centralized solutions with limited anonymity;
- the use of ring signatures entails scalability problems due to a manifold increase in the size of data in a transaction and requires algorithmically complex verification;
- the use of zero-knowledge proof requires substantial computing power and trusted participants to bootstrap the network, as well as the use of new non-standardized cryptographic primitives;
- the confidential transactions algorithm (Mimblewimble protocol) requires interaction between the receiver and the sender, leaves room for activity monitoring, and does not break links between transactions.

The current level of applied cryptography and the maturity of technology implementations do not allow us to recommend the use of any particular technology to ensure data privacy in distributed ledgers. To ensure the required level of data privacy, it is proposed to put in place access restrictions (roles or channels) and to apply industry-proven cryptography

methods and methods designed to restrict access to a blockchain network, similar to centralized and cloud solutions. To increase the security level of blockchain solutions offered in the market for native tokens (cryptocurrencies), improved regulation is required, as well as steps to mitigate risks of losing control over assets stored in the form of tokens during their storage and trading (in accordance with practices applied by traditional financial institutions).

INTEROPERABILITY BETWEEN MULTIPLE BLOCKCHAIN PLATFORMS

Interoperability between multiple blockchain platforms is a challenging task due to a number of reasons: different consensus requirements, availability/unavailability of the option to use multi-signatures or smart contracts in a certain system, etc. It is also worthwhile to mention the lack of industrial demand for integration owing to a small number of blockchain solutions implemented and the need to integrate them with centralized systems.

For example, a distributed P2P architecture implies that there is no single integration point. Some platforms do not have the required functionality, and there are also difficulties associated with the use of identification of network participants and data sets from one blockchain in another one, etc.

Generally, there are three interoperability schemes [50]:

1. A notary scheme: the use of a set of participants monitoring third-party blockchain A and 'notarizing' actions on blockchain B, to which data is transferred. In this case, it is necessary to have dedicated blockchain C to manage participants in the notary scheme (it can be the same as A or B).
2. Relay schemes: the use of smart contracts or a multi-signature. A smart contract or another mechanism of blockchain A can monitor and affect the state of blockchain B. In this case, no dedicated blockchain (as in a notary scheme) is required, but one of the blockchains (A or B) acts as leading blockchain. There are two types of relay schemes:
    - One-way relay scheme with one-way interoperability [51]; and
    - Two-way relay scheme that enables two-way interoperability [55].
3. A hash-locking scheme: blockchain A and blockchain B monitor the same hash function. Unlike a relay scheme, it is not required for either blockchain A or blockchain B to act as leading blockchain; exchange of hashes is sufficient. In this case, the amount of transmitted information needed for interoperability is successfully minimized.

As part of ensuring interoperability between multiple blockchain platforms, the following token-handling scenarios are possible:

1. Token portability. A token can be sent from blockchain A to blockchain B and back.
2. Atomic swap. A mechanism designed to guarantee transfer of tokens between two parties.
3. Cross-chain oracles. Blockchain B monitors events in blockchain A using a smart contract or another mechanism and performs a specific action when a particular event occurs.
4. Cross-chain asset encumbrance. A token is locked on blockchain A and can be unlocked when a certain event happens on blockchain B.

Comparison of potential usage scenarios and implementation mechanisms shows that [53]:

- Hash-locking can only be applied for an atomic swap.
- A one-way relay scheme can be used for all scenarios, except for an atomic swap.
- A notary scheme and a two-way relay scheme can be used for all four scenarios.
- When using hash-locking, the total amount of issued tokens on each blockchain remains unchanged, and when using a notary or relay scheme, all work with a token can be transferred entirely from one blockchain to another [52].

The use of interoperability mechanisms between multiple blockchain platforms in commercial solutions is currently impossible due to the scalability constraints of the proposed solutions and little experience in applying technologies. However, it is worth noting several projects that will help address the issue of interoperability of certain blockchain platforms in a particular case:

1. Implementation of a two-way relay scheme for two dedicated Dogethereum blockchain networks [56].
2. Implementation of the Interledger protocol based on atomic swaps [57].
3. Cosmos [54] and PolkaDot [58] projects running on a notary scheme using a native token for multiple blockchain networks. These technologies can be used primarily for private (Cosmos) and public (PolkaDot) blockchain networks that constitute separate blockchain platforms.

In the near term, existing interoperability solutions can provide the basis for new workable solutions.

PUBLIC AND PRIVATE BLOCKCHAINS

A **public blockchain** with an infinite number of anonymous participants has no management tools or tools to identify network participants (users and network nodes). Accordingly, it is impossible to run AML/KYC verification procedures directly on the blockchain platform, without involving a third-party service.

The nodes of a public blockchain can be located anywhere globally, the entire code and protocols are open, and all data is available for verification. Management of such blockchain is consensus-based, with no organization or individual being responsible for the blockchain functionality or for any data being stored on the blockchain.

