Information systems. Computer sciences. Issues of information security

Информационные системы. Информатика. Проблемы информационной безопасности

UDC 004
https://doi.org/10.32362/2500-316X-2023-11-3-7-16

RESEARCH ARTICLE

Development of a research environment for the operational and computational architecture of central bank digital currency software

Alexander S. Albychev [1, 2, @],
Stanislav A. Kudzh [2]

[1] *The Federal Treasury of the Ministry of Finance of the Russian Federation, Moscow, 101000 Russia*
[2] *MIREA – Russian Technological University, Moscow, 119454 Russia*
[@] *Corresponding author, e-mail: albychev@mirea.ru*

Abstract
Objectives. The development and implementation of information and computing architecture and information support for a state central bank digital currency (CBDC) is based on the selection of a software and hardware platform, including technologies and methods for supporting interaction between the elements of the computing complex. The implementation of CBDC technologies significantly depends both on the operational and computing architecture, as well as on the technological characteristics of the means for implementing digital currency information support, which determines the need to develop an appropriate research environment. Thus, the present study sets out to develop an infrastructure for the experimental research environment of the operational and computing architecture used to provide information support for the CBDC.
Methods. Digital technologies required for forming an CBDC implementation stack are under development in many countries of the world. The basis for the formation of a software and hardware complex for providing CBDC information support is comprised of theoretical and experimental studies into contemporary digital transaction management tools.
Results. The main architectural and technological components that make up the CBDC operational and computing environment comprise operational and computing architectures, blockchain technologies, consensus algorithms, and various forms of digital currencies. Five CBDC operational and computing architecture options are presented. Information models of interaction between the participants in transactions of the central bank digital currency were studied with the aim of establishing the effects of an architectural solution to the characteristics of the computing complex used to provide information support. Features of various digital currencies in the form of accounts and tokens were analyzed.
Conclusions. A research environment infrastructure for the CBDC operational and computing information support architecture has been developed. The prerequisites for a comprehensive analysis of the technological characteristics of the CBDC operational and computing environment are set out along with a comparison of operational and computing architecture variants. As a result of the analysis, a summary list of the characteristics of the studied architectures is drawn up. This provides for selecting the optimal operational and computing architecture depending on the requirements imposed on the CBDC.

Keywords: digital currency, central bank digital currency, blockchain, consensus algorithm, digital currency architecture

• **Submitted:** 20.03.2023 • **Revised:** 14.04.2023 • **Accepted:** 20.04.2023

For citation: Albychev A.S., Kudzh S.A. Development of a research environment for the operational and computational architecture of central bank digital currency software. *Russ. Technol. J.* 2023;11(3):7–16. https://doi.org/10.32362/2500-316X-2023-11-3-7-16

Financial disclosure: The authors have no a financial or property interest in any material or method mentioned.

The authors declare no conflicts of interest.

НАУЧНАЯ СТАТЬЯ

Среда исследований операционно-вычислительной архитектуры информационного обеспечения цифровой валюты центрального банка

А.С. Албычев [1, 2, @],
С.А. Кудж [2]

[1] *Федеральное казначейство Министерства финансов Российской Федерации, Москва, 101000 Россия*
[2] *МИРЭА – Российский технологический университет, Москва, 119454 Россия*
[@] *Автор для переписки, e-mail: albychev@mirea.ru*

Резюме
Цели. Внедрение и разработка информационно-вычислительной архитектуры и информационного обеспечения цифровой валюты центрального банка (ЦВЦБ) страны основываются на выборе программно-аппаратной платформы, включая технологии и способы взаимодействия элементов вычислительного комплекса. Внедрение технологий ЦВЦБ существенно зависит как от операционно-вычислительной архитектуры, так и от технологических характеристик конкретной реализации информационного обеспечения цифровой валюты, что определяет необходимость разработки соответствующей среды исследований. Цель статьи – разработка инфраструктуры среды экспериментальных исследований операционно-вычислительной архитектуры информационного обеспечения ЦВЦБ.
Методы. Развитие цифровых технологий не сформировало стек реализации ЦВЦБ, а комплекс технологических реализаций находится в разработке во многих странах мира. Основой для формирования программно-аппаратного комплекса информационного обеспечения являются теоретические и экспериментальные исследования современных инструментов цифрового управления транзакциями.
Результаты. Рассмотрены архитектурные и технологические компоненты, составляющие операционно-вычислительную среду цифровой валюты центрального банка: операционно-вычислительные архитектуры, блокчейн-технологии, алгоритмы консенсуса, формы представления цифровых валют. Представлено 5 вариантов операционно-вычислительных архитектур ЦВЦБ. Проведено исследование информационных моделей взаимодействия участников транзакций ЦВЦБ, направленных на установление степени влияния архитектурного решения на характеристики вычислительного комплекса информационного обеспечения. Проанализированы особенности цифровых валют в форме аккаунтов и токенов.
Выводы. Разработана инфраструктура среды исследований операционно-вычислительной архитектуры информационного обеспечения ЦВЦБ. Созданы предпосылки для комплексного анализа технологических характеристик операционно-вычислительной среды ЦВЦБ. Проведен анализ вариантов операционно-вычислительных архитектур. В результате анализа сформирован сводный перечень характеристик приведенных архитектур. В зависимости от требований, предъявляемых к ЦВЦБ, на основе этого перечня может быть выбрана наиболее адекватная операционно-вычислительная архитектура.

