Development of DLT-Based Central Bank Digital Currency Prototype on Corda Network

Georgii Rulev * and Vasilii Krikunov

Moscow Institute of Physics and Technology, Moscow, Russia
Email: rulev.gk@phystech.edu (G.R.); krikunov.vv@phystech.edu (V.K.)
*Corresponding author

Abstract*—The article showcases the outcomes of developing a pilot platform for a Central Bank Digital Currency (CBDC) using the R3 Corda development environment. Additionally, it presents a global architecture for CBDCs within which the developed pilot solution can be applied. The developed pilot solution encompasses a set of implemented mechanisms, such as token issuance (utilizing the UTXO[1] model, where UTXO stands for Unspent Transaction Output), transactions (consensus mechanism[2]), and token distribution among participant nodes. The pilot platform is comprehensively described through functional and technical architecture (including participant environment, nodes, Distributed Ledger Technology (DLT) architectures), interaction structures, and token structures. Additionally, the code of key implemented mechanisms is detailed in Section VI. The proposed model of the global architecture for Central Bank Digital Currencies (CBDCs) is outlined in Section V and encompasses not only the structure for constructing such large-scale systems but also the potential technological stack for implementing individual components and layers of the architecture. Global architecture is grounded on analysis of already piloted CBDC systems while also addressing future requirements concerning security, load capacity, resilience, and interoperability. Additionally, it anticipates the possibility of integration with existing payment mechanisms and with other CBDC systems developed on alternative technological platforms such as Hyperledger, E-Currency, and others. This article showcases the latest advancements in constructing high-transaction systems based on distributed ledgers. The pilot platform described in this article has validated the feasibility of employing the proposed methods, and its core can be reused for industrial implementation by Central Banks globally.

***Keywords*—central bank digital currency, Distributed Ledger Technology (DLT), Web3, corda, prototype**

I. Introduction

In addressing the technical considerations for the development of Central Bank Digital Currencies (CBDCs), several key questions emerge. Firstly, the implementation of the token issuance mechanism must be carefully considered to ensure integrity and security. Secondly, the consensus mechanism's design is crucial for achieving network agreement while maintaining efficiency. Thirdly, ensuring the network can handle high transaction volumes without compromising transaction history poses a significant challenge. Furthermore, identifying the optimal cryptographic tools for use within CBDCs is essential for safeguarding transactions and privacy. The issue of interoperability between different networks, such as Corda and Hyperledger, requires innovative solutions to enable seamless transaction flow across platforms. Additionally, the programmability of CBDC tokens introduces complexity in terms of smart contract integration and execution. Lastly, minimizing reliance on oracles for external data verification is pivotal to enhancing the system's autonomy and reliability. These considerations are foundational in constructing a robust and scalable CBDC platform.

This article explores the development and outcomes of a pilot platform for Central Bank Digital Currencies (CBDCs) using the R3 Corda development environment [1]. It details a global architecture for CBDCs, where the pilot solution fits, covering token issuance, transactions, and distribution mechanisms. The work represented in this article covers methods for the development of CBDC platform's functional and technical architectures, interaction and token structures, and key code implementations were extensively discussed. It proposes a global architecture model for CBDCs, considering the structure, technological stack, and integration with existing and future payment systems, emphasizing security, load capacity, resilience, and interoperability.

This research demonstrates the potential for applying these methodologies in real-world central bank implementations, offering insights into building high-transaction systems with distributed ledgers for leading central banks who are considering implementation of CBDC within the country.