Public blockchains have the following properties:

- The use of probabilistic consensus to change data in most cases does not guarantee finality of settlements on such a network due to there being different versions of the data set at any given time and due to the probabilistic mechanism for choosing a single final version of data [8];
- Unpredictable network behavior associated with activity within the network and changes made to the technology platform;
- Constraints on network performance and scalability;
- Potential indirect links between the platform used by the network and a specific organization or individual responsible for technology development and stabilization and impacting the ability to use this platform;
- Network participant anonymization mechanisms can be implemented, and data or the fact of transactions between network participants can be concealed with the help of cryptographic solutions.

A **private blockchain** with a limited number of identified nodes implies that there is an operator managing the network, and that network participants can be identified and certain restrictions can be imposed on them. However, it is possible to implement both a centralized decision-making mechanism within the network and decentralized network management solutions. With regard to network management, the operator can represent one of the participants (a vertical model) or cause the network to be managed jointly by a consortium of participants. With regard to data privacy on a private network, access rights to certain objects, similar to conventional systems, could be divided.

Private blockchains have the following properties:

- A possibility to guarantee settlement finality using deterministic consensus;
- Stable and predictable network behavior;
- A possibility to optimize the network structure subject to performance and scalability requirements;

- A possibility to restrict data access using built-in mechanisms;
- Dependency on the network operator;
- Network participant anonymization mechanisms can be implemented, and data or the fact of transactions between network participants can be concealed with the help of cryptographic solutions.

A hybrid configuration based on a managed private blockchain network integrated with multiple public blockchain networks is also described by financial infrastructure participants [41]. When using a private blockchain, there is a near absence of "horizontal" solutions bringing together user participants with equal rights from multiple jurisdictions in a consortium. Pilot "vertical" solutions, constrained by a specific legal framework, controlled by a certain owner, and solving the owner's tasks (including solution monetization tasks) dominate the market. In contrast, for a public blockchain, in most cases, it is impossible to identify a certain owner of the technology and a controlling body or community, and this results in a significantly lesser interest from the regulator and makes it necessary to revise existing standards to adapt to new native tokens embedded in technology in accordance with the Web 3.0 concept [59].

PERFORMANCE AND SCALABILITY

This problem is known as the scalability trilemma [12, 36]:

A blockchain solution can only at most have two of the following three properties:

1. Decentralization (defined as the system being able to run in a scenario where each participant only has access to O (c*) resources, i.e. a regular laptop or small VPS).
2. Scalability (defined as being able to process O (n**) > O (c) transactions).
3. Security (defined as being secure against attackers with up to O (n) resources).

The first public blockchain platforms had significant performance constraints associated with substantial computing and communication costs attributable to the use of the proof-of-work consensus concept and non-deterministic public network architecture, and other constraints. As a result, the waiting time for a transaction to be accepted by the first blockchain networks could be as long as minutes, hours, or even days in case of any deviation from the normal network operation. The transaction rate gradually increased from 7 transactions per second in Bitcoin and 14 transactions per second in Ethereum to more than 1,000 transactions per second in Stellar, BitShares, and Waves based on the proof-of-stake consensus algorithm [35]. Later implementations of public blockchain platforms involve the use of a sharding mechanism and double-layer blockchain architecture, and the transfer of some functionality to blocks and other acceleration mechanisms, external to the core blockchain network, allowing one to benefit from even greater network performance [39, 40].

Private blockchain platforms use deterministic consensus models (most frequently those based on PBFT [37]). They allow to achieve greater performance - up to 20,000 transactions per second [38] or more.

Some financial infrastructure participants already offer the implementation of a hybrid model that uses more than one blockchain platform. The most common option is the use of a fast private blockchain platform with a deterministic consensus to work with public platforms containing native tokens, thereby ensuring settlement finality and the required level of data privacy [41].

Thus, the performance and scalability of market solutions allow for addressing challenges faced by the financial infrastructure without apparent limits, with a speed of more than 1,000 transactions per second and a possibility to scale the solution using sharding technologies and hybrid implementations, if necessary.

* c is the size of computational resources (including computation, bandwidth, and storage) available to each node.

** n is the size of the ecosystem in some abstract sense, with the assumption that transaction load, state size, and the market cap of a cryptocurrency are all proportional to n.

STANDARDIZATION OF REQUIREMENTS TO BLOCKCHAIN NETWORKS

Standardization of functional and non-functional requirements to blockchain platforms and other aspects of introducing standards to facilitate their use are crucial to implement DLT-based solutions.

In 2016, NSD initiated the establishment, within ISSA, of a working group of financial infrastructure participants to work with blockchain (the CSD Working Group on DLT). The Working Group, in cooperation with leading market participants from across the globe, issued the following reports:

1. Infrastructure for Crypto-Assets: A Review by Infrastructure Providers [42];
2. Distributed Ledger Technology: Principles for Industry-Wide Acceptance [43];
3. General Meeting Proxy Voting on Distributed Ledger. Product Requirements [44];
4. Table of ISO 20022 Messages Used for Voting at General Meetings [45].