Ключевые слова: цифровая валюта, цифровая валюта центрального банка, блокчейн, алгоритм консенсуса, архитектура цифровой валюты

• **Поступила:** 20.03.2023 • **Доработана:** 14.04.2023 • **Принята к опубликованию:** 20.04.2023

Для цитирования: Албычев А.С., Кудж С.А. Среда исследований операционно-вычислительной архитектуры информационного обеспечения цифровой валюты центрального банка. *Russ. Technol. J.* 2023;11(3):7–16. https://doi.org/10.32362/2500-316X-2023-11-3-7-16

Прозрачность финансовой деятельности: Авторы не имеют финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

INTRODUCTION

The development of modern financial, electronic payment, digital currency and blockchain technologies [1] has led to the prospect of sovereign states issuing digital currencies. Central bank digital currencies (CBDCs) are under consideration by a number of states as a new form of monetary representation alongside existing currencies [2, 3]. Such digital currencies, which are managed by a state central bank (CB), are issued in a 1:1 ratio to the national currency.

CBDC research focuses on various aspects of digital currencies [3, 4]. Some studies consider performance issues associated with technological support for digital currencies [5–7], i.e., the ability to process a certain number of financial transactions in a period of time. Others focus on the reliability of data storage [3, 7, 8], security against unauthorized digital currency transactions [4, 7, 9], as well as privacy [7, 9, 10], as among the key characteristics of a CBDC.

Blockchain technologies [5, 11] are used in digital currencies to ensure the authenticity of transaction history. Meanwhile, consensus algorithms [7, 12, 13] are required to prevent the unscrupulous behavior of one or more participants in the blockchain network. In other words, in the absence of a single source of trustworthy information, there is a need for a consensus algorithm to avoid this.

As a rule, studies explore two ways of the digital currency storing data: accounts and tokens [8, 9, 14–16]. The first form of data storage implies that the account owner has some number reflecting the current account balance; here, financial transactions consist of changing the corresponding number in the participants of the transaction. Although tokens are described in less detail, in general they can be represented as a bundle of a unique token identifier and denomination. Each token is assigned a current owner, for example, using a unique owner identifier. Financial transactions in this case consist of changing the unique owner ID for one or more tokens.

Studies [7, 14, 17] have noted that one of the main issues in the development of CBDC is the choice of operational and computational architecture. An operational and computational architecture describes the participants of the system that ensures the functioning of a digital currency, as well as the connections between them. Some researchers use a different, broader term—CBDC design [5, 18]—which includes, among other things, details of the digital currency realization. When choosing the operational and computational architecture, it is important to consider both organizational requirements, such as the Know Your Customer (KYC) principle [6, 14, 19], along with the various technical aspects.

The aim of the article is to develop the infrastructure of the research environment of the operational and computational architecture of the information support of the central bank digital currency.

1. VARIANTS OF CBCD OPERATIONAL-COMPUTING ARCHITECTURE IMPLEMENTATION

Let us consider the variants of operational and computational architectures used to ensure the functioning of CBDC in terms of their advantages and disadvantages.

1.1. Centralized two-level architecture

As the simplest option in terms of architecture, we can consider a centralized two-level architecture, where the only organization that ensures the functioning of CBDC will be the CB (Fig. 1).

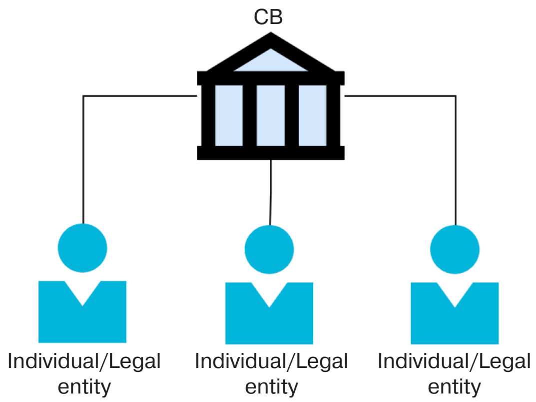

Fig. 1. Diagram of a centralized two-level CBDC architecture

In such a CBDC implementation variant, the only source of reliable information on the movement and ownership of funds is the CB, which also carries out all technological support. The CB performs both the issuance of digital currency and the processing of transactions. The advantages of this option include:

1) ease of implementation, since there is no need to coordinate the work of several organizations;
2) minimization of delays in transactions due to the absence of intermediaries;
3) the CB has a real-time access to all data.

