IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 March 2024, accepted 2 May 2024, date of publication 9 May 2024, date of current version 16 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3399113

APPLIED RESEARCH

Retail Central Bank Digital Currency Design Choices: Guide for Policymakers

ANASTASIA TSAREVA AND MIKHAIL KOMAROV, (Senior Member, IEEE)
Graduate School of Business, HSE University, 101000 Moscow, Russia

Corresponding author: Anastasia Tsareva (an.tsareva.2001@gmail.com)

The publication was prepared within the framework of the Academic Fund Program at HSE University (grant N°23-00-035 "Overcoming the limitations of the interaction of cyber-physical systems in heterogeneous networks of the Internet of Remote Things using machine learning methods").

ABSTRACT Central bank digital currencies (CBDCs), particularly retail CBDCs intended for daily public transactions, have garnered attention globally. Benefits of CBDC implementation heavily depend on its design, which, if not executed well, can lead to technological and privacy issues. Through case study examination, decision tree analysis, and IT system architecture modelling, this paper identifies key architectural and technological facets of retail CBDCs. We propose a decision-making methodology allowing policymakers to tailor CBDC design to their unique circumstances and requirements. In achieving this, we first outline core and optional CBDC properties and examine design choices from existing projects, form a list of assumptions affecting CBDC architecture and design, as well as vital design choices and trade-offs. Our research includes the development of 36 distinct IT architectures for CBDCs, demonstrating how different assumptions linked to policy objectives can influence the CBDC system design. These findings offer practical guidelines for policymakers, emphasizing the necessity to clearly define and prioritize policy objectives to form correct assumptions before applying our methodology. This approach helps to ensure that the CBDC design is optimally aligned with national economic goals and technological capabilities.

INDEX TERMS CBDC, central bank digital currency, decision-making methodology, design choices, IT architecture.

I. INTRODUCTION

Central bank digital currency (CBDC) - a digital form of money that is issued and backed by a Central Bank (CB) - has been a topic of significant interest in recent years. Countries around the world explore the potential benefits and drawbacks of issuing digital versions of their national currencies. There is a distinction between wholesale and retail (or general purpose) CBDC. In this paper, we focus on retail CBDC.

As of July 2023, there are four production-ready retail CBDCs in the world – in the Bahamas, the Eastern Caribbean, Nigeria and Jamaica [1]; around 100 countries are exploring CBDCs [2]. The reasons why CBs are exploring CBDCs include decreased cash use, accelerated by the Covid-19 pandemic, and the rise of digital currencies like Bitcoin. Moreover, CBDCs may offer benefits such as enhanced accessibility, offline payments, innovation potential, monetary control, and security. However, these potential advantages of CBDCs are not guaranteed, and the specific benefits of a CBDC depend on how it is designed and implemented. As with any new financial technology, there is a risk that the introduction of a CBDC could have unintended negative consequences including risks to monetary sovereignty, financial stability, technological vulnerabilities or design mistakes, privacy concerns [3]. Many countries are still in the early stages of investigating the case for introducing a CBDC, with key design choices still under consideration. In designing a retail CBDC, there is a myriad of key architectural and technological aspects that should be considered. Elsayed and Nasir [4] highlight that "there is no global consensus regarding the underlying technology of CBDCs". Indeed, despite the growing body of research, significant theoretical gaps remain regarding the optimal architectural and technological frameworks for implementing retail CBDCs. These gaps are crucial as they pose a challenge for policymakers and financial institutions aiming to build a CBDC system. This paper seeks to address these gaps by proposing a structured methodology to assist in

The associate editor coordinating the review of this manuscript and approving it for publication was Francisco J. Garcia-Penalvo.

TABLE 1. CBDC definitions.

№	Sources	Definition
1.	Löber & Houben (2018); BIS (2020); World Economic Forum (2023).	a digital form of CB money that is different from balances in traditional reserve or settlement accounts [5, 6, 7]
2.	U.S. Department of the Treasury (2022)	a digital form of a country's sovereign currency [8]
3.	Son, Bilgin, & Ryu (2022)	a CB-issued digital currency denominated in the national unit of account [9]
4.	Kiff, Alwazir, Davidovic, Farias, Khan, Khiaonarong, ... & Zhou (2020)	a digital representation of sovereign currency that is issued by a jurisdiction's monetary authority and appears on the liability side of the monetary authority's balance sheet [10]
5.	Allen, Čapkun, Eyal, Fanti, Ford, Grimmelmann, ... & Zhang (2020)	fiat currencies issued by CBs in digital form in place of, or as a complement to, physical currency [11]
6.	Yao (2018)	a credit-based currency in terms of currency value, a crypto-currency from a technical perspective, an algorithm-based currency in terms of implementation and a smart currency in application scenarios [12]
7.	Board of Governors of the Federal Reserve System (2022)	a digital liability of the Federal Reserve that is widely available to the general public [13]
8.	Lovejoy, Fields, Virza, Frederick, Urness, Karwaski, ... & Narula (2022)	a currency that is electronic, a liability of the CB denoted in the national unit of account, broadly available, and used for retail and person-to-person payments [14]
9.	Bjerg (2017)	electronic, universally accessible, CB issued money [15]
10.	Barrdear & Kumhof (2016)	universally accessible and interest-bearing CB liability, implemented via distributed ledgers, that competes with bank deposits as medium of exchange [16]
11.	Pocher & Veneris (2021)	institutional frameworks of programmable money investigated by many CBs [17]
12.	Jiang & Lucero (2021)	a kind of digital liability issued and guaranteed by a sovereign CB that operates in a digital infrastructure with potentially more affordances than previous kind of currency, such as electronic accounts or paper cash [18]
13.	Bech & Garratt (2017)	gives broad access to accounts at the CB [19]

the decision-making process for designing CBDC systems. We address the following research questions, using case study examination, decision tree analysis, IT system architecture modelling:

- What are the key design choices and trade-offs in CBDC systems?
- What assumptions affect CBDC architecture and design?
- What target architecture could look like depending on the assumptions of the CBDC?

Research on CBDC design choices can help policymakers understand the potential impacts of different design choices and make informed decisions. In this paper, four major terms are used: design choice, assumption, trade-off, and add-on. The central concept in the research is technology and architecture design choice. Design choices involve a set of trade-offs (decisions to accept one option over another). Design choices are based on a variety of factors (assumptions), such as priorities, constraints, requirements of the system, etc. Every assumption includes a list of questions to be answered to determine design choices. Add-on is a feature that enhances the functionality of the system and can be implemented at any CBDC system (although some designs can facilitate their implementation).

II. METHODS

Methods of the research include:

- Comparison analysis of existing research which can help to identify key issues and challenges related to CBDC design, as well as existing approaches and solutions.
- Case studies: Studying the experiences of countries or organizations that have implemented or are in the process of implementing CBDCs can provide valuable insights into the design and implementation process, as well as the potential impacts and outcomes of CBDCs.
- Decision tree analysis: a modelling tool which resembles a tree, where each branch represents a possible decision, outcome, or reaction. The model inputs questions (assumptions) leading to a decision.
- IT Systems Architecture Modeling: a technique used to describe the structure of an IT system which can be used for understanding and planning the interaction of the system components, exploring different scenarios, and testing the feasibility of different approaches. Also, such models can serve as a reference during implementation and maintenance. Specifically, conceptual (logical) models are used to describe the logical components of the system and their relationships.

In terms of paper's methodology, four major terms are used: design choice, assumption, trade-off, and add-on. The central concept in the research is design choice. Design choice refers to a decision to be made on the CBDC's technology and architecture. Design choices involve a set of trade-offs. A trade-off refers to a decision to accept one option over another. Design choices (incl. trade-offs) are based on a variety of factors (assumptions), such as the priorities, constraints, requirements of the system, etc. Every assumption includes a list of questions to be answered which determine design choices. Add-on is a feature that enhances the functionality of the system, it can be implemented at any system (although in some realizations it can be done easier and bring more value) and does not directly affect design choices (but can be affected by other assumptions).

III. LITERATURE REVIEW AND IDENTIFICATION OF KEY DESIGN CHOICES AND ASSUMPTIONS

To identify key design choices for retail CBDC it is necessary to clearly understand what a CBDC is in the first place, drawing on a broad range of existing literature. Table 1. presents definitions suggested by different researchers.

TABLE 2. Properties of various forms of money: Cash, Bank deposits, Central bank Reserves, CBDC.

Property	Cash	Bank deposits	CB reserves	Retail CBDC
Electronic		✓	✓	✓
CB issued	✓		✓	✓
Universally accessible	✓	✓		✓

The examples of definitions above suggest that there is no consensus on the definition of a CBDC. Some authors (e.g., [8], [15]) provide only a very general description of CBDC, while others (e.g., [6]) attribute to CBDCs the features of crypto currencies. The variety of definitions and the absence of consensus among scholars illustrate the complexity and evolving nature of CBDC conceptualization.

CBDC can be defined using comparison with other forms of money [14], [15], [19], [20], see Table 2.

CBDCs, apart from deposits, are digital currencies issued and backed by a Central Bank. Deposits, on the contrary, are created when banks issue loans: Whenever a bank makes a loan, it simultaneously creates a matching deposit in the borrower's bank account [21]. CBDCs are electronic (in contrast to cash). CBDCs differ from CB reserves in that they are accessible to the general public. To get a deeper understanding of what defines CBDC, let us consider its features suggested by different authors:

1) Issuance by a CB [10], [13], [14], [15], [16], [22];
2) Legal tender [8], [10], [23];
3) Liability of the CB (CB backed) [10], [16], [17], [22], [23];
4) Convertibility one-for-one into other forms of money [6], [8], [20], [23];
5) Electronic form [14], [15], [16], [22], [23];
6) Universal accessibility (availability to general public) [13], [14], [15], [16];
7) Programmability [10], [17];
8) Ability to make offline transactions [6];
9) Interest bearing instrument [16];
10) Decentralization [16].

Out of 10 features listed above, decentralization might be the most complex one and needs clarification. Decentralization refers to the distribution of power, authority, or decision-making in a system or network. In the context of digital currencies, decentralization implies that CBDC platform does not rely on a single authority (a CB) to issue, manage, and control the currency. Instead, these functions are distributed among various participants or nodes in the network, based on a consensus mechanism. According to Buterin [24], the co-founder of Ethereum, there are three types of decentralization: architectural, political, and logical. Although CBDCs can be architecturally decentralized, they are always politically and logically centralized. Architectural decentralization is achieved through a DLT – a single database where multiple identical copies are distributed among several participants [25]. DLT enables the decentralized management and storage of transactional data across a network of participants or nodes, without a central authority maintaining a single copy of the ledger [26]. Nodes maintain copies of the transaction history, making it difficult to alter the data [27].

Such features as consistent availability, resistance to cyberattacks, compliance with AML and CFT, high throughput, scalability, security, disaster recovery, and interoperability are not included in the table since these non-functional requirements can be attributed to any large-scale financial system of national importance.

Out of the 10 core features of CBDC described above, six (1-6) can be defined as core ones. If at least one of the core features is missing, the system cannot be considered a retail CBDC. Therefore, design decisions cannot affect them. The last four features (7-10) can be considered as additional (optional) features rather than core or obligatory ones. While these features may have certain benefits in certain contexts, they are not necessary for a CBDC. Consequently, design decisions can affect them.

Currently, there are many research projects in progress around the world related to the CBDC. Around the globe, many CBs are researching or even piloting CBDC projects. In the USA, the Boston Federal Reserve Bank and MIT's Project Hamilton focuses on CBDC transactions' speed, scalability, and fault tolerance [14]. This initiative, rooted in centralized trust and the UTXO transaction mode, showcases strengths in privacy and transaction scalability but confronts challenges in auditability and future adaptability. Parallel to this, China's digital yuan, the E-CNY, offers the uniqueness of functioning like cash, with the innovative feature of offline transactions simply by closely shaking phones [18]. Sweden's e-krona, developed on the Corda DLT platform using UTXO model, presents a hybrid model where the CB plays a pivotal role in issuing the currency, commercial banks execute retail transactions, with notaries preventing double-spending [28].