The ISO 20022 universal financial industry message scheme and the single global identification system for financial market participants substantially facilitate interoperability between conventional systems and blockchain [46].

The International Standardization Organization (ISO) has the Technical Committee responsible for standardization of blockchain and distributed ledger technologies [47]. Several global consortiums bring together financial market participants, solution vendors, and representatives from other areas to create and implement open source blockchain platforms [48, 49].

The current level of standardization shows that market participants have a lot of work to do to reduce the cost of implementing and supporting blockchain platforms in commercial operation. For these purposes, an adequate number of global and sectoral bodies have been established, and the results of their work can be expected in the short to medium term.

BLOCKCHAIN GOVERNANCE

Blockchain solutions used within the financial infrastructure should be subject to requirements of continuity, reliability and technical support level, similar to the requirements applicable to conventional IT systems. NSD guarantees compliance with these requirements with the help of a dedicated blockchain network operator (selected by a consortium of network participants or the one spearheading the creation of and operating a certain blockchain network).

The main responsibilities of the operator are to:

1. Ensure platform reliability and security.
2. Set out and apply common usage rules that recognize the legal significance of platform content, and monitor observance of such rules by participants.
3. Ensure development of the platform and add new capabilities.
4. Scale the solution.

Operator requirements:

1. Neutrality with respect to business services deployed on the platform and participants' transactions.
2. Sustainability, self-sufficiency, distant planning horizon, and transparent business development strategy.
3. High level of business continuity, cybersecurity, and corporate governance.
4. Financial liability for failure to perform properly.

TOKENIZATION OF CASH

To implement some of the financial infrastructure functions, it is advisable to implement payment functionality directly on the blockchain in the form of a real-time gross settlement (RTGS) system [60] or to apply other settlement models. This functionality requires availability of cash within the blockchain and is accordingly classified by the ISSA Working Group by issuance method:

ISSUANCE METHOD	DEGREE OF RISK, FROM 1 TO 5	ISSUERS	COLLATERAL KEEPERS	EXAMPLES
Central Bank Digital Currency (CBDC)	1	Central banks	Central banks	Digital currency in China [16], E-Krona in Sweden [13]; Project Inthanon in Thailand [14]; Eastern Caribbean Central Bank; Central Bank of Uruguay [15]
Tokens backed by cash held in reserve accounts with the central bank and guaranteed by the central bank	2	Central securities depositories and/ or associations of commercial banks	Central banks	Digital Singapore dollar and the opportunity to use tokens issued by multiple central banks (Project Ubin involving the Bank of England and the Bank of Canada) [17]; Project Stella of the European Central Bank and the Bank of Japan [18]
Tokens backed by cash held in the central bank's general reserve account and not enjoying central bank guarantees	3	Central securities depositories and/ or associations of commercial banks	Central banks	Project Finality funded by 14 banks, formerly known as Utility Settlement Coin (USC) [19]
Tokens backed by cash deposits with a commercial bank	4	Commercial banks	Commercial banks	Signet Coin of Signature Bank [20]; Project JPM Coin of J.P. Morgan [21]
Tokens issued by organizations without a banking license	5	Mostly, trusts of cryptocurrency trading platforms	Commercial banks	Gemini Dollar from Gemini cryptocurrency exchange [22]; Paxos Standard (PAX) from Paxos [23]; Huobi HUSD from Huobi cryptocurrency exchange [24], and USD Coin from Circle and Coinbase [24]

The current model of risk allocation within the financial infrastructure and legislative restrictions prevent dealing in tokens issued by organizations without a banking license or native tokens, and force market participants who use these solutions to work in a limited number of jurisdictions.

The use of tokens backed by cash deposits with a commercial bank is fully controlled by a certain legal entity and entails risks due to the lack of control by the regulator. The first three models that have the least risks and are controlled by the regulator appear to be the most promising for use by central securities depositories.

A good example of blockchain usage is the digital currency plan announced by the People's Bank of China. The Chinese regulator plans to issue tokenized cash that will be 100% backed by the reserves. There will be no need to open a bank account to use this payment method, but KYC identification could be required.

Technically, the digital currency distribution mechanism will be two-tiered:

- Between the central bank and commercial banks
- Between commercial banks and individuals and entities.

The model is declared to have the following advantages:

1. The opportunity to more accurately calculate some macroeconomic indicators, such as inflation.
2. Better capabilities for real-time data collection, such as data regarding money creation, accounting and circulation, providing useful information for monetary policy makers.
3. Contributing to anti-money laundering, combating the financing of terrorism and tax evasion.
4. Internationalizing the use of the national currency – Yuan (CNY).
5. Decreasing information asymmetry between financial institutions and regulators.
6. Reducing the cost of cash money issuance (printing and minting).

Thus, the People's Bank of China can potentially gain control over socio-economic activities in the country through the issuance of digital money. It is also worth noting that the proposed digital currency cannot be a direct competitor to existing cryptocurrencies, such as Bitcoin or Ethereum, due to centralization of the issuance process and the lack of privacy when using the Chinese digital currency.