However, this operational and computational architecture has significant disadvantages:

1) all technical support for CBDC must be provided by a single issuer—the CB;
2) organizational support of CBDC is also fully entrusted to the CB (e.g., compliance with the KYC principle).

With such an operational and computational architecture, the reliability of data storage and security can be provided with different quality levels depending on the implementation of the technological support of the data center.

1.2. Centralized three-level architecture

By supplementing the two-level architecture with an intermediate link in the form of private banks, a three-level architecture is formed. Private banks can help to reduce the organizational burden on CB by ensuring compliance with the KYC principle. A scheme of the three-level architecture is shown in Fig. 2.

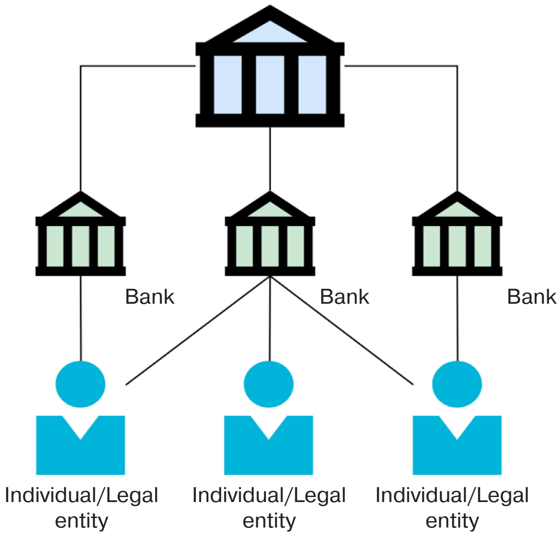

Fig. 2. Diagram of the centralized three-level architecture of CBDC

The advantages of this architecture are:

1) ease of implementation, since data storage and transaction execution are provided by the CB;
2) organizational support (compliance with the KYC principle) is distributed among the private banks;
3) the CB has a real-time access to all data;
4) the CB provides banks with a single tool for transactions.

The main disadvantage of this architecture is that all technical support for CBDC must be provided by a single issuer, i.e., the CB.

As in the two-level architecture, reliability of data storage and security in this case is also highly dependent on the Central Bank.

1.3. Four-level architecture with a single CBDC operator

In the article [7], several operational and computational architectures are proposed, one of which consists in transferring the technological support for the operation of the CBDC to a separate organization—the CBDC operator. The diagram in Fig. 3 shows the connection between the elements of the architecture.

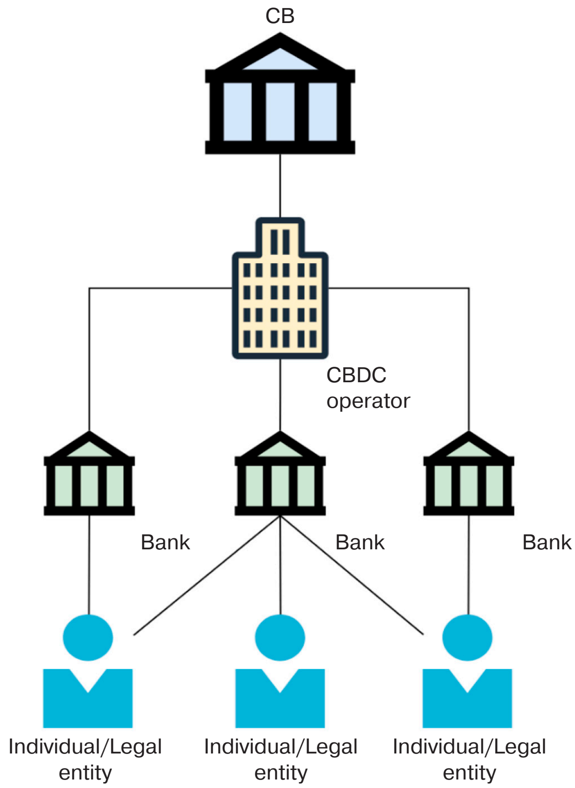

Fig. 3. Diagram of the four-level architecture with a single operator of CBDC

In many ways, this operational and computational architecture is similar to the three-tiered centralized architecture. However, the division of responsibility between the CBDC operator, CB and private banks offers the following additional advantages:

1) the resource-intensive task of transaction execution is ensured by the CBDC operator;

2) organizational support (compliance with the KYC principle) is distributed among the private banks;
3) CBDC operator provides banks with a single tool for transactions.

However, the disadvantages of such a four-level architecture are significant:
1) CB does not have access to all data in real time; a separate API is required to access transaction history;
2) all transaction data is under the control of one organization;
3) all technical support for CBDC must be provided by a single provider—the CBDC operator.

The listed disadvantages suggest that a monopoly on transaction processing may lead to unfair use of the CBDC system. In addition, as in the case of the centralized architectures described, the issue of scaling the transaction processing system becomes the task of one organization.