Design choices considered in existing research include: permissioning, access model, privacy-enhancing technology, signatures, anonymous transactions, holding limits, decentralization, fungibility, architecture, offline mode, programmability, interest bearing, and data model [10], [11], [17], [22], [23], [29], [30], [31], [32]. Although some authors consider offline mode, Privacy-Enhancing Technology (PET), and possibility to conduct anonymous transactions as design choices, we believe that these are not design choices, but rather assumptions which affect design choices:

- The level of anonymity required for the CBDC can be an important factor to consider in determining the access model. Token-based CBDCs offer a higher level of anonymity than account-based CBDCs, as they do not require user identification for every transaction. Moreover, whether the

TABLE 3. Architecture types.

	Single-tier architecture	*Two-tier architecture*	*Hybrid*
Issuing party	CB	CB	CB
Onboarding and KYC responsibility	Commercial banks / payment service providers (PSPs)	Commercial banks / PSPs	Commercial banks / PSPs
Transactions handling	CB (all retail transactions)	PSPs (all retail transactions) CB (wholesale transactions)	CB and PSPs (all retail transactions)
Advantages	• Simplicity. • Financial inclusion promotion due to direct relationship between the CB and end-users. • Reduced counterparty risk: the CB is the sole issuer and guarantor of the CBDC. • Faster and cheaper transactions.	• Reduced operational and technological burden on the CB. • Maintains the role of commercial banks and PSPs in the financial system, promoting stability. • Allows for more innovation and competition in the provision of CBDC-related services, as intermediaries can develop their own solutions.	• Allows the CB to restart the payment system if intermediaries fail (in case the CB keeps the full ledger, with all the information on the conducted transactions). • Combines advantages of single-tier and two-tier architectures.
Disadvantages	• Increased operational and technological burden on the CB. • Possible disintermediation of commercial banks and payment service providers. • Privacy concerns, as the CB would have direct access to transaction data of all users.	• Increased counterparty risk: transactions involve multiple parties. • Possible exclusion of unbanked and underbanked populations if they cannot access services from intermediaries. • Reduced level of transaction efficiency and increased cost compared to single-tier architecture.	• Increased complexity in the coordination and synchronization of ledgers between the CB and intermediaries. • Reduced level of transaction efficiency and increased cost compared to single-tier architecture. • Combines disadvantages of single-tier and two-tier architectures.

CB wants to allow users to conduct anonymous transactions affects PET.

• Offline mode will play a role in determining data model. UTXO-based model may be more challenging to implement in an offline scenario, as the user would need to track multiple UTXOs and their corresponding balances locally on their device. Moreover, offline mode affects key management model.

• PETs are a part of privacy assumption for data model design choice. Advanced PETs are easier to implement UTXO models. For instance, in UTXO models Mimblewimble protocol can be used to reduce the amount of open data in each transaction.

Programmability, holding limits, and interest bearing are add-ons rather than design choices or assumptions since they can be implemented at any system. Programmability refers to whether developers can code rules into a CBDC system. Such rules can be embedded at any CBDC system: centralized or decentralized, based on token-based or account-based models, etc. The possibility to bear interest and hold limits are examples of simple programmability which is why they can also be characterized as add-ons.

Moreover, there are some design choices (permissioning and fungibility) highlighted by other authors which in essence have one straightforward answer (there are no options, no trade-offs for CBDC).

• Permissioning: Permissioned / Permissionless. CBDC system should be permissioned because in a permissionless CBDC system anyone can participate in the network without any approval or authorization from the CB which goes against the core principles of central banking – maintaining financial stability and regulating monetary policy.

• Fungibility: Fungible / Non-Fungible Units. Fungibility means that individual units of the currency are interchangeable and indistinguishable from one another. CBDC should be fungible since CBDC is intended to function as a digital representation of a country's fiat currency.

The limitations of the research include the necessity to analyze the access model (account-based or token-based) and the data model (UTXO or account balance data model) as a combined design choice due to their interdependency. Signatures design choice should be expanded to digital signatures and key management design choice. Architecture type, and decentralization design choices remain as described in existing research.

IV. MAPPING CBDC DESIGN: FROM CORE ARCHITECTURES TO DIGITAL SIGNATURES

A. ARCHITECTURE TYPE: SINGLE-TIER / TWO-TIER / HYBRID

Auer and Böhme [31] identified three CBDC architectures: single-tier, two-tier, and hybrid. These differ in the involvement of intermediaries and distribution mechanisms, but in each case, the central bank is the sole issuer of CBDC. Key features, as well as advantages and disadvantages of three architecture types, are summarized in Table 3.

According to Pocher and Veneris [17], two-layer models (which include two-tier and hybrid architectures) may be favored by CB, as they traditionally interact with commercial banks and PSPs rather than with public end-users.

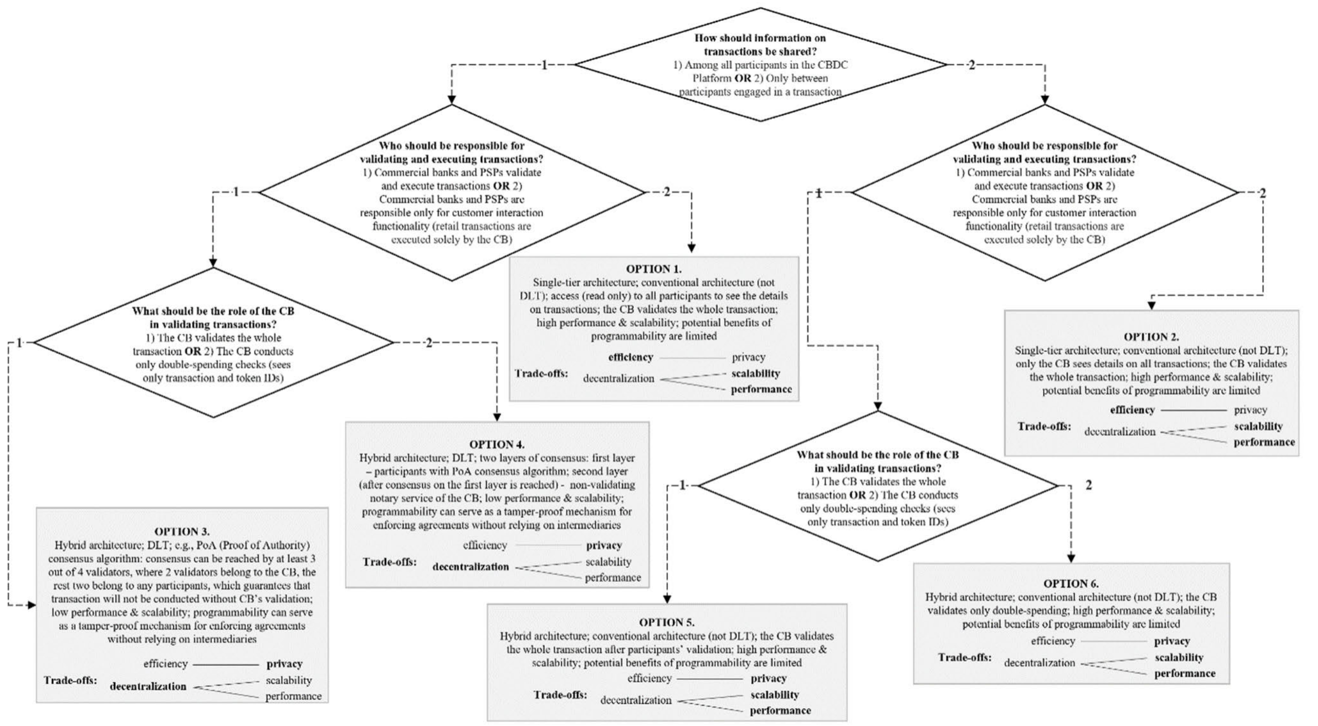


FIGURE 1. Decision-making process on architecture type and decentralization design choices.

Such models can leverage existing customer-facing services and avoid unnecessary duplication of KYC resources. Some argue that two-tier architecture does not warrant the CBDC label [31]. Indeed, in the two-tier architecture, the CB remains responsible only for the issuance of the wholesale CBDC, the retail part is not a direct claim on the CB (currency is not CB backed) and, therefore, such system cannot be considered a proper retail CBDC system. Earlier in this paper, 6 core features of CBDC were identified. If at least one of the core features is missing, the system cannot be considered a retail CBDC. Two core features are missing in the case of two-tier architecture: issuance by a CB and liability of the CB. Therefore, two-tier architecture cannot be used for a retail CBDC.

From advantages and disadvantages described in Table 3, a trade-off between transaction efficiency and privacy can be derived. In the one-tier architecture, the CB has direct access to transaction data of all users, but transactions can be settled very fast as there are no intermediaries. In the hybrid architecture, there is a reduced level of transaction efficiency due to involvement of intermediaries but there is a possibility for commercial banks and PSPs not to share their clients' data with the CB (in this system anonymity of a client towards the CB can be achieved).

Assumption affecting the architecture type design choice is responsibility for retail transactions execution. If the CB argues that retail transactions should be executed by commercial banks and other payment service providers, then a hybrid architecture type should be chosen. In case the CB is supposed to be a sole transactions executor, single-tier architecture is the option. Since architecture design choice is closely interconnected with decentralization design choice, the decision-making process on architecture design choice (illustrated as decision tree) is embedded into the decision-making process on decentralization design choice (Fig. 1).

B. DECENTRALIZATION DESIGN CHOICE

DLT can be used as the underlying infrastructure for CBDCs, providing a secure and transparent way to manage transactions and records. Benefits of DLT usually include resilience (fault tolerance), security (attack resistance), transparency, efficiency (through removal of intermediaries), decentralization of power, immutability. Let us consider all the benefits stated above through CBDC perspective.

1) RESILIENCE (FAULT TOLERANCE)

DLT is considered to make the system more resilient because it is not dependent on a single central authority. In CBDC the CB is the only participant that can issue digital currency. CBDC, according to its core features, is a liability of the CB guaranteeing that every token is CB backed. Therefore, the CB, being the operator of the platform, must participate in the verification of all transactions, thus being a single point of failure. Moreover, all nodes in the CBDC platform run the same client software, which also poses a threat in case this software has a bug. This eliminates the resilience advantage that DLT provides.

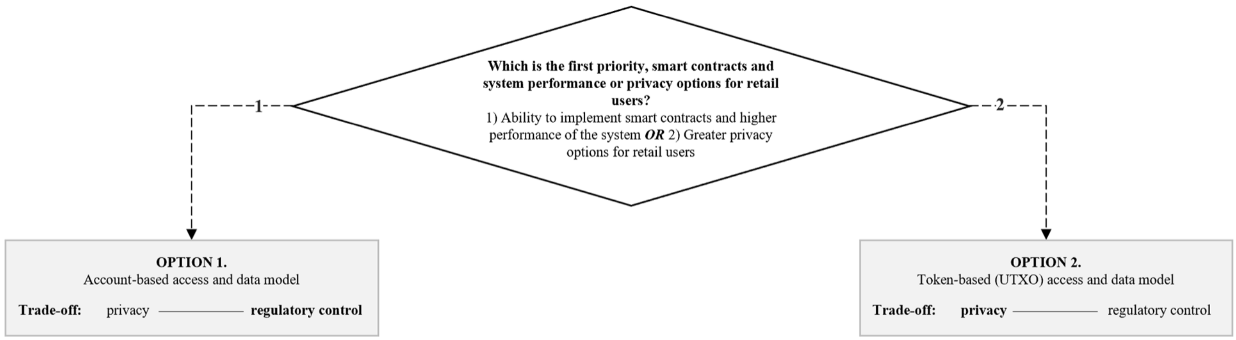


FIGURE 2. Decision-making process on access and data model design choice.