PRACTICAL EXPERIENCE

Commercial implementation of blockchain networks in the financial infrastructure did not gain popularity in the early years of the technology. In 2018, multiple reports were published, according to which:

1. Only 1% of CIOs indicated any kind of blockchain adoption within their organisations [10].
2. Only 8% of CIOs were in the short-term 'planning or [looking at] active experimentation with blockchain [10].
3. Only 4% out of 398 well-known blockchain projects at enterprises resulted in a production deployment [11].

Since 2015, NSD has gained extensive experience in implementing blockchain solutions for the financial infrastructure:

1. A solution to automate voting at general meetings (insert: picture about voting).
2. Two pilot commercial paper issues using smart contracts.
3. Pilot project for an OTC tri-party repo transaction.
4. Test transaction to raise funding by issuing tokens on blockchain.
5. Participation in a distributed digital depository project.
6. Active participation in international ISSA and Hyperledger working groups.
7. Providing advice to third-party projects involving tokenized assets.

After a series of pilot transactions, NSD has proceeded to commercial implementation of the technology and participation in building a regulatory framework for its further application in existing and emerging business lines. As part of this activity, blockchain solutions are looked at from three perspectives:

- cost effectiveness;

- a possibility to apply conventional services to new asset types; and
- a possibility to apply new services to conventional asset types.

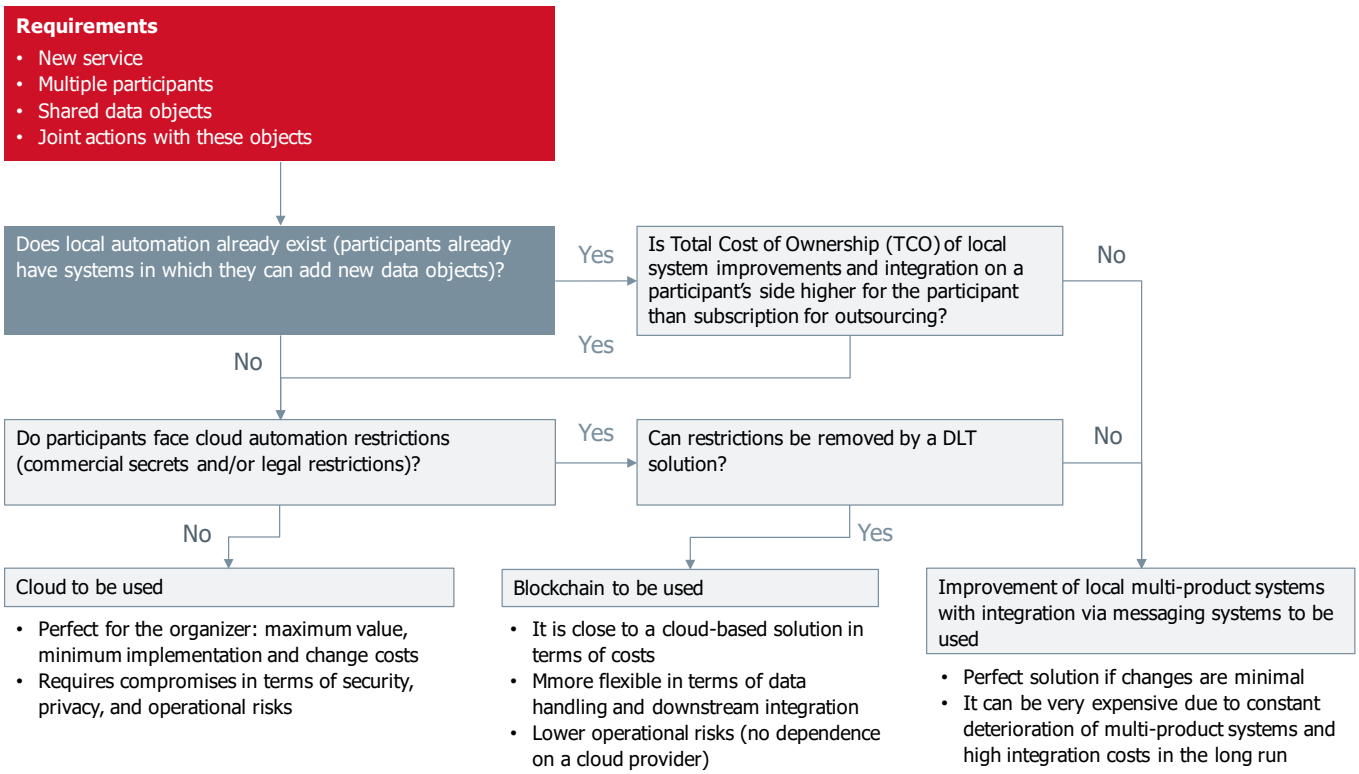
Each of these perspectives is discussed in more detail below.