1.4. Four-level architecture with segmentation between several CBDC operators

The four-level architecture involving several CBDC operators (Fig. 4), also proposed in [7], solves a number of problems associated with the data monopoly: a single point of failure of the system is eliminated, along with an increase in scalability. This is achieved by segmenting the CBDC data.

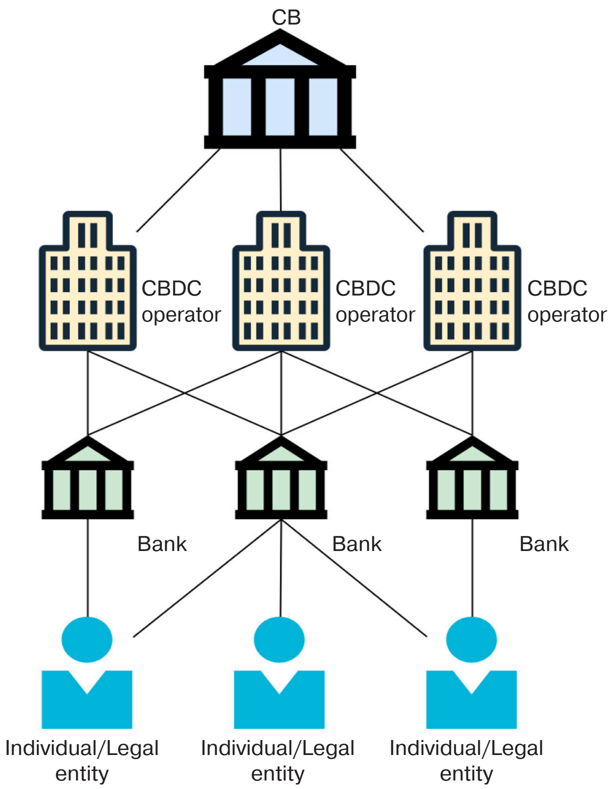

Fig. 4. Diagram of the four-level architecture with segmentation between several CBDC operators

The advantages of this architecture are as follows:
1) organizational support (compliance with the KYC principle) is distributed among the private banks;
2) computational workload of transaction processing is distributed among several CBDC operators.

The disadvantages include:
1) difficulty in accessing transaction history on the part of the CB due to CBDC data segmentation;
2) increasing complexity of transactions processing related to the involvement of two or more operators;
3) more complicated logistics of interaction between banks and operators due to the use of many-to-many communication.

Although there is no single point of failure, each segment in this architecture is the responsibility of only one organization; however, in the event of a failure, transaction data can be lost. It is also possible for an operator to unfairly use the CBDC system, although the scope is limited to a single segment.

1.5. Four-level architecture with segmentation and replication between several CBDC operators

In order to eliminate the disadvantages of an operational and computational architecture with segmentation, a refinement involving data replication between CBDC operators is proposed. As shown in Fig. 5, each segment must be replicated between multiple operators. Executing the transaction would require a consensus between the CBDC operators owning the segment. In such a case, the consensus algorithm can be flexibly selected to suit security and performance preferences.

The more CBDC operators are involved in the operation of a single segment, the higher the reliability of the system, but also the higher the redundancy of the stored data. The more CBDC operators are involved in transaction processing to ensure consensus, the more resistant the system is to unfair actions on the part of operators. However, at the same time the performance decreases.

The operating and computing architecture under consideration has the following advantages:
1) organizational support (compliance with the KYC principle) is distributed among the private banks;
2) computational workload of transaction processing is distributed among several CBDC operators;
3) operator disconnection does not lead to loss of data or availability of CBDC service;
4) availability of consensus algorithm when performing transactions allows operators to mutually verify results in order to avoid unfair actions.

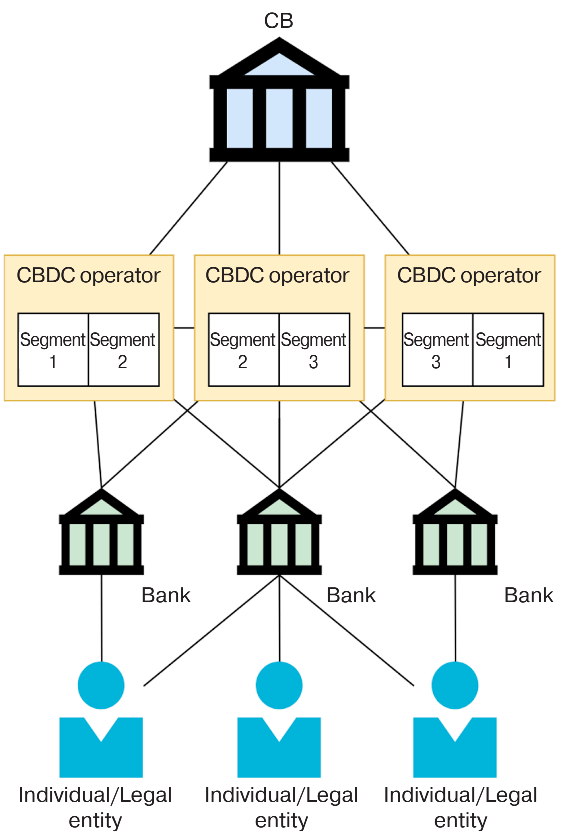

Fig. 5. Diagram of the four-level architecture with segmentation and replication between the several CBDC operators

The operating and computing architecture has a number of disadvantages:

1) difficult access to transaction history for CB due to its segmentation;
2) icreasing complexity of transactions related processing to the involvement of two or more operators;
3) more complicated logistics of interaction between banks and operators because of the use of many-to-many communication;
4) increased resource intensity of transaction processing and increase of the total volume of stored data due to redundancy.