2) SECURITY (ATTACK RESISTANCE)

If one node on the network is compromised, the rest of the network remains secure. However, in CBDC if the CB is compromised, the whole system is compromised since CB is operator of the platform.

3) IMMUTABILITY

After records are written into a distributed ledger, they cannot be altered by any other party.

4) TRANSPARENCY

In systems employing DLT all participants have access to the same information which allows for increased accountability.

5) EFFICIENCY

DLT may increase efficiency and reduce the time it takes to complete transactions by removing intermediaries since transactions can be conducted and verified directly by participants. The end users of CBDC are the citizens of a country who have no access to the CBDC platform where only second-tier-banks and CB operate. Moreover, the CB should check every CBDC transaction, being a bottleneck of the platform and making it less efficient.

6) DECENTRALIZATION OF POWER

When implementing DLT in CBDC platform, there still will always be a node (or a cluster of nodes) of a CB that will have more rights than other network participants. For example, the CB is the only participant that can issue digital currency which eliminates the decentralization of power advantage that DLT brings.

Among the six potential advantages of DLT, transparency and immutability remain the most significant. Depending on the CBDC requirements, the transparency advantage might not be important or even desired for CBDC. The immutability feature can be used to distribute trust and governance in countries where the CB has a lower level of trust. Consequently, the need for transparency and distribution of trust and governance within the CBDC platform can be considered as assumptions defining the decentralization design choice.

All in all, CBDCs cannot be fully decentralized (even from architectural perspective). This position is confirmed by other authors. McKinsey [33] claims that CBDCs are typically centralized by design, as they are issued and managed by a CB or government. According to Rahman [34], the CBDC is centralized since the nature of the CB is centralized. The decentralized model of CBDC proposed in the paper [34] is only for international transactions between member countries, where a decentralized CBDC is issued and managed jointly by many CBs. According to National Bank of Ukraine [35], use of DLT for decentralizing the transaction validation function contradicts the principle that only the CB may issue CBDC. Other authors do not see contradiction between CBDC and DLT but state that CBDCs do not necessarily deploy DLTs [16], [17]. If the CB decides to use DLT for the digital currency's underlying infrastructure, consensus algorithm is required to ensure that all participants in the network agree on a single version of the shared ledger, maintaining consistency, integrity, and security [36]. Moreover, DLT type should be chosen: blockchain, block-based directed acyclic graph, or transaction-based directed acyclic graph [37].

Alternative to DLT is a conventional centralized database system. In this case, the CB is the sole trusted authority responsible for the validation, confirmation, and security of transactions, as well as the maintenance of the CBDC ledger. Centralized databases have advantages like ease of implementation and control, as well as high performance and scalability. They can be verifiable ledgers where a single entity or organization maintains control over the database, but the data recorded in the ledger can be independently verified by other parties (e.g., through authenticated data structures) [11], [38]. Fig. 1 presents the decision-making process on architecture type and decentralization design choices.

C. ACCESS AND DATA MODEL

The key distinction between token-based and account-based models is the form of verification needed when a transaction is executed [39]. Token-based model relies on the ability of the payee to verify the validity of the payment object [5]. In an account-based model, the identity of the account holder is the form of verification needed when a transaction is executed.

The first assumption influencing the design choice is implementation of smart contracts. Smart contracts are easier to implement in an account-based system where an account can be a smart contract, which stores and manages data.

Performance is the second assumption. Account-based systems are more efficient: a transaction is processed by deducting the transaction amount from the sender's account balance and adding it to the recipient's one. In a UTXO-based model, a transaction references previous transactions as inputs and creates new outputs. This involves multiple UTXOs management, which is more data-intensive and computationally expensive, especially for large transactions with many inputs or outputs. Moreover, since an account-based model updates account balances directly, it is easy and fast to check the state at any given time. In a UTXO-based model, the balance of an address is determined by summing up the values of all UTXOs associated with that address. Although UTXO-based systems have the advantage of transaction independence, managing and searching through UTXOs and validating the history of UTXOs can become resource-intensive as the number of transactions grows. Therefore, account-based systems tend to demonstrate higher performance.

Another assumption is privacy. UTXO-based systems can potentially offer greater privacy than account-based ones [17], [40].

While in UTXO model transactions are traceable, it is harder to link transactions together to track the activities of a specific user, especially if the user uses different addresses for each transaction (e.g., this can be enabled by stealth-addresses). The UTXO model allows for implementation of advanced privacy-enhancing technologies (e.g., Mimblewimble protocol). Also, the UTXO model may provide more privacy because each transaction output can be spent separately, making it harder to link transactions together. Fig. 2 presents the decision-making process on access and data model.

D. USER DIGITAL SIGNATURES AND KEY MANAGEMENT

The CBDC system could use a no-signature approach, where transactions are not signed or use signatures which requires asymmetric cryptography implementation. The first assumption influencing the design choice is offline functionality. In offline-mode, direct communication with the commercial bank / PSP is not possible in real-time. Therefore, user signatures are required to serve as a means of validating and authorizing transactions conducted offline. Another important assumption is security. Digital signatures can help to protect against unauthorized modifications or fraudulent activities, ensuring that the transactions are genuine and that the payment details have not been tampered with. Performance is the third assumption. Digital signatures and the necessary verification processes can add complexity and potentially slow transactions. Consequently, if the CB's priority is transaction speed and scalability, digital signatures might be seen as a hindrance. In this regard, there is a trade-off between performance and security in terms of signatures: Stronger digital signatures can increase the security of a system by making it harder for malicious actors to tamper with transactions. However, digital signatures also increase the computational overhead of the system, slowing down transaction processing times and reducing overall efficiency.

In case user digital signatures are used, another question arises: Who should hold the private key. They can be held by users themselves (e.g., on their devices) or by the commercial banks / PSPs. The CB must not hold users' private keys. Otherwise, the key idea of digital signatures implementation (that only user can sign their transaction and, therefore, spend their money) is destroyed.

If private keys are held by users, users maintain control of their own digital assets and transactions, which strengthens the trust in the digital signature process. On the flip side, if a user stores the private key on a device without any backups and loses that device, it can have significant implications for the security and accessibility of the private key and associated data.

If a commercial bank or a PSP holds a user's private keys, it has control over the user's digital assets. The bank uses a user's private key to sign a transaction on their behalf, and anyone can verify the transaction using the corresponding public key. In terms of non-repudiation mechanism, since a commercial bank / PSP controls the private key, the commercial bank / PSP, not the user, would be the entity that could not deny having signed a transaction. This could still provide a measure of accountability within the banking system itself, but it would not provide non-repudiation from the user's perspective. Moreover, the commercial bank / PSP holding users' private keys becomes a single point of failure: If the commercial bank's / PSP's systems were compromised, attackers could potentially gain access to many users' private keys, leading to large-scale fraud or theft. While it is technically possible for a commercial bank / PSP to hold users' private keys and use digital signatures in this way, it would raise significant issues around security, trust, and the balance of power between commercial banks / PSPs and their customers. Still, users do not need to worry about protecting their private keys, which could be a benefit for individuals lacking the necessary skills or technology to securely manage a private key.

The design choice on where to store the private key depends on several assumptions:

1) Offline functionality: If offline functionality is required, the private keys should be stored on the user's device. Otherwise, the user will not be able to sign the transaction.

2) Infrastructure: If the existing infrastructure, such as mobile devices or secure hardware, can adequately support private key storage and management, then storing keys on users' devices could be feasible.

3) User competence: If it is assumed that users are knowledgeable, competent, and responsible enough to handle their private keys securely, then storing keys on users' devices could be feasible. If user competence is high, policymakers can let the user decide where to store their private keys.

There are two trade-offs between user control over their funds and user experience and between user control over

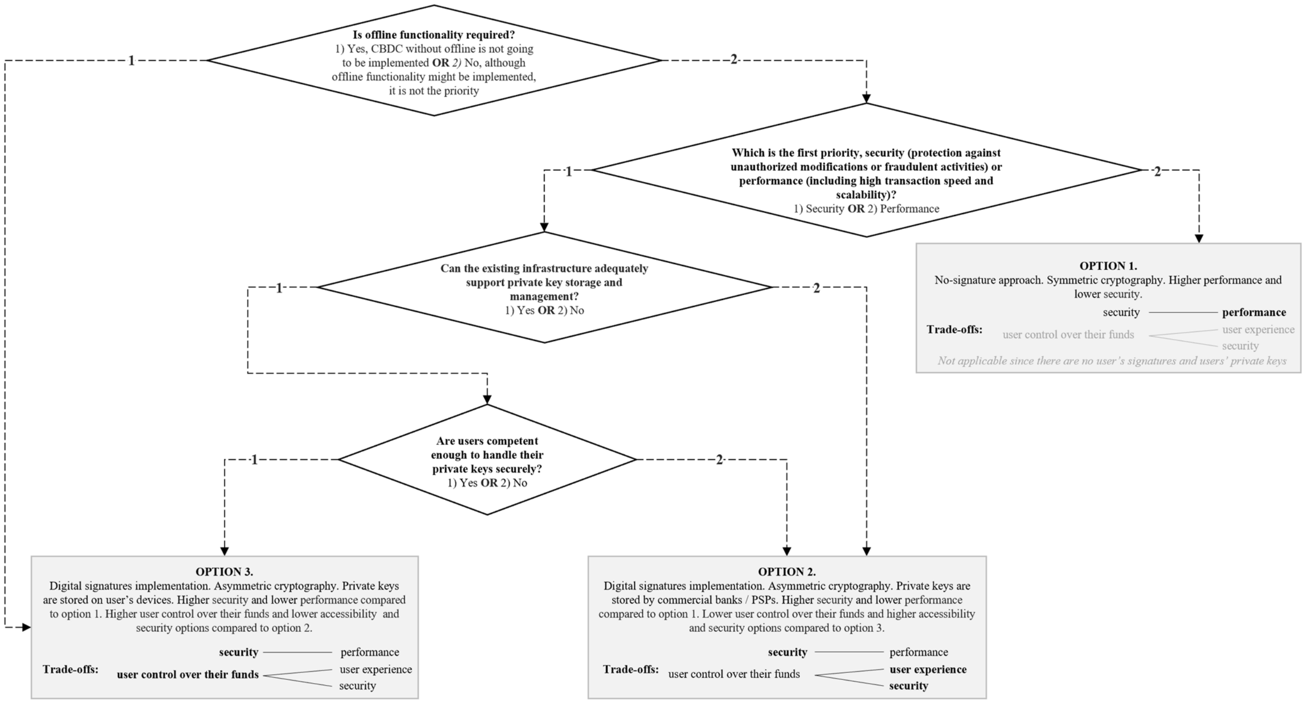


FIGURE 3. Decision-making process on user digital signatures and key management design choice.

TABLE 4. CBDC design choices, assumptions, trade-offs and high-level options in the design choice.

Design Choice	*Assumptions*	*Trade-Offs*	*High-Level Options in The Design Choice*
Architecture Type	• responsibility for retail transactions execution	• efficiency and privacy	• single-tier • hybrid
Decentralization	• transparency • distribution of trust and governance	• decentralization and scalability • decentralization and performance	• DLT • conventional architecture
Access and Data Model	• smart contracts • privacy • performance	• privacy and regulatory control	• token-based model • account-based model
User Digital Signatures and Key Management	• offline functionality • security • performance • infrastructure • user competence	• security and performance • user control over their funds and user experience • user control over their funds and security	• no-signature approach • implementation of signatures (private keys are stored by commercial banks / PSPs) • implementation of signatures (private keys are stored on users' devices)

their funds and security. Fig. 3 presents the decision-making process on digital signatures and key management design choice.

V. TARGET IT ARCHITECTURES FOR CBDC GIVEN DIFFERENT ASSUMPTIONS

CBDC design choices, assumptions, trade-offs and high-level options in the design choice are summarized in Table 4.