Assessment of Cost Effectiveness of Blockchain

The key factor in choosing new technologies to be applied in business is significant cost saving as compared to existing business processes. The analysis of blockchain usage examples shows that there is an opportunity to achieve savings thanks to using this technology – versus centralized or cloud solutions – for creating new systems with multiple participants (regardless of the area of application, be it, for example, financial infrastructure or logistics):

- Co-financing the creation and maintenance of a distributed architecture system;
- Reducing CAPEX thanks to their distribution between network participants and the shared use of system components.

The proposed method to analyze cost effectiveness is shown in the diagram below:



A Possibility to Apply Conventional Services to New Asset Types

The current and most popular technological solutions based on public blockchain platforms are native tokens. Institutional investors are not willing to take on risks associated with the loss of control over such assets during their storage and trading, and they need safekeeping and settlement services from the traditional financial infrastructure. Regulators, in turn, impose certain requirements to identification of holders of such assets and to monitoring of settlement of their transactions from the AML perspective, in line with the global trends in the field of control over financial flows in all jurisdictions.

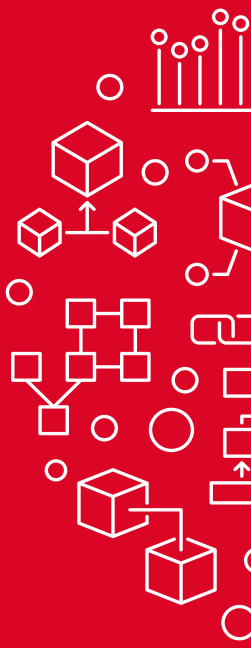
Accordingly, this demand could be met by existing financial institutions in strict accordance with the regulators' requirements, and existing financial institutions could provide their services for tokenized assets, including the issuance of new tokens, the servicing of existing ones (including safekeeping and settlements), and provision of various services

based on such tokens (similar to corporate action services or other services). Solutions for these types of services could be either centralized or decentralized or hybrid.

The development of the Web 3.0 concept or of the "Internet of data" [62] implies both the creation of a decentralized P2P management system for the next Internet generation, and the creation of many native payment and investment tools with decentralized management to implement this concept and their integration with the "Internet of things" [63, 64, 65]. Also, the micropayment service for which the Bitcoin network was originally designed is still relevant [8]. This makes it possible to create services for such assets in the long run.

Commodity markets and blockchain

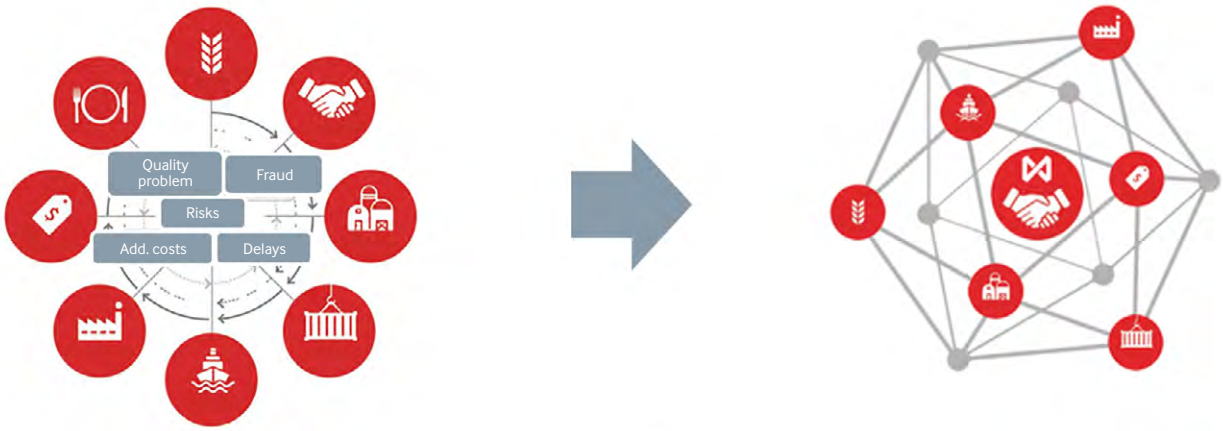
Commodity markets are traditionally considered more conservative from a technological point of view. However, the use of blockchain to automate this area is considered as one of the options to facilitate current business processes – from using letters of credit and common documentation to trade settlements and creating derivatives directly on a distributed ledger [67]. Integration of trading and supply chain management into a single ecosystem will give rise to additional benefits – transparency of the entire process, a new level of combating counterfeiting of any kind, and availability of a single source of data regarding transactions and movement of goods. Examples of such markets include the electricity market and agricultural commodity market [67].



Electricity trading without a wide product range and variety of logistics solutions could be organized in a similar way.

Due to the fact that the sector is one of the oldest and has a well-developed risk sharing infrastructure, the most likely scenario is step by step penetration of blockchain into the commodities trade - from the emergence of P2P marketplaces, and migration of certain business processes to blockchain (operations involving letters of credit and warehouse receipts) to the implementation of global blockchain ecosystems that not only support the full cycle of over-the-counter and exchange trading in various commodities and derivatives, but are also integrated with distributed supply chain management [68], factoring [70], insurance services, local tax systems, and regulatory bodies [66].