2. RESEARCH ENVIRONMENT INFRASTRUCTURE

In order to solve this problem, we will develop a research environment infrastructure using virtualization technologies [20].

The blockchain network will include several organizations, each organization having one or more nodes [21]. Then the total amount of CPU, RAM, and disk space required for the experiment can be calculated by the formula:

$$R_{\text{total}} = \sum_{i=1}^{O} \sum_{j=1}^{N_i} \left(R_{ij} R_{\text{h}} + R_{\text{c}} \right),$$

where O is the number of organizations; N_i is the number of nodes in ith organization; R_{ij} is the amount of resource required for the jth node in the ith organization to function; R_{h} is the resource overhead for hypervisor operation, proportional to the allocated resource; R_{c} is the resource overhead for hypervisor operation required to keep the node running regardless of the amount of resource allocated to it.

Thus, assuming that the amount of RAM required by the nodes is invariant and equal to 2, $R_{\text{h}} = 0$, and $R_{\text{c}} = 0.2$, 22 GB of RAM will be required to maintain a CBDC model containing four organizations (one with 4 nodes and the other three with 2 nodes each).

In the case of a digital currency implementation in the form of accounts, the transactions themselves (without considering the computational complexity of the consensus algorithm) have a computational complexity of $O(1)$, since changes of one or two scalar values are trivial operations. However, when implementing digital currencies in the form of tokens, transactions can have greater computational complexity.

Both forms of digital currency representation can be considered in terms of financial transaction transparency for regulatory authorities. If the history of transactions is stored, as in the case of accounts with numerical representation of the balance, it can be extremely difficult to trace the ways of transferring a certain amount of money. It is problematic to reliably distinguish the fact of targeted funds expenditure from other funds if they are passed through a single account. On the contrary, with tokens, when each monetary unit has its own unique identifier, the transaction history reflects the transfer of a particular monetary unit from one owner to another. Thus, it is possible to implement a mechanism to identify misuse of funds.

In order to carry out research on the technological parameters of the information support of the data center, an infrastructure for the research environment using *VMWare ESXi*[1] was developed.

The tools used are:

- modified version of *Repexlab*[2] for work with *VMWare ESXi*;
- plug-in *vagrant-vmware-esxi*[3];
- utility program *ovftool*[4];
- system *Ansible*[5];
- monitor *atop*[6].

[1] https://www.vmware.com/products/esxi-and-esx.html. Accessed March 17, 2023.

[2] https://github.com/rnd-student-lab/repexlab. Accessed March 17, 2023.

[3] https://github.com/josenk/vagrant-vmware-esxi. Accessed March 17, 2023.

[4] https://developer.vmware.com/web/tool/4.4.0/ovf. Accessed March 17, 2023.

[5] https://www.ansible.com/. Accessed March 17, 2023.

[6] https://www.atoptool.nl/. Accessed March 17, 2023.