As shown in Fig. 1-3, there are 6 options in the architecture type and decentralization design choices, 2 options in the access and data model, 3 options in the user digital signatures and key management design choice. Since every group of options is independent, the total number of IT architectures given these design choice options is equal to the product of these options – 36 (given in the Appendix A). All possible combinations of assumption options and the resulting architectures are presented in the Appendix B. Two examples of CBDC conceptual architecture diagrams are presented below, illustrating the following aspects: retail CBDC platform contour; main participants; interactions between the participants; functions of every participant; for retail CBDC platform, API Layer, business logic layer and data layer are depicted; where private keys are stored (if any) illustrating the participant signing the transaction.

Fig. 4 presents an architecture diagram that is recommended for consideration when policymakers decide that:

1) Information on transactions should be shared among all participants in the CBDC Platform.

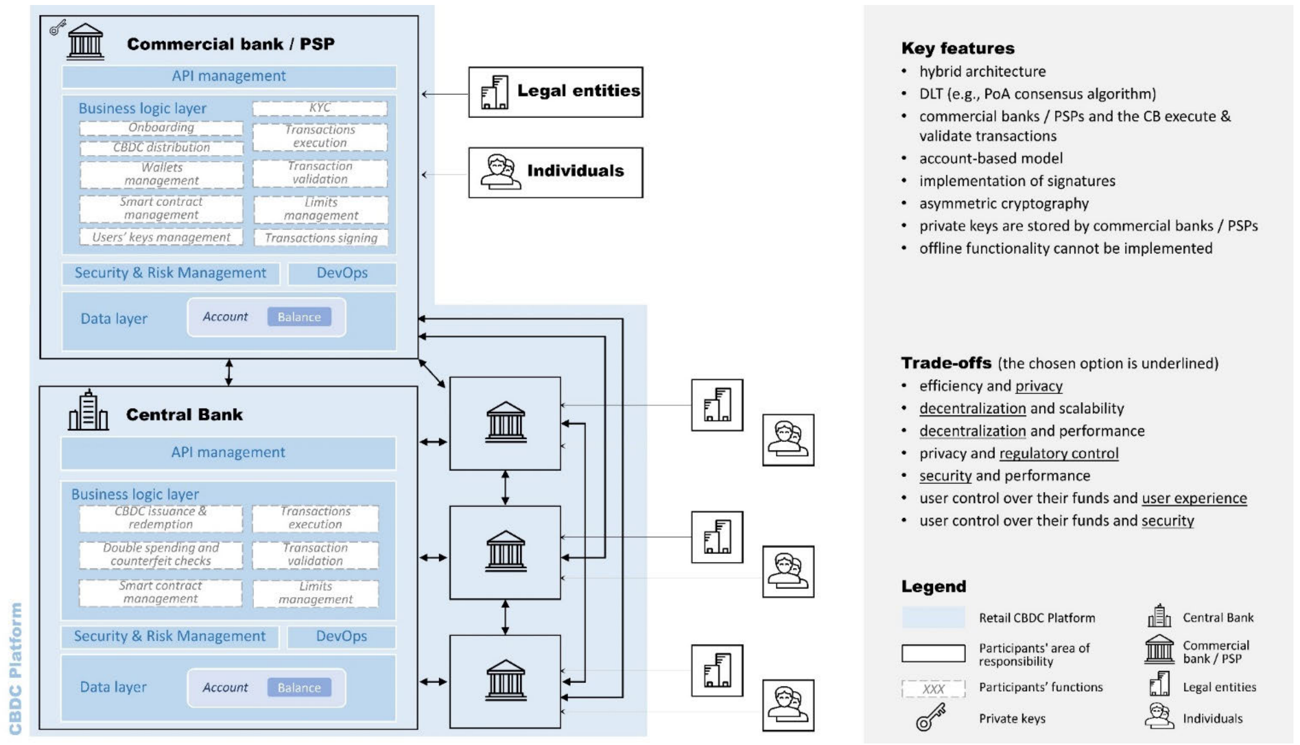


FIGURE 4. Architecture diagram (architecture option $N_{\underline{o}}$ 26 according to Appendixes A and B).

2) Participants validate and execute transactions.

3) The CB validates the whole transaction.

4) The priority is the ability to implement smart contracts and higher performance of the system rather than greater privacy options for retail users.

5) Offline functionality is not required (though it might be implemented, it is not the priority).

6) The priority is security (protection against unauthorized modifications or fraudulent activities) rather than performance, incl. high transaction speed and scalability.

7) The existing infrastructure (mobile devices or secure hardware) can adequately support private key storage and management.

8) Users are not competent enough to handle their private keys securely.

Such assumptions imply the following technological and architectural features of the retail CBDC design:

1) Hybrid architecture: transactions are executed by commercial banks and other payment service providers. In Fig. 4 commercial banks and PSPs are depicted inside the CBDC Platform contour.

2) DLT: such design choice is made because of two assumptions made – information on transactions should be shared among all participants in the CBDC Platform and participants validate and execute transactions. In Fig. 4 commercial banks and PSPs, as well as the CB, are interconnected with bidirectional arrows.

3) Account-based model: since the importance of performance and ease of smart contract implementation outweighs the importance of greater privacy options, account-based should be used.

4) Implementation of signatures: although offline functionality is not necessarily required, the priority is security (protection against unauthorized modifications or fraudulent activities) rather than performance meaning that user signatures must be implemented.

5) Asymmetric cryptography: asymmetric cryptography is a prerequisite for signatures implementation.

6) Private keys are stored by commercial banks / PSPs: although the existing infrastructure can adequately support private key storage and management, users are not competent enough to handle their private keys securely.

7) Offline functionality cannot be implemented: the private keys are stored by commercial banks which hinders offline mode implementation.

Described architecture design implies the importance of following priorities over others:

- Privacy over efficiency (due to hybrid architecture).
- Decentralization over scalability (due to DLT implementation).
- Decentralization over performance (due to DLT implementation).
- Regulatory control over privacy (due to account-based access and data model).
- Security over performance (due to signatures implementation).
- User experience over user control over their funds (due to storage of private keys by commercial banks / PSPs).

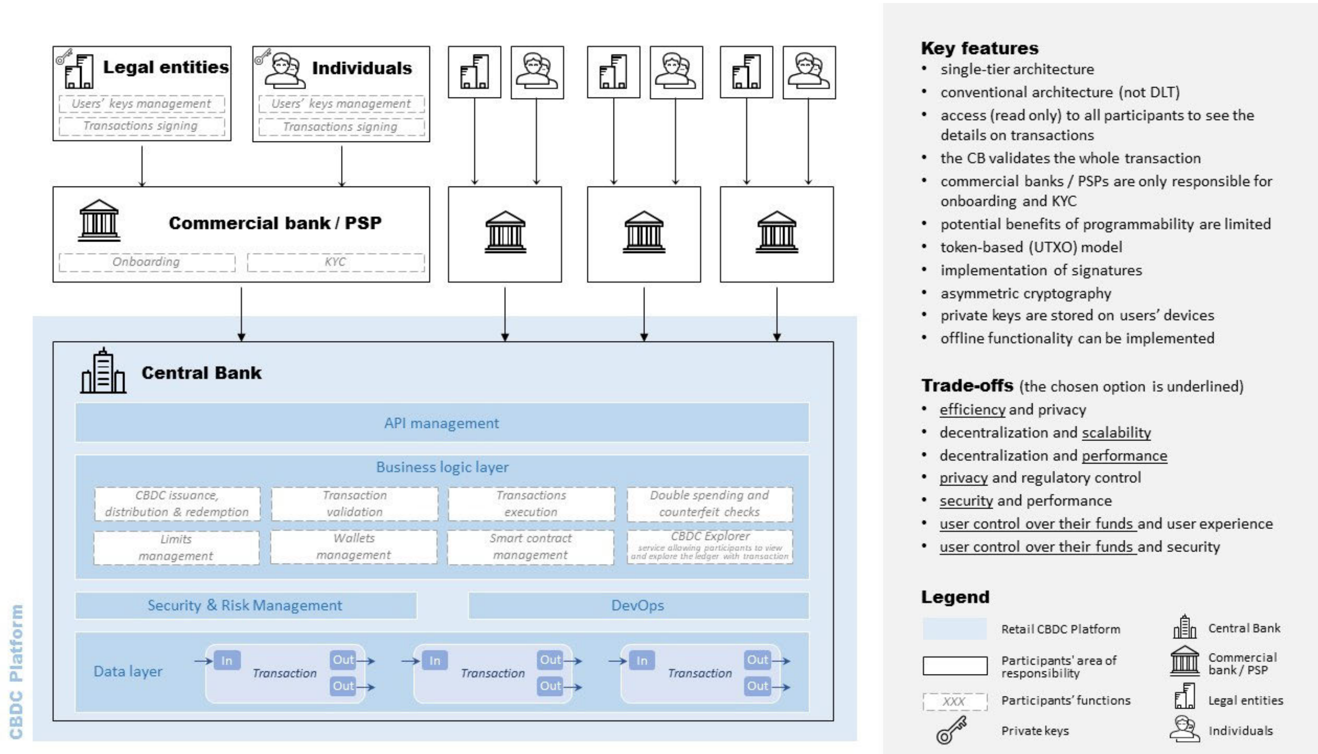


FIGURE 5. Architecture diagram (architecture option № 1 according to Appendixes A and B).

• Security of private key storage over user control over their funds (due to storage of private keys by commercial banks / PSPs).

Fig. 5 depicts architecture diagram that is recommended for consideration when policymakers decide that:

1) Information on transactions should be shared among all participants in the CBDC Platform.

2) Commercial banks and PSPs are responsible only for customer interaction functionality (retail transactions are executed solely by the CB).

3) The first priority is greater privacy options for retail users rather than the ability to implement smart contracts and higher performance of the system.

4) Offline functionality is required (CBDC without offline is not going to be implemented).

Such assumptions imply the following technological and architectural features of the retail CBDC design:

1) Single-tier architecture: only the CB executes transactions.

2) Conventional architecture (not DLT): although information should be shared among all participants, only the CB can make a decision whether to execute a transaction, other participants have a read only access. Consequently, DLT is not a viable option for such assumptions.

3) Access (read only) to all participants to see the details on transactions: the CB has a special service called CBDC Explorer allowing participants to view and explore the ledger with transactions.

4) The CB executes and validates the whole transaction: see the corresponding functions in the business logic layer in the CB contour.

5) Commercial banks / PSPs are only responsible for onboarding and KYC: commercial banks / PSPs do not execute transactions, they are outside the CBDC Platform contour.

6) Potential benefits of programmability are limited: centralized control restricts the ability for commercial banks and PSPs to implement new functionalities and customize the system according to their specific requirements.

7) Token-based (UTXO) model: since the importance of privacy is bigger than performance and ease of smart contract implementation, UTXO should be used. This model can offer more privacy but makes it harder to meet AML and KYC requirements.

8) Implementation of signatures: since there is an assumption that offline functionality is required, signatures are a must.

9) Asymmetric cryptography: asymmetric cryptography is a prerequisite for signatures implementation.

10) Private keys are stored on users' devices: to enable offline functionality, private keys must be stored on users' devices.

Described architecture design implies the importance of following priorities over others:

• Efficiency over privacy (due to single-tier architecture).

- Scalability over decentralization (due to conventional architecture).
- Performance over decentralization (due to conventional architecture).
- Privacy over regulatory control (due to token-based (UTXO) access and data model).
- Security over performance (due to signatures implementation).
- User control over their funds over user experience (due to storage of private keys on the users' devices).
- User control over their funds over security (due to storage of private keys on the users' devices).

VI. DISCUSSION

While many papers focus on the implications of the CBDC adoption [41], [42], [43], we studied design principles of CBDC, aiming at identifying architecture and technology design choices for retail CBDC and suggesting methodology for decision-making on CBDC design choices.