The first steps in this direction are already being taken by consortiums of global banking groups and global leaders in commodity trading [69], which clearly proves the viability of a model of distribution of development and implementation costs of such systems between all participants and the need for a blockchain solution, mainly if many parties that do not have a single set of standardized systems participate in the project.



TRANSPARENT AND UNIFIED LEDGER

of deals and settlements – unified document interchange

TRACEABLE LIFECYCLE

of each lot with all survey reports, origins and other details

IMMUTABILITY

of accounts through cryptography – no way for fraud or manipulation

A Possibility to Apply New Services to Conventional Asset Types

Around the globe, there are many pilot solutions for tokenized traditional assets, which are provided by third-party vendors or developed in-house. However, most of these remain at the pilot stage and never get to the stage of commercial operation [10, 11]. One of the reasons for this is the lack of clear advantages and confirmed demand for the technology from businesses, the state, or regulators.

An essential prerequisite for success is confirmed demand from at least one of the parties. This demand may be driven by:

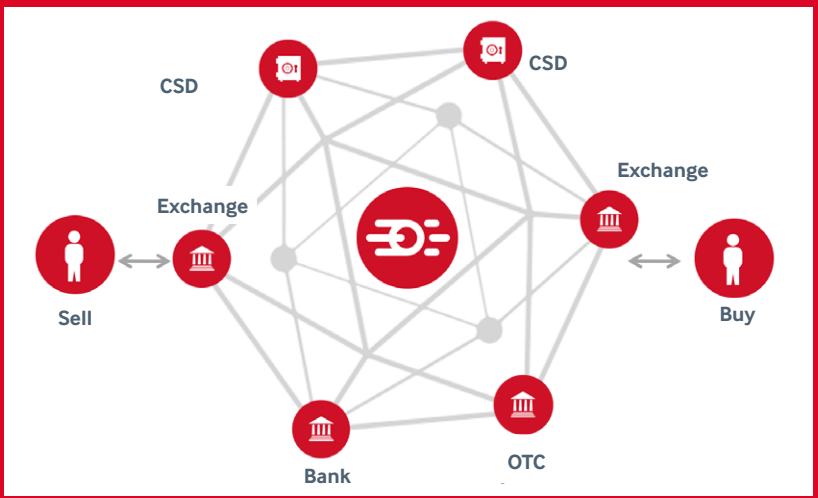
- Improved transaction transparency
- The impossibility to tamper with the ledger
- No need for reconciliation when using multiple systems
- Business process simplification due to a single document interchange system integrated with the settlement system
- Cost savings due to no need for multiple data duplication to ensure business continuity
- Additional investor confidence in a distributed asset management system
- Simplified application of various settlement models through the use of smart contracts
- Creation of a new funding instrument for a large number of retail investors (which the current infrastructure is not suited for)

The following factors also need to be checked:

- Is an asset to be tokenized sufficiently liquid?
- What type of blockchain (public or private) needs to be used?
- Who will issue the token on the blockchain?
- How will this blockchain be governed?
- How will the blockchain solution development costs be returned?

In the case of confirmed demand and certainty with the factors listed above, there is a reason to choose blockchain as the way to implement business requirements and provide new services. The advent of blockchain, similar to the advent of the Internet, can provide opportunities to implement new services the implementation of which is impossible using traditional architecture.

Decentralized Digital Depository



The Decentralized Digital Depository is a global distributed account management system that offers the following benefits:

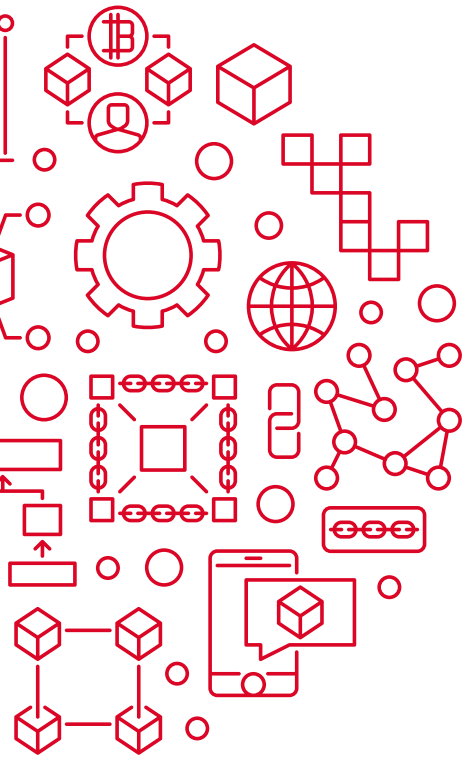
1. A single global account management system on the blockchain instead of local systems at each central securities depository or bank.
2. The account is owned and managed by the account holder (an individual or a legal entity), who also selects a bank to provide services for this account. There is no need to change the account details when changing banks. The same is true when changing account jurisdictions.
3. Should the bank go bankrupt, the complete set of data on the account balances in this bank remains in the distributed ledger, and the account holder can gain access to his account by having another financial infrastructure participant identify him.
4. In the event of a default of financial infrastructure in a certain jurisdiction, foreign investors may gain access to asset management through another partner in another jurisdiction.