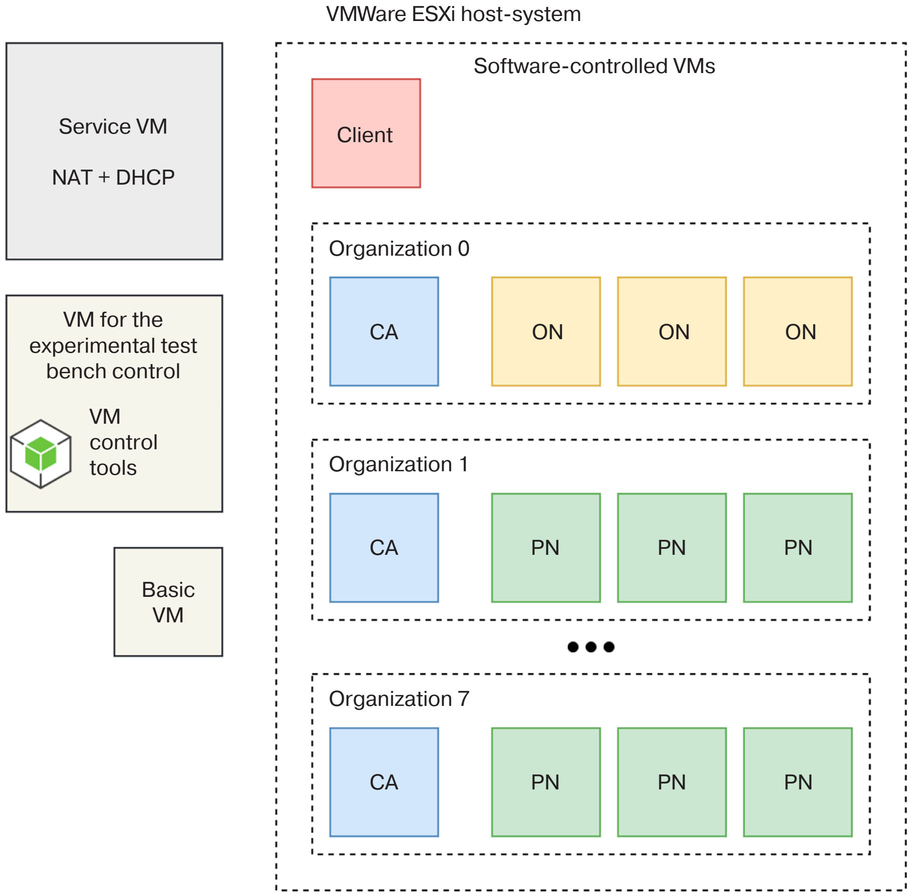

Fig. 6. Scheme of the research environment infrastructure (NAT—network address translation; DHCP— dynamic host configuration protocol; CA—certification authority; ON—orderer node; PN—peer node)

The general configuration diagram is shown in Fig. 6.

The experiment management toolkit was hosted on a dedicated virtual machine (VM). The service VM was used to configure the NAT network and DHCP service, assigning IP addresses according to the MAC addresses of the software-managed VMs. A pre-configured VM was used (in Fig. 6, the Base VM), which was subsequently cloned to create and configure the software-managed VMs. When all 33 software-managed VMs were started and provisioned, the central processing unit (CPU) load from the installed monitoring system appeared to be acceptable, as shown in Fig. 7.

3. ANALYSIS OF THE OPERATIONAL COMPUTING ARCHITECTURES CHARACTERISTICS

A number of properties characterizing the considered operational and computational architectures are shown in the table. On their basis, a selection of the architecture most adequate to the requirements for the CBDC can be made.

The application of consensus algorithms becomes expedient when a segment is located at several CBDC operators. Regardless of the form of presentation of the CBDC, the design should determine the acceptable number of operators per segment, which implies experimental research. This requires the development of an experimental-research environment for the operation of the CBDC model.

CONCLUSIONS

A review of the architectural and technological components that make up a CBDC has been carried out. The main operational and computational CBDC architecture variants, which differ in their essential characteristics, are compared. A consolidated list of characteristics of the given operational and computational architectures formed as a result of the analysis is drawn up. On the basis of this list, the most adequate operational-computing architecture depending on the CBDC requirements can be selected. The discussion has been mainly focused on the forms of representation of digital currencies and their impact on the properties of digital currencies. While storing digital currencies in the form of accounts may be less resource-intensive than storage in the form of tokens, the history of digital