The development process of the pilot platform consisted of the following steps:

[1] An output created in a transaction, which must be referenced in a future transaction to spend funds.
[2] A consensus mechanism is the programming and process used in blockchain systems to achieve distributed agreement about the ledger's state or the state of a data set

Manuscript received July 1, 2024; revised July 22, 2024; accepted July 30, 2024; published February 10, 2025.

a. Strategy and use case definition: key use cases for CBDC pilot were defined, e.g., Peer-to-Peer (P2P) transactions, programmability, offline payments, etc.
b. Functional requirements: application and system requirements were defined, including scalability, interoperability, processes diagrams etc.
c. IT architecture: system, infrastructure, application architecture were developed.
d. Pilot platform development: key components including the back-end and front-end of the platform were developed in agile sprints.
e. Testing: testing of core functionality was conducted

For the development of CBDC pilot R3 Corda platform was chosen. This is an open and enterprise Distributed Ledger Technology (DLT) solution developed by R3 [2–7]. It includes both open-source and enterprise versions, as well as special CBDC sandboxes designed for use in financial markets. R3 Corda provides flexible tools and architecture specifically tailored to the needs of financial institutions.

Some key benefits of Corda noted in the context of the Central Bank:

– Performance: Corda has a high level of performance, making it suitable for the high-frequency transaction models typical of digital banking.
– Scalability: The platform provides the ability to add new participants and launch nodes on several servers, which is important for expanding the digital banking system without reducing its performance.
– Security: Corda supports trust chain management and ensures data privacy, which is critical for systems working with financial assets.
– The ability to implement smart contracts: This allows you to create a variety of agreements and automate their execution, which is useful for a number of operations in the digital currency, including managing digital assets and enforcing agreements.
– Ease of use: Corda provides a convenient API for managing platform nodes, which simplifies the deployment, maintenance and administration of the digital banking system.

Based on these factors, Corda appears to be one of the most promising options for implementing digital currency, especially given its successful implementation in a number of pilot projects and commercial solutions in the financial industry.

II. Literature Overview

The literature on financial technologies and digital currencies encompasses a wide array of studies focusing on the advancements, challenges, and implementations of such technologies *et al*. [8–10]. Mngomezulu *et al*. [11] explore the application of Bluetooth and Near Field Communication (NFC) in financial transactions, while Igboanusi *et al.* [12] propose an offline transaction architecture using blockchain. Omilabu *et al*. [13] provide a comparative analysis of wireless technology applications, highlighting their relevance in the current digital landscape. Noether and Mackenzie [14] delve into the privacy aspects of transactions with ring confidential transactions, and Metere and Dong [15] focus on the cryptographic analysis of commitment schemes. The emergence of Central Bank Digital Currencies (CBDCs) has sparked extensive research, as seen in the works of Opare and Kim [16], Klein *et al*. [17], and various publications by Accenture and the Digital Dollar Foundation, examining the policy, technical considerations, and implications of implementing CBDCs [18–20]. The exploration of Distributed Ledger Technology (DLT) for financial infrastructures is another critical focus, with insights from Project Ubin [4], the Riksbank's e-krona pilot [21], and the World Economic Forum [22]. These studies collectively offer a comprehensive overview of the current state and future prospects of digital currencies and blockchain technology in the financial sector, underscoring the importance of interoperability, security, and efficient transaction mechanisms in the evolving landscape of digital finance.

III. Material and Methods

The classical approach to developing complex systems entails the creation of Pilot and Target versions of the platform. The key distinction between Pilot and Target platforms lies in the fact that the system developed in the Pilot project serves as a "sandbox," wherein models of environments for all participants will be created, rather than industrial versions of their systems. Moreover, the process of industrial operation of the system created in the Pilot is not envisaged; rather, it involves demonstrative testing to validate hypotheses. The outcomes of this work can be utilized in the transition process from the Pilot architecture to the Target, with partial reuse of several artifacts generated in the pilot project (for instance: software code of DLT components, diagrams and algorithms for module interaction, solutions in web and mobile interfaces, libraries at the protocol level of NFC interaction).

The Pilot platform should include service services facilitating the registration and blocking of network participants, as well as a dynamic registry of network addresses to establish direct interaction between participants. Moreover, participant registration in the network should be implemented, including within the "Issuance of Second-Layer Bank's Wallets" scenario (Fig. 1). Further details regarding the implementation requirements of service services are provided in the "System Architecture" section.