CONCLUSIONS

Blockchain is undoubtedly one of the most promising technologies for the financial market infrastructure; however, it remains an alternative way to work with data (along with centralized and cloud solutions). The use of distributed ledger technology by the financial infrastructure makes it possible to simplify processes, as compared to the use of multiple centralized solutions, to improve the transparency of the financial market for the regulator, and to create an enabling environment for application of flexible settlement models directly on the blockchain.

For the purposes of providing new services and dealing with new asset types, the application of this solution could be economically feasible and logically relevant (compared with other implementation options). The current level of solutions in terms of data privacy requires traditional approaches to working with data and an adequate level of scalability and performance while using distributed ledgers.

A blockchain platform could facilitate the introduction of new settlement models and the provision of such services as, for example, factoring. Transferring the entire set of business processes associated with a certain asset or service type to blockchain, adding tokenized funds to the blockchain perimeter, and adapting the financial infrastructure to transactions in new asset types using distributed ledger technology seem to be the most cost-efficient option.



REFERENCES

[1] Narayanan, Arvind; Bonneau, Joseph; Felten, Edward; Miller, Andrew; Goldfeder, Steven (2016). Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton: Princeton University Press. ISBN 978-0-691-17169-2.

[2] US patent 4309569, Ralph Merkle, "Method of providing digital signatures", published Jan 5, 1982, assigned to The Board Of Trustees Of The Leland Stanford Junior University

[3] Merkle R.C. (1988) A Digital Signature Based on a Conventional Encryption Function. In: Pomerance C. (eds) Advances in Cryptology — CRYPTO '87. CRYPTO 1987. Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg

[4] Haber, Stuart; Stornetta, W. Scott (January 1991). "How to time-stamp a digital document". Journal of Cryptology. 3 (2): 99–111.

[5] Gartner. Market guide for blockchain consulting and proof-of-concept development services. 2018. https://gtnr.it/2NB9Pp3

[6] Bayer, Dave; Haber, Stuart; Stornetta, W. Scott (March 1992). Improving the Efficiency and Reliability of Digital Time-Stamping. Sequences

[7] "Hashcash - A Denial of Service Counter-Measure" (PDF). hashcash.org. 1 August 2002

[8] Nakamoto, Satoshi (October 2008). "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). bitcoin.org

[9] Project Bletchley Whitepaper Archived 11 January 2017 at the Wayback Machine, Microsoft, 2016-09-19. Retrieved 2016-12-24.

[10] "Hype Killer - Only 1% of Companies Are Using Blockchain, Gartner Reports | Artificial Lawyer". Artificial Lawyer. 4 May 2018. Retrieved 22 May 2018.

[11] https://www.pwc.com/m1/en/services/assurance/documents/accelerating-blockchain.pdf

[12] https://github.com/ethereum/wiki/wiki/Sharding-FAQ

[13] https://www.riksbank.se/en-gb/payments--cash/e-krona/e-krona-reports/e-krona-project-report-2/

[14] https://www.bot.or.th/Thai/PressandSpeeches/Press/News2562/n562e.pdf

[15] https://www.bis.org/publ/bppdf/bispap101.pdf

[16] https://info.binance.com/en/research/marketresearch/CBDC.html?fbclid=IwAR2Y7W5Jw8p0Am1486bwmgwltdJkJV5k-LN8sBg5YHIeP88iBfJ0ovFqnDM

[17] https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Cross-Border-Interbank-Payments-and-Settlements.pdf?la=en&hash=F7F232705054CC226297BF396608CA026C3C7139

[18] https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical190604_1.en.pdf?19a53d7118406fc74c32d7ab2565052d

[19] https://www.fnality.org

[20] https://tassat.com/press-releases/truedigital-launches-revolutionary-real-time-payments-platform-with-signature-bank

[21] https://en.wikipedia.org/wiki/JPM_Coin

[22] https://gemini.com/wp-content/themes/gemini/assets/img/dollar/gemini-dollar-whitepaper.pdf

[23] https://account.paxos.com/whitepaper.pdf

[24] https://loopring.org/resources/pwc-loopring-stablecoin-paper.pdf

[25] https://hackernoon.com/a-huge-list-of-cryptocurrency-thefts-16d6bf246389

[26] https://arxiv.org/pdf/1904.05234.pdf

[27] https://arxiv.org/ftp/arxiv/papers/1801/1801.03294.pdf

[28] https://www.businessinsider.com/bitcoin-price-government-auction-winners-2017-5

[29] https://eprint.iacr.org/2017/238.pdf

[30] https://zcoin.io/zcoins-privacy-technology-compares-competition/

[31] Ronald L. Rivest, Adi Shamir, Yael Tauman. How to leak a secret // Advances in Cryptology — ASIACRYPT 2001 / C. Boyd (ed.). — Berlin, Heidelberg : Springer-Verlag, 2001. — P. 552—565. — (Lecture Notes in Computer Science[en]. Vol. 2248).