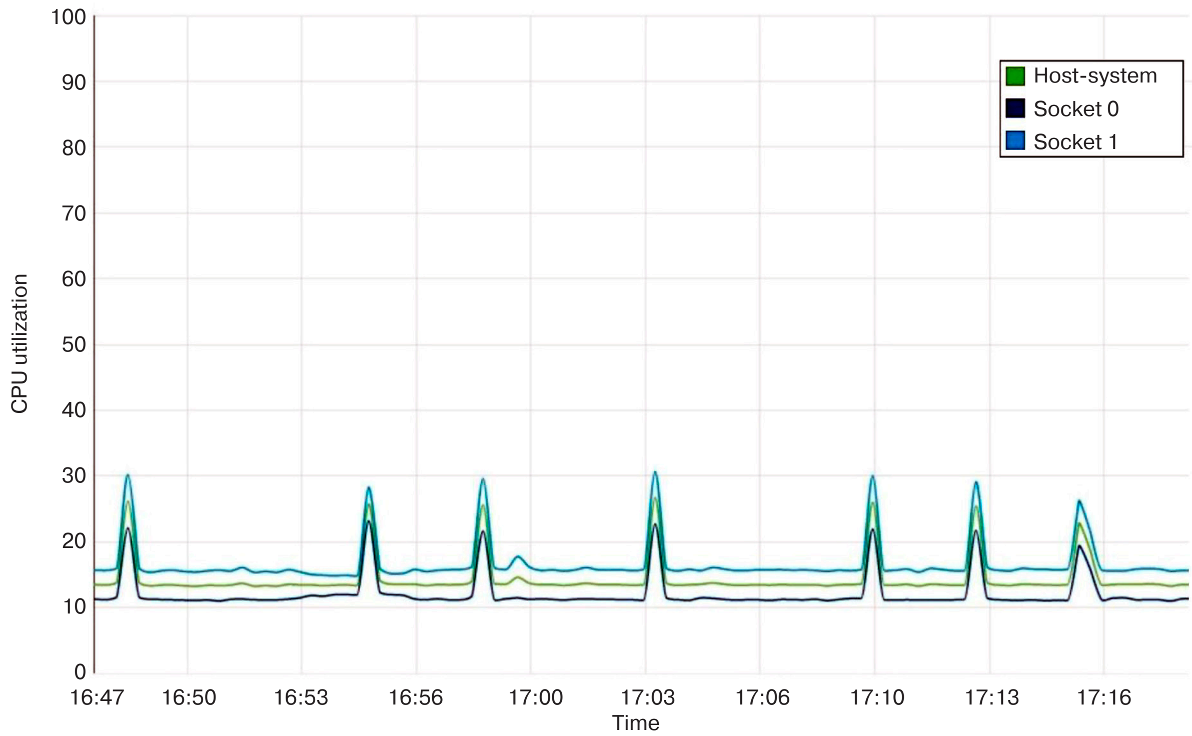

Fig. 7. CPU resource utilization after provisioning of VMs under *VMWare ESXi* hypervisor

Table. Characteristics of operational computer architectures

Characteristic	A1	A2	A3	A4	A5
Technological infrastructure for storing the entire volume of data is provided by CB	+	+	–	–	–
Technological infrastructure for processing the entire volume of transactions is provided by CB	+	+	–	–	–
Technological infrastructure for storing all data is provided by the operator	–	–	+	+	+
Technological infrastructure for processing the entire volume of transactions is provided by the operator	–	–	+	+	+
Technological infrastructure is distributed and scaled horizontally among several operators	–	–	–	+	+
KYC principle is carried out by CB	+	–	–	–	–
KYC principle is carried out by private banks	–	+	+	+	+
The system will retain partial functionality when one operator's services are disconnected	–	–	–	+	+
The system will remain fully operational when one operator's services are disconnected	–	–	–	–	+
The system will retain partial functionality when CB services are disconnected	–	–	+	+	+
The system will remain fully operational when CB services are disconnected	–	–	+	–	–
CB has real-time access to all data	+	+	–	–	–
Operators verify the results of transaction processing	–	–	–	–	+
Data backup with independent operators	–	–	–	–	+
No cross-segment transactions	+	+	+	–	–
CB provides a platform for individuals/legal entities	+	–	–	–	–
CB provides a platform for banks	+	+	–	–	–
CB provides a platform for operator(s)	–	–	+	+	+
Operator(s) provide(s) a platform for banks	–	–	+	+	+
Private banks provide a platform for individuals/legal entities	–	+	+	+	+

Note: A1—centralized two-level architecture; A2—centralized three-level architecture; A3—four-level architecture with a single CBDC operator; A4—four-LEVEL architecture with segmentation between several CBDC operators; A5—four-level architecture with segmentation and replication among several CBDC operators.

currency transactions in the form of tokens provides a more convenient tool for auditing.

The infrastructure of the research environment for the operational and computational architecture used to provide CBDC information support has been developed, on which basis prerequisites for a comprehensive analysis of technological characteristics of the operational and computational environment of CBDC can be identified. Further research should be focused on the choice of technological support for the development of the experimental and research environment, including experimental and analytical evaluation of the dependence of the characteristics of CBDC on the consensus algorithm used, the form of presentation of the digital currency, and various other parameters.

Authors' contribution. All authors equally contributed to the research work.

REFERENCES

1. Allen F., Gu X., Jagtiani J. Fintech, cryptocurrencies, and CBDC: Financial structural transformation in China. *J. Int. Money Finance.* 2022;124(3–4):102625. https://doi.org/10.1016/j.jimonfin.2022.102625
2. Wang Y.-R., Ma C.-Q., Ren Y.-S. A model for CBDC audits based on blockchain technology: Learning from the DCEP. *Res. Int. Bus. Financ.* 2022;63(3):101781. https://doi.org/10.1016/j.ribaf.2022.101781
3. Choi K.J., Henry R., Lehar A., Reardon J., Safavi-Naini R. A proposal for a Canadian CBDC. *SSRN Electron. J.* 2021. https://doi.org/10.2139/ssrn.3786426
4. Chu Y., Lee J., Kim S., Kim H., Yoon Y., Chung H. Review of offline payment function of CBDC considering security requirements. *Appl. Sci.* 2022;12(9):4488. https://doi.org/10.3390/app12094488
5. Zhang T., Huang Z. Blockchain and central bank digital currency. *ICT Express.* 2022;8(2):264–270. https://doi.org/10.1016/j.icte.2021.09.014
6. Tsai W.-T., Zhao Z., Zhang C., Yu L., Deng E. A multi-chain model for CBDC. In: *2018 5th International Conference on Dependable Systems and Their Applications* (*DSA*). Dalian, China: IEEE; 2018. P. 25–34. https://doi.org/10.1109/DSA.2018.00016
7. Jin S.Y., Xia Y. CEV Framework: A central bank digital currency evaluation and verification framework with a focus on consensus algorithms and operating architectures. *IEEE Access.* 2022;10:63698–63714. https://doi.org/10.1109/ACCESS.2022.3183092
8. Opare E.A., Kim K. A compendium of practices for central bank digital currencies for multinational financial infrastructures. *IEEE Access.* 2020;8:110810–110847. https://doi.org/10.1109/ACCESS.2020.3001970
9. Lee Y., Son B., Park S., Lee J., Jang H. A survey on security and privacy in blockchain-based central bank digital currencies. *J. Internet Serv. Inform. Secur.* 2021;11(3):16–29. https://doi.org/10.22667/JISIS.2021.08.31.016
10. Ballaschk D., Paulick J. The public, the private and the secret: Thoughts on privacy in central bank digital currencies. *Journal of Payments Strategy & Systems.* 2021;15(3):277–286. Available from URL: https://www.bundesbank.de/resource/blob/880792/7f4b5efd53026f51a9f53b176859e715/mL/digital-currencies-ballaschk-paulick-data.pdf
11. Monrat A.A., Schelén O., Andersson K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access.* 2019;7:117134–117151. https://doi.org/10.1109/ACCESS.2019.2936094
12. Hang L., Kim D.-H. Optimal blockchain network construction methodology based on analysis of configurable components for enhancing Hyperledger Fabric performance. *Blockchain: Res. Appl.* 2021;2(1):100009. https://doi.org/10.1016/j.bcra.2021.100009
13. Lashkari B., Musilek P. A comprehensive review of blockchain consensus mechanisms. *IEEE Access.* 2021;9:43620–43652. https://doi.org/10.1109/ACCESS.2021.3065880
14. Auer R., Böhme R. The technology of retail central bank digital currency. *BIS Quarterly Review*. 2020. Available from URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3561198
15. Ozili P.K. Central bank digital currency research around the world: a review of literature. *J. Money Launder. Control.* 2022;26(2):215–226. https://doi.org/10.1108/JMLC-11-2021-0126
16. Bordo M.D., Levin A.T. Central bank digital currency and the future of monetary policy. *NBER Working Paper Series*. 2017;Working Paper 23711. https://doi.org/10.3386/w23711
17. Zhang J., Tian R., Cao Y., Yuan X., Yu Z., Yan X., et al. A hybrid model for central bank digital currency based on blockchain. *IEEE Access.* 2021;9:53589–53601. https://doi.org/10.1109/ACCESS.2021.3071033
18. Allen S., Čapkun S., Eyal I., Fanti G., Ford B.A., Grimmelmann J., et al. Design choices for central bank digital currency: Policy and technical considerations. *NBER Working Paper Series*. 2020;Working Paper 27634. https://doi.org/10.3386/w27634
19. Chaum D., Grothoff C., Moser T. How to issue a central bank digital currency. *SNB Working Papers*. 2021;3. 38 p. https://doi.org/10.2139/ssrn.3965032
20. Netto M.A.S., Menon S., Vieira H.V., Costa L.T., de Oliveira F.M., Saad R., et al. Evaluating load generation in virtualized environments for software performance testing. In: *2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum*. 2011. P. 993–1000. https://doi.org/10.1109/IPDPS.2011.244

21. Albychev A.S., Ilin D.Y., Nikulchev E.V., Magomedov S.G. Development of a methodology for experimental studies of technologies for central bank digital currencies. *Vestnik of RSREU.* 2022;82:136–146 (in Russ.). https://doi.org/10.21667/1995-4565-2022-82-136-146

About the authors

Alexander S. Albychev, Deputy Head of the Federal Treasury, The Ministry of Finance of the Russian Federation (6/1, Bol'shoi Zlatoustinskii per., Moscow, 101000 Russia); Head of the State Financial Technologies Department, Institute for Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: albychev@mirea.ru. https://orcid.org/0000-0001-9632-7806

Stanislav A. Kudzh, Dr. Sci. (Eng.), Professor, Rector, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: rector@mirea.ru. Scopus Author ID 56521711400. https://orcid.org/0000-0003-1407-2788

Об авторах

Албычев Александр Сергеевич, заместитель руководителя, Федеральное казначейство Министерства финансов Российской Федерации (101000, Россия, Москва, Большой Златоустинский пер., д. 6, стр. 1); заведующий кафедрой «Государственные финансовые технологии» Института кибербезопасности и цифровых технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: albychev@mirea.ru. https://orcid.org/0000-0001-9632-7806

Кудж Станислав Алексеевич, д.т.н., профессор, ректор ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: rector@mirea.ru. Scopus Author ID 56521711400. https://orcid.org/0000-0003-1407-2788

Translated from Russian into English by Lyudmila O. Bychkova
Edited for English language and spelling by Thomas A. Beavitt