CBDC design choices heavily depend on the objectives policymakers aim to achieve with the CBDC system. These objectives might include advancing innovation and technologies, enhancing financial inclusion, financial system resilience, improving payment efficiency, maintaining monetary sovereignty, etc. The objectives should not only be clearly defined but also prioritized since trade-offs inevitably arise when designing CBDC system. Policymakers have to constantly select options which require sacrificing the benefits associated with other options. Our study outlines these trade-offs explicitly, offering a unique contribution by illustrating how different combinations of design choices impact the achievement of policy goals. Moreover, policymakers should invest in educating the public, commercial banks / PSPs, legal entities, and other stakeholders about CBDCs. Transparent communication about the benefits, risks, and design choices of CBDCs can foster acceptance and adoption. We provide a comprehensive framework that facilitates this educational communication, which is another advancement over the existing discussions in the literature. All in all, having well-defined and prioritized policy objectives and educated public will help policymakers to successfully design and adopt the CBDC system.

The presented architecture options depend on the selected assumptions which reflect policy objectives and goals. Still, some design choices (and corresponding architecture options) bring more benefits than others. To evaluate the internal and external factors affecting CBDC design, enabling policymakers to make informed decisions and manage risks effectively, we recommend employing a SWOT analysis for every architecture option, incorporating recent technological and regulatory developments.

VII. CONCLUDING REMARKS AND FUTURE RESEARCH OPPORTUNITIES

The contribution of the research is twofold. From the practical perspective, the paper provides insight and guidance for policymakers (specifically, Central Banks) on the implementation of a retail CBDC facilitating the understanding of what

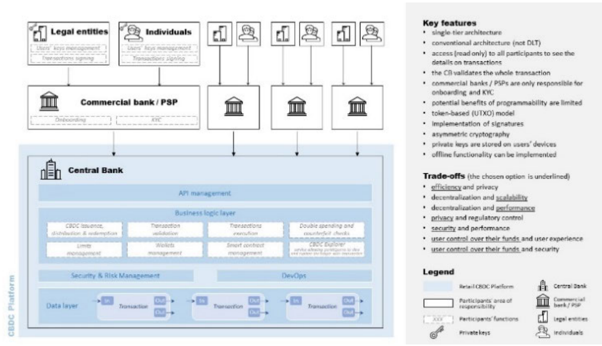


FIGURE 6. Architecture diagram 1.

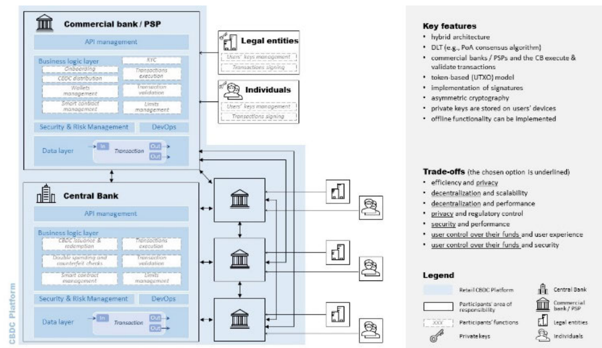


FIGURE 7. Architecture diagram 2.

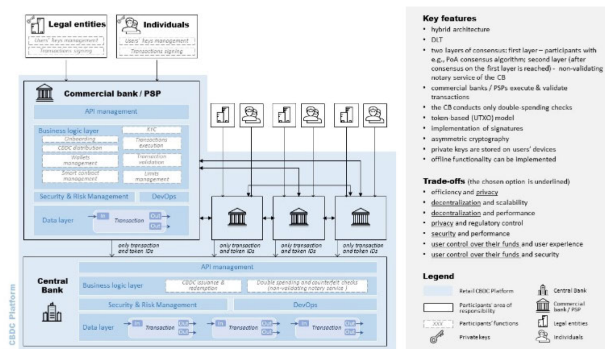


FIGURE 8. Architecture diagram 3.

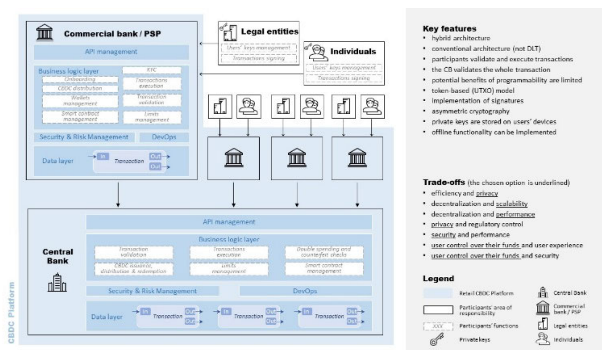


FIGURE 9. Architecture diagram 4.

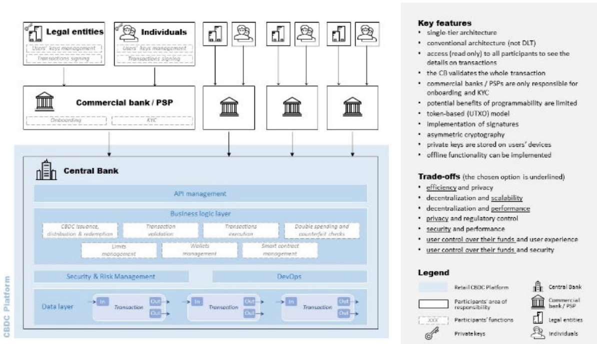


FIGURE 10. Architecture diagram 5.

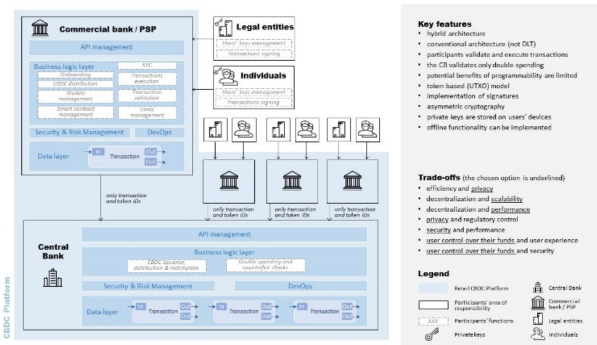


FIGURE 11. Architecture diagram 6.

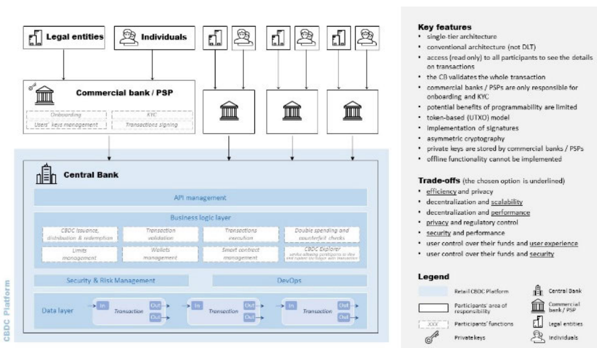


FIGURE 12. Architecture diagram 7.

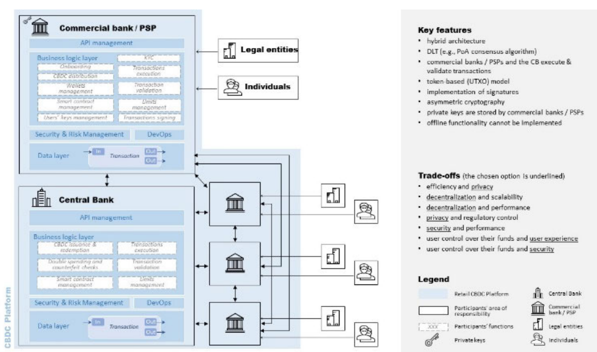


FIGURE 13. Architecture diagram 8.

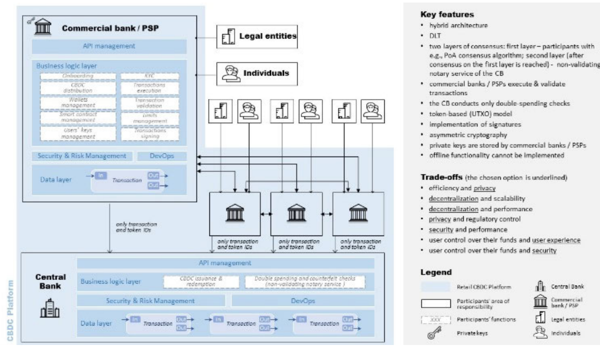


FIGURE 14. Architecture diagram 9.

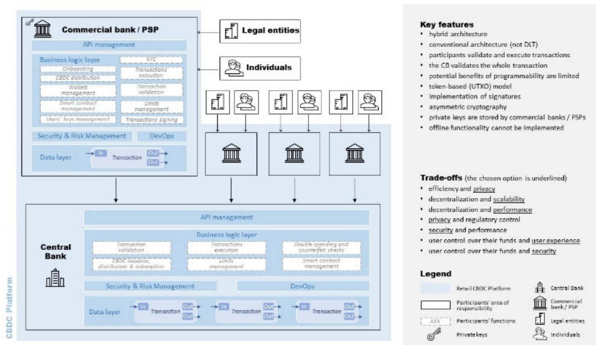


FIGURE 15. Architecture diagram 10.

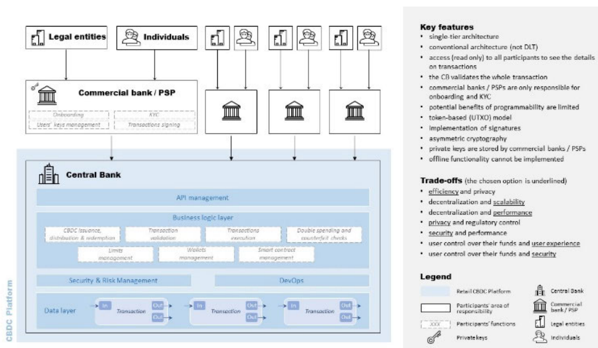


FIGURE 16. Architecture diagram 11.

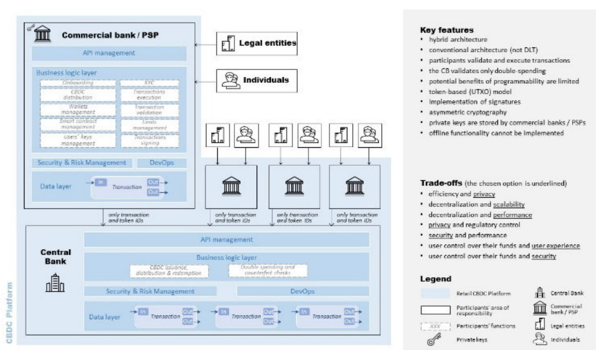


FIGURE 17. Architecture diagram 12.

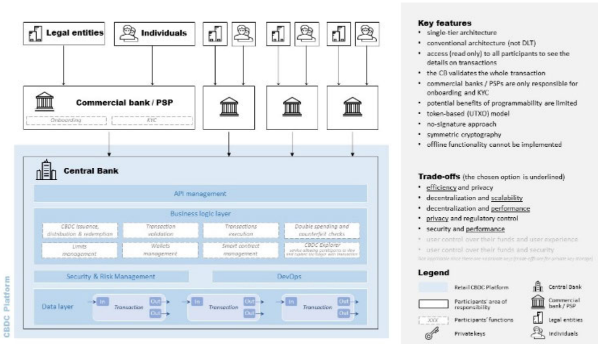


FIGURE 18. Architecture diagram 13.

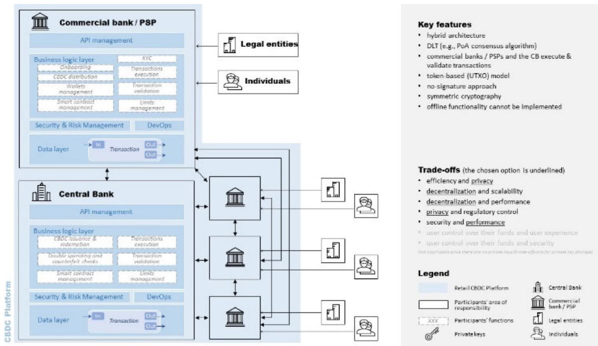


FIGURE 19. Architecture diagram 14.

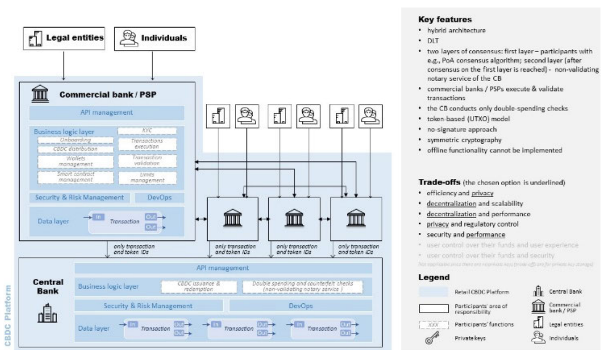


FIGURE 20. Architecture diagram 15.

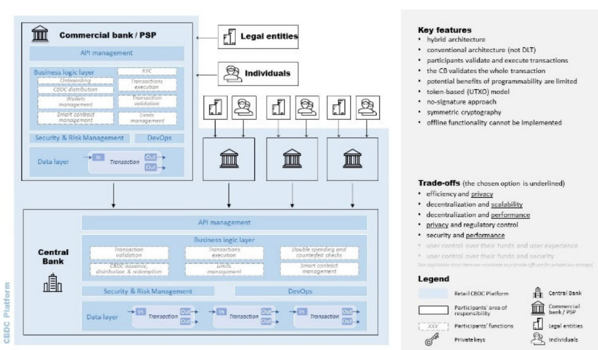


FIGURE 21. Architecture diagram 16.

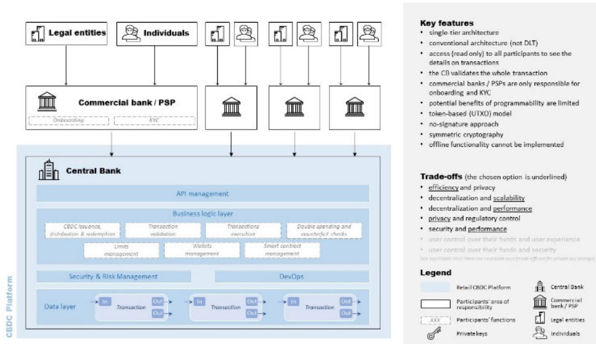


FIGURE 22. Architecture diagram 17.

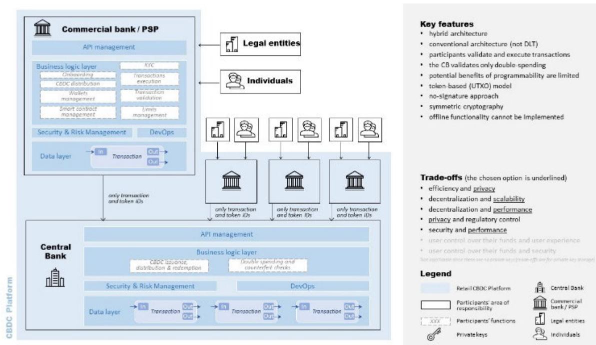


FIGURE 23. Architecture diagram 18.

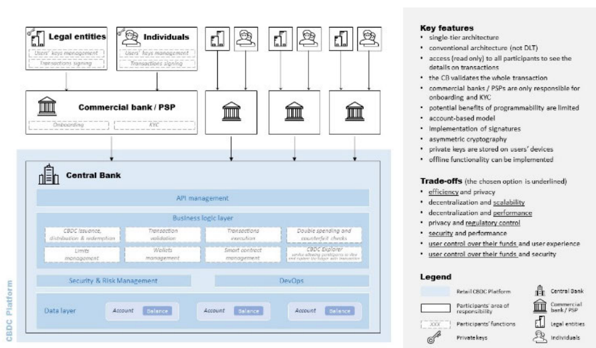


FIGURE 24. Architecture diagram 19.

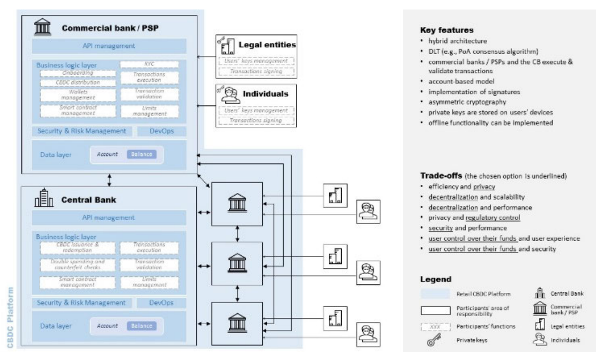


FIGURE 25. Architecture diagram 20.

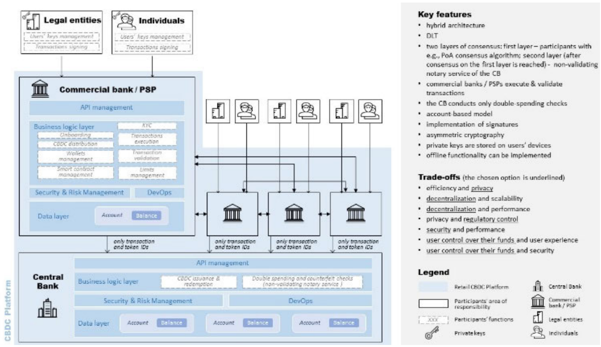


FIGURE 26. Architecture diagram 21.

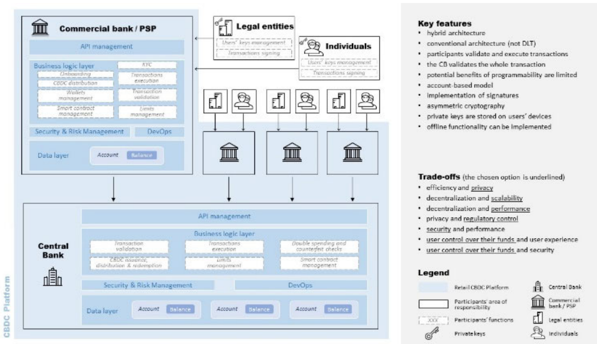


FIGURE 27. Architecture diagram 22.

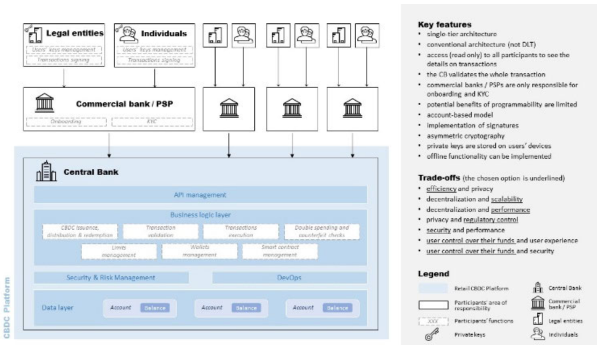


FIGURE 28. Architecture diagram 23.

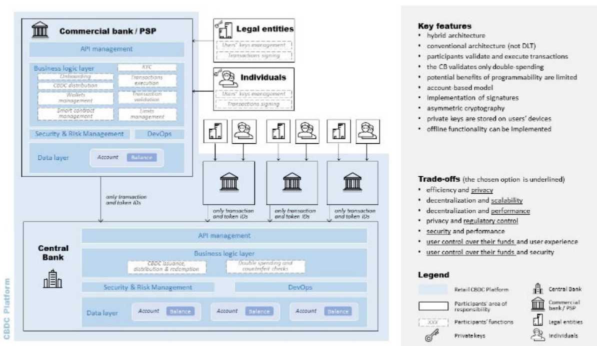


FIGURE 29. Architecture diagram 24.

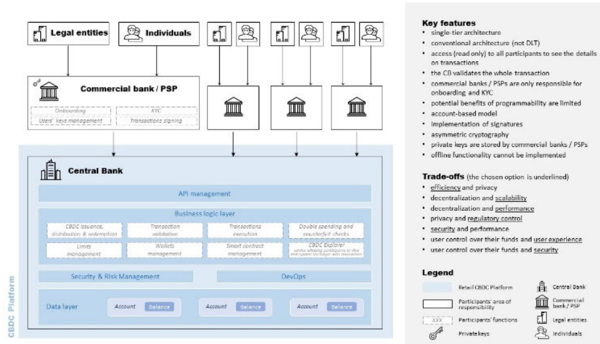


FIGURE 30. Architecture diagram 25.

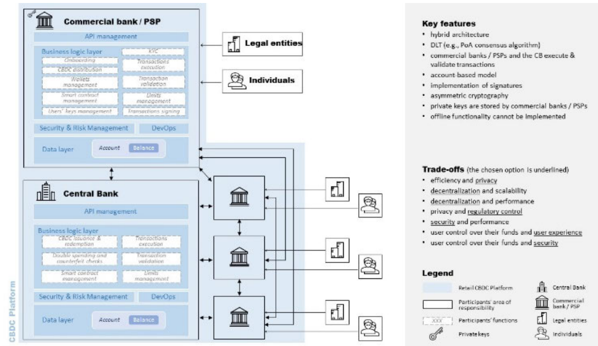


FIGURE 31. Architecture diagram 26.

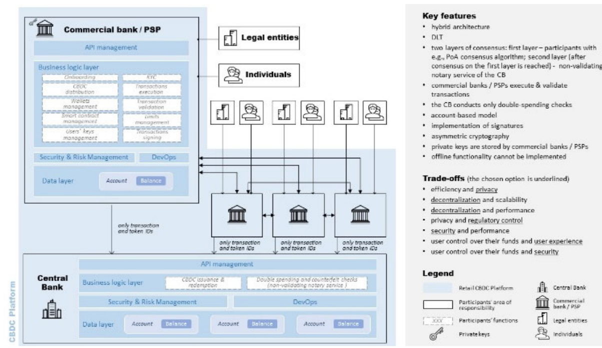


FIGURE 32. Architecture diagram 27.

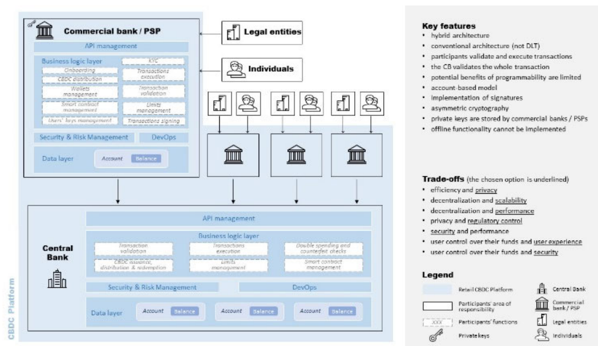


FIGURE 33. Architecture diagram 28.

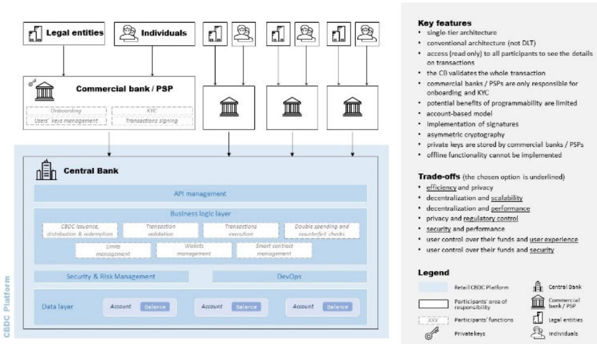


FIGURE 34. Architecture diagram 29.

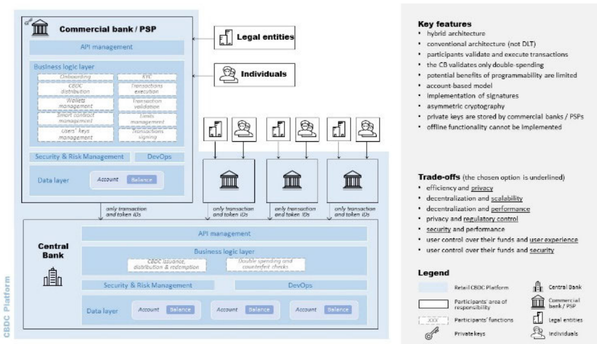


FIGURE 35. Architecture diagram 30.

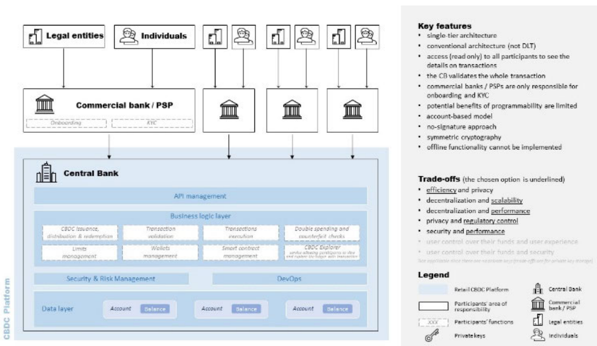


FIGURE 36. Architecture diagram 31.

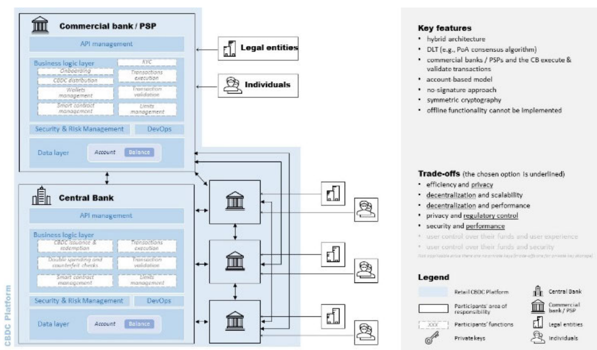


FIGURE 37. Architecture diagram 32.

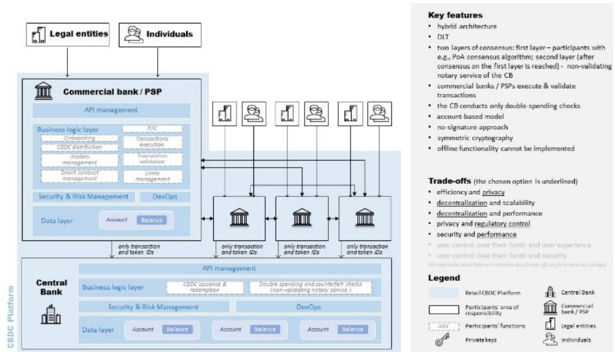


FIGURE 38. Architecture diagram 33.

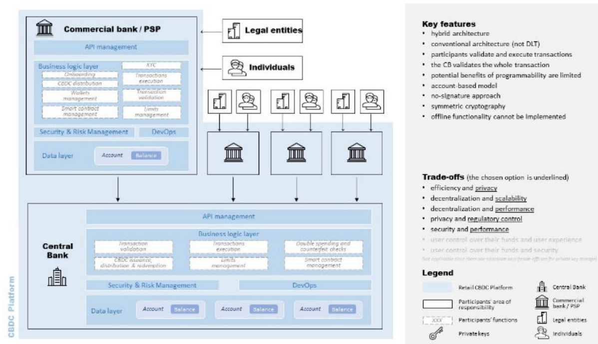


FIGURE 39. Architecture diagram 34.

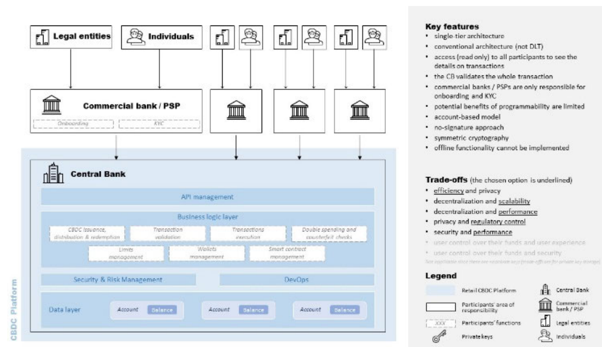


FIGURE 40. Architecture diagram 35.

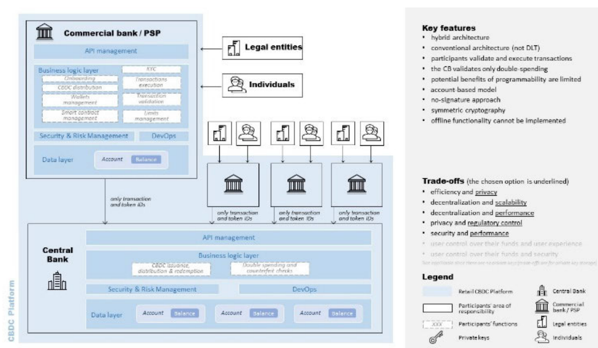


FIGURE 41. Architecture diagram 36.

architecture and technology design choices may best suit their specific requirements. This practical application helps to bridge the gap between theoretical research and real-world application, ensuring that the implications of our findings are

TABLE 5. Combinations of assumption options and the resulting CBDC architecture.

№	Assumption										
	ARCHITECTURE TYPE & DECENTRALIZATION										
1	**How should information on transactions be shared?** 1) Among all participants in the CBDC Platform 2) Only between participants engaged in a transaction	1	1	1	1	1	1	2	2	2	2
2	**Who should be responsible for validating and executing transactions?** 1) Commercial banks and PSPs validate and execute transactions 2) Commercial banks and PSPs are responsible only for customer interaction functionality (retail transactions are executed solely by the CB)	2	2	1	1	1	1	1	1	2	2
3	**What should be the role of the CB in validating transactions?** 1) The CB validates the whole transaction 2) The CB conducts only double-spending checks (sees only transaction and token IDs)	-	-	1	1	2	2	1	1	-	-
	ACCESS AND DATA MODEL										
4	**Which is the first priority, smart contracts and system performance or privacy options for retail users?** 1) Ability to implement smart contracts and higher performance of the system 2) Greater privacy options for retail users	2	2	2	2	2	2	2	2	2	2
	USER DIGITAL SIGNATURES AND KEY MANAGEMENT										
5	**Is offline functionality required?** 1) Yes, CBDC without offline is not going to be implemented *2)* No, although offline functionality might be implemented, it is not the priority	1	2	1	2	1	2	1	2	1	2
6	**Which is the first priority, security (protection against unauthorized modifications or fraudulent activities) or performance (including high transaction speed and scalability)?** 1) Security 2) Performance	-	1	-	1	-	1	-	1	-	1
7	**Can the existing infrastructure adequately support private key storage and management?** 1) Yes 2) No	-	1	-	1	-	1	-	1	-	1
8	**Are users competent enough to handle their private keys securely?** 1) Yes 2) No	-	1	-	1	-	1	-	1	-	1
	RESULT. № of the architecture diagram (№ of the architecture diagram corresponds with the number of architecture diagram in the Appendix A)	**1**	**1**	**2**	**2**	**3**	**3**	**4**	**4**	**5**	**5**

№	Assumption																									
	ARCHITECTURE…																									
1	**How should…**	2	2	1	1	1	1	1	1	2	2	2	2	2	2	1	1	1	2	2	2	1	1	1	1	1
2	**Who should be…**	1	1	2	2	1	1	1	1	1	1	2	2	1	1	2	1	1	1	2	1	2	2	1	1	1
3	**What should be…**	2	2	-	-	1	1	2	2	1	1	-	-	2	2	-	1	2	1	-	2	-	-	1	1	2
	ACCESS AND…																									
4	**Which is the…**	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1
	USER DIGITAL…																									
5	**Is offline…**	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	2	1	2	1
6	**Which is the…**	-	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	-	1	-	1	-
7	**Can the existing…**	-	1	2	1	2	1	2	1	2	1	2	1	2	1	-	-	-	-	-	-	-	1	-	1	-
8	**Are users…**	-	1	-	2	-	2	-	2	-	2	-	2	-	2	-	-	-	-	-	-	-	1	-	1	-
	RESULT	**6**	**6**	**7**	**7**	**8**	**8**	**9**	**9**	**10**	**10**	**11**	**11**	**12**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**19**	**20**	**20**	**21**

directly applicable to the formulation and execution of policy. From the research perspective, the paper suggested methodology for decision-making on CBDC design, which can be further refined and tested through future studies (such as simulations or pilot studies). This methodology not only enriches the academic discussion around CBDCs but also provides a structured approach that can be utilized by other researchers to explore new questions in this evolving field.

First, core and optional CBDC features were defined to clarify the understanding of what CBDC is in the first place. We further were able to identify 4 major CBDC design choices (architecture type, decentralization, access and data model, user digital signatures and key management) which provide a clear categorization that assists policymakers in navigating the complex landscape of CBDC design, an advancement over the existing research which tends to offer more general guidance. Moreover, several important design aspects have been shown. First, a CBDC system should be permissioned, and its units should be designed as a fungible digital asset. Secondly, CBDCs are always politically and logically centralized but can be decentralized from architectural perspective (although not fully). Thirdly, while DLT has gained popularity, it lacks significant advantages for CBDCs in some contexts. Finally, the programmability feature is an add-on which can be implemented in any CBDC design, although it is easier to implement in an account-based

TABLE 5. ***(Continued.)*** **Combinations of assumption options and the resulting CBDC architecture.**

№	Assumption																									
	ARCHITECTURE…																									
1	**How should…**	1	2	2	2	2	2	2	1	1	1	1	1	1	2	2	2	2	2	2	1	1	1	2	2	2
2	**Who should be…**	1	1	1	2	2	1	1	2	2	1	1	1	1	1	1	2	2	1	1	2	1	1	1	2	1
3	**What should be…**	2	1	1	-	-	2	2	-	-	1	1	2	2	1	1	-	-	2	2	-	1	2	1	-	2
	ACCESS AND…																									
4	**Which is the…**	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	USER DIGITAL…																									
5	**Is offline…**	2	1	2	1	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
6	**Which is the…**	1	-	1	-	1	-	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2
7	**Can the existing…**	1	-	1	-	1	-	1	2	1	2	1	2	1	2	1	2	1	2	1	-	-	-	-	-	-
8	**Are users…**	1	-	1	-	1	-	1	-	2	-	2	-	2	-	2	-	2	-	2	-	-	-	-	-	-
	RESULT	**21**	**22**	**22**	**23**	**23**	**24**	**24**	**25**	**25**	**26**	**26**	**27**	**27**	**28**	**28**	**29**	**29**	**30**	**30**	**31**	**32**	**33**	**34**	**35**	**36**

model and it can bring more benefits if implemented in a DLT-based system.

Next, assumptions and trade-offs for every design choice were defined allowing for designing the decision-making process. Assumptions and trade-offs were incorporated into the IT architecture design process which resulted in 36 architecture options (diagrams). From a management perspective, a methodology was proposed for decision-making on CBDC design choices. However, it is important to note that the architectures require further refinement for each individual country. The paper presents guidelines for the policymakers rather than answers to all questions regarding CBDC design choices. Before using suggested methodology, policymakers should define and prioritize policy objectives to make correct assumptions. Moreover, it is recommended to conduct SWOT analysis for the selected CBDC architecture design given country-specific aspects.

Future research directions on CBDC architecture and design choices may include:

(1) Simulations and pilot studies: Validate the proposed frameworks and methodologies.

(2) CBDC system design choices, focusing on the characteristics of distributed ledgers: Explore consensus mechanisms, chain and block sizes, network parameters.

(3) Wholesale CBDCs design choices: Address challenges of cross-border CBDCs, incl. foreign exchange and international compliance.

(4) Integration of CBDCs with systems like RTGS and international payment systems: Compare existing standards and propose new ones for smoother integration.

(5) Technology architecture: Explore optimal technology choices from programming languages to hardware configurations.

(6) Exploration of the socio-economic impacts of CBDC design choices.

(7) Development of a digital decision-making tool to allow policymakers to input specific conditions and receive tailored CBDC designs.

APPENDIX A

See Figures 6–41.

APPENDIX B

See Table 5.

REFERENCES

[1] R. Auer, G. Cornelli, and J. Frost. (2023). *Rise of the Central Bank Digital Currencies*. International Journal of Central Banking. Accessed: Dec. 17, 2023. [Online]. Available: https://www.bis.org/publ/work880.htm

[2] K. Georgieva, "The future of money: Gearing up for central bank digital currency," Speech Transcript, Atlantic Council, Washington, DC, USA, Tech. Rep., Feb. 9, 2022. [Online]. Available: https://www.imf.org/en/News/Articles/2022/02/09/sp020922-the-future-of-money-gearing-up-for-central-bank-digital-currency

[3] M. K. Brunnermeier, H. James, and J. P. Landau, "The digitalization of money," Nat. Bur. Econ. Res., Cambridge, MA, USA, Working Paper W26300, 2019. [Online]. Available: https://doi.org/10.3386/w26300

[4] A. H. Elsayed and M. A. Nasir, "Central bank digital currencies: An agenda for future research," *Res. Int. Bus. Finance*, vol. 62, Dec. 2022, Art. no. 101736, doi: 10.1016/j.ribaf.2022.101736.

[5] K. Löber and A. Houben. (2018). *Central Bank Digital Currencies*. Committee Payments Market Infrastructures Markets Committee, Bank for International Settlements, Basel, Switzerland. [Online]. Available: https://www.bis.org/cpmi/publ/d174.pdf

[6] BIS. (2020). *Central Bank Digital Currencies: Foundational Principles and Core Features*. [Online]. Available: https://www.bis.org/publ/othp33.htm

[7] World Economic Forum. (2023). *Central Bank Digital Currency: Global Interoperability Principles*. [Online]. Available: https://www.weforum.org/publications/central-bank-digital-currency-global-interoperability-principles/

[8] U.S. Department of the Treasury. (2022). *The Future of Money and Payments*. [Online]. Available: https://home.treasury.gov/system/files/136/Future-of-Money-and-Payments.pdf

[9] J. Son, M. H. Bilgin, and D. Ryu, "Consumer choices under new payment methods," *Financial Innov.*, vol. 8, no. 1, pp. 1–22, Sep. 2022, doi: 10.1186/s40854-022-00387-w.

[10] J. Kiff, J. Alwazir, S. Davidovic, A. Farias, A. Khan, T. Khiaonarong, M. Malaika, H. Monroe, N. Sugimoto, H. Tourpe, and Z. Zhou, ''A survey of research on retail central bank digital currency,'' *SSRN Electron. J.*, p. 66, Jan. 2020, doi: 10.2139/ssrn.3639760.

[11] S. Allen, S. Čapkun, I. Eyal, G. Fanti, B. Ford, J. Grimmelmann, A. Juels, K. Kostiainen, S. Meiklejohn, A. Miller, E. S. Prasad, K. Wüst, and F. Zhang, ''Design choices for central bank digital currency: Policy and technical considerations,'' Nat. Bur. Econ. Res., Work. Paper w27634, p. 110, 2020.

[12] Q. Yao, ''A systematic framework to understand central bank digital currency,'' *Sci. China Inf. Sci.*, vol. 61, no. 3, Mar. 2018, doi: 10.1007/s11432-017-9294-5.

[13] Board of Governors of the Federal Reserve System. (2022). *Money and Payments: The U.S. Dollar in the Age of Digital Transformation*. [Online]. Available: https://www.federalreserve.gov/publications/january-2022-cbdc.htm

[14] J. Lovejoy, C. Fields, M. Virza, T. Frederick, D. Urness, K. Karwaski, A. Brownworth, and N. Narula, ''A high performance payment processing system designed for central bank digital currencies,'' Cryptol. ePrint Arch., MIT Digital Currency Initiative, Cambridge, MA, USA, Paper 2022/163, 2022. [Online]. Available: https://eprint.iacr.org/2022/163

[15] O. Bjerg, ''Designing new money: The policy trilemma of central bank digital currency,'' Copenhagen Bus. School's (CBS), Copenhagen, Denmark, Working Paper, 2017, doi: 10.2139/ssrn.2985381.

[16] J. Barrdear and M. Kumhof, ''The macroeconomics of central bank issued digital currencies,'' Bank England, London, U.K., Working Paper 605, 2016. [Online]. Available: https://www.bankofengland.co.uk/-/media/boe/files/working-paper/2016/the-macroeconomics-of-central-bank-issued-digital-currencies

[17] N. Pocher and A. Veneris, ''Privacy and transparency in CBDCs: A regulation-by-design AML/CFT scheme,'' *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 2, pp. 1776–1788, Jun. 2022, doi: 10.1109/TNSM.2021.3136984.

[18] J. C. Jiang and K. Lucero, ''Background and implications of China's central bank digital currency: E-CNY,'' Univ. Florida Levin College Law, Res. Paper 23-7, p. 37, 2023, vol. 33.

[19] M. L. Bech and R. Garratt. (2017). *Central Bank Cryptocurrencies*. BIS Quarterly Review. [Online]. Available: https://www.bis.org/publ/qtrpdf/r_qt1709f.htm

[20] Bank of England. (2020). *Central Bank Digital Currency-Opportunities, Challenges, and Design*. Bank of England Discussion Paper. [Online]. Available: https://www.bankofengland.co.uk/paper/2020/central-bank-digital-currency-opportunities-challenges-and-design-discussion-paper

[21] M. McLeay, A. Radia, and R. Thomas. (2014). *Money Creation in the Modern Economy*. Bank of England Quarterly Bulletin. [Online]. Available: https://www.bankofengland.co.uk/quarterly-bulletin/2014/q1/money-creation-in-the-modern-economy

[22] P. Cheng, ''Decoding the rise of central bank digital currency in China: Designs, problems, and prospects,'' *J. Banking Regulation*, vol. 24, no. 2, pp. 156–170, Jun. 2023, doi: 10.1057/s41261-022-00193-5.

[23] R. S. Samudrala and S. K. Yerchuru, ''Central bank digital currency: Risks, challenges and design considerations for India,'' *CSI Trans. ICT*, vol. 9, no. 4, pp. 245–249, Dec. 2021, doi: 10.1007/s40012-021-00344-5.

[24] V. Buterin. (2017). *The Meaning of Decentralization*. Accessed: Jan. 17, 2024. [Online]. Available: https://medium.com/

[25] J. L. Romero Ugarte, ''Distributed ledger technology (DLT): Introduction,'' *Banco de Espana Article, no.*, vol. 19, no. 18, pp. 1–11, 2018. [Online]. Available: https://ssrn.com/abstract=3269731

[26] Committee on Payments and Market Infrastructures. (2017). *Distributed Ledger Technology in Payment, Clearing, and Settlement: An Analytical Framework*. [Online]. Available: https://www.bis.org/cpmi/publ/d157.htm

[27] N. Dashkevich, S. Counsell, and G. Destefanis, ''Blockchain application for central banks: A systematic mapping study,'' *IEEE Access*, vol. 8, pp. 139918–139952, 2020, doi: 10.1109/ACCESS.2020.3012295.

[28] S. Riksbank. (2023). *E-Krona Pilot, Phase 3: E-Krona Report*. [Online]. Available: https://www.riksbank.se/globalassets/media/rapporter/e-krona/2023/e-krona-pilot-phase-3.pdf

[29] United States Office of Science, Technology Policy. (2022). *Technical Evaluation for a U.S. Central Bank Digital Currency System*. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Technical-Evaluation-U.S.-CBDC-System.pdf

[30] R. Auer, G. Cornelli, and J. Frost. (2020). *Central Bank Digital Currencies: Drivers, Approaches, and Technologies*. VoxEU-CEPR's Policy Portal. [Online]. Available: http://raphaelauer.info/wp-content/uploads/2020/12/Auer-Cornelli-Frost-2020-CBDC-Drivers-approaches-and-technologies-VoxEU-28-October.pdf

[31] R. Auer and R. Böhme. (2020). *The Technology of Retail Central Bank Digital Currency*. [Online]. Available: https://www.bis.org/publ/qtrpdf/r_qt2003j.htm

[32] R. Auer and R. Böhme. (2021). *Central Bank Digital Currency: The Quest for Minimally Invasive Technology*. [Online]. Available: https://www.bis.org/publ/work948.htm

[33] McKinsey. (2023). *What is Central Bank Digital Currency (CBDC)*. [Online]. Available: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-central-bank-digital-currency-cbdc

[34] A. A. Rahman, ''A decentralized central bank digital currency,'' Global Currency Initiative (GCI), Jember, Indonesia, Working Paper 1, 2022. [Online]. Available: https://mpra.ub.uni-muenchen.de/111361/

[35] National Bank of Ukraine. (2019). *Analytical Report on the E-Hryvnia Pilot Project*. [Online]. Available: https://bank.gov.ua/admin_uploads/article/Analytical

[36] S. Y. Jin and Y. Xia, ''CEV framework: A central bank digital currency evaluation and verification framework with a focus on consensus algorithms and operating architectures,'' *IEEE Access*, vol. 10, pp. 63698–63714, 2022, doi: 10.1109/ACCESS.2022.3183092.

[37] S. Smetanin, A. Ometov, N. Kannengießer, B. Sturm, M. Komarov, and A. Sunyaev, ''Modeling of distributed ledgers: Challenges and future perspectives,'' in *Proc. IEEE 22nd Conf. Bus. Informat. (CBI)*, vol. 1, Jun. 2020, pp. 162–171, doi: 10.1109/CBI49978.2020.00025.

[38] R. Tamassia, ''Authenticated data structures,'' in *Proc. 11th Annu. Eur. Symp. Algorithms (ESA)*, vol. 11, Budapest, Hungary, Sep. 2003, pp. 2–5, doi: 10.1007/978-3-540-39658-1_2.

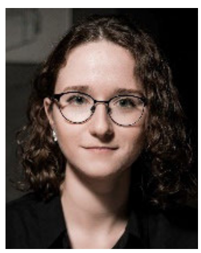
[39] C. M. Kahn and W. Roberds, ''Why pay? An introduction to payments economics,'' *J. Financial Intermediation*, vol. 18, no. 1, pp. 1–23, Jan. 2009, doi: 10.1016/j.jfi.2008.09.001.

[40] BIS Annual Economic Report. (2021). *Promoting Global Monetary and Financial Stability*. [Online]. Available: https://www.bis.org/publ/arpdf/ar2021e.htm

[41] J. Abad, G. N. N. Barrau, and C. Thomas, ''CBDC and the operational framework of monetary policy,'' Bank Int. Settlements (BIS), Basel, Switzerland, Working Paper 1126, 2023. [Online]. Available: https://www.bis.org/publ/work1126.htm

[42] S. M. Davoodalhosseini, ''Central bank digital currency and monetary policy,'' *J. Econ. Dyn. Control*, vol. 142, Sep. 2022, Art. no. 104150, doi: 10.1016/j.jedc.2021.104150.

[43] S. Williamson, ''Central bank digital currency: Welfare and policy implications,'' *J. Political Economy*, vol. 130, no. 11, pp. 2829–2861, Nov. 2022, doi: 10.1086/720457.



ANASTASIA TSAREVA is currently pursuing the master's degree with the Business Analytics and Big Data Systems Program, Graduate School of Business, HSE University. In addition to her studies, she is a System Analyst in an IT-consulting company. She has twice received the Gold Medal from the All-Russian Olympiad for Students ''I am a Professional'' in the business informatics track.

MIKHAIL KOMAROV (Senior Member, IEEE) is currently a Professor with the Department of Business Informatics, Graduate School of Business, HSE University. He is a Specialist in wireless data transmission and IT. He is the Vice-Chair of the Special Interest Group on IoT at the Internet Society.