[32] https://eprint.iacr.org/2019/508.pdf

[33] https://eprint.iacr.org/2017/1066.pdf

[34] https://zcoin.io/cryptographic-description-of-zerocoin-attack/

[35] Blockchain Quick Reference: A guide to exploring decentralized blockchain application development By Brenn Hill, Samanyu Chopra, Paul Valencourt https://books.google.ru/books?id=RcJoDwAAQBAJ&pg=PA36&lpg=PA36&dq=cryptokitty+ethereum+performance+references&source=bl&ots=ueYSfKMGld&sig=ACfU3U3v87VnUb83Ney6SOnxBH6C-MfcNw&hl=en&sa=X&ved=2ahUKEwi7wqeQtsvkAhXrIlsKHaHWDcY4ChDoATAAegQICBAB#v=onepage&q=cryptokitty%20ethereum%20performance%20references&f=false

[36] https://arxiv.org/abs/1801.04335

[37] http://stsam.irgups.ru/sites/default/files/articles_pdf_files/75-83.pdf

[38] https://arxiv.org/pdf/1901.00910.pdf

[39] https://test.ton.org/ton.pdf

[40] https://www.codementor.io/blog/blockchain-scalability-5rs5ra8eej

[41] http://www.dtcc.com/~/media/Files/Downloads/WhitePapers/Crypto-Asset-Whitepaper-2019.pdf

[42] https://issanet.org/e/pdf/2018-10_ISSA_report_Infrastructure_for_Crypto-Assets.pdf

[43] https://issanet.org/e/pdf/2018-06_ISSA_DLT_report_version_1.0.pdf

[44] https://issanet.org/e/pdf/2017-11_General_Meeting_Proxy_Voting_on_Distributed_Ledger_v2-1.pdf

[45] https://issanet.org/e/pdf/MDR_Part3_ProxyVoting_Maintenance_2014_2015_DLT_aligned.xlsx

[46] http://www.pynx.net/asianregionalpublic2018/files/Session%2011_Alexandre%20Kech_SWIFT.pdf

[47] https://www.iso.org/committee/6266604.html

[48] https://hyperledger.org

[49] https://entethalliance.org

[50] H. Jin, X. Dai, J. Xiao, Towards a novel architecture for enabling interoperability amongst multiple blockchains, in: 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS), IEEE, pp. 1203–1211.

[51] BTCRelay. a bridge between the Bitcoin blockchain & Ethereum smart contracts, 2018. http://btcrelay.org/.

[52] V. Buterin, Chain interoperability, 2016. https://static1. squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+ Interoperability.pdf

[53] https://www.ingwb.com/media/2667864/assessing-interoperability-solutions-for-distributed-ledgers.pdf

[54] https://cosmos.network/cosmos-whitepaper.pdf

[55] https://blockstream.com/sidechains.pdf

[56] https://arxiv.org/pdf/1908.03999.pdf

[57] https://www.hyperledger.org/projects/quilt

[58] https://polkadot.network/PolkaDotPaper.pdf

[59] Matthew Hodgson (9 October 2016). "A decentralized web would give power back to the people online". TechCrunch. AOL Inc. Retrieved 1 December 2016.

[60] https://www.ecb.europa.eu/paym/intro/governance/shared/pdf/201709_dlt_impact_on_harmonisation_and_integration.pdf

[61] European Business Organization Law Review March 2019, Volume 20, Issue 1, pp 111–137| Cite as Blockchain and Smart Contracting for the Shareholder Community

[62] "Q&A with Tim Berners-Lee, Special Report". businessweek.com. Retrieved 14 April 2018.

[63] http://ceur-ws.org/Vol-2161/paper6.pdf

[64] https://arxiv.org/ftp/arxiv/papers/1801/1801.02027.pdf

[65] Berners-Lee, T.; Hendler, J.; Lassila, O. (2001). "The Semantic Web". Scientific American. 2841 (5): 34. Bibcode:2001SciAm.284e..34B. doi:10.1038/scientificamerican0501-34.

[66] https://www.bcg.com/publications/2018/reality-check-blockchain-commodity-trading.aspx

[67] https://uis.brage.unit.no/uis-xmlui/handle/11250/2563235

[68] https://www.tradelens.com/

[69] https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/about-deloitte/20181002-DLT-v01.pdf

[70] http://ceur-ws.org/Vol-2334/DLTpaper2.pdf

Address: 12, Spartakovskaya Street,
Moscow, Russian Federation
Phone: +7 495 234-48-27
E-mail: blockchain@nsd.ru
Website: nsd.ru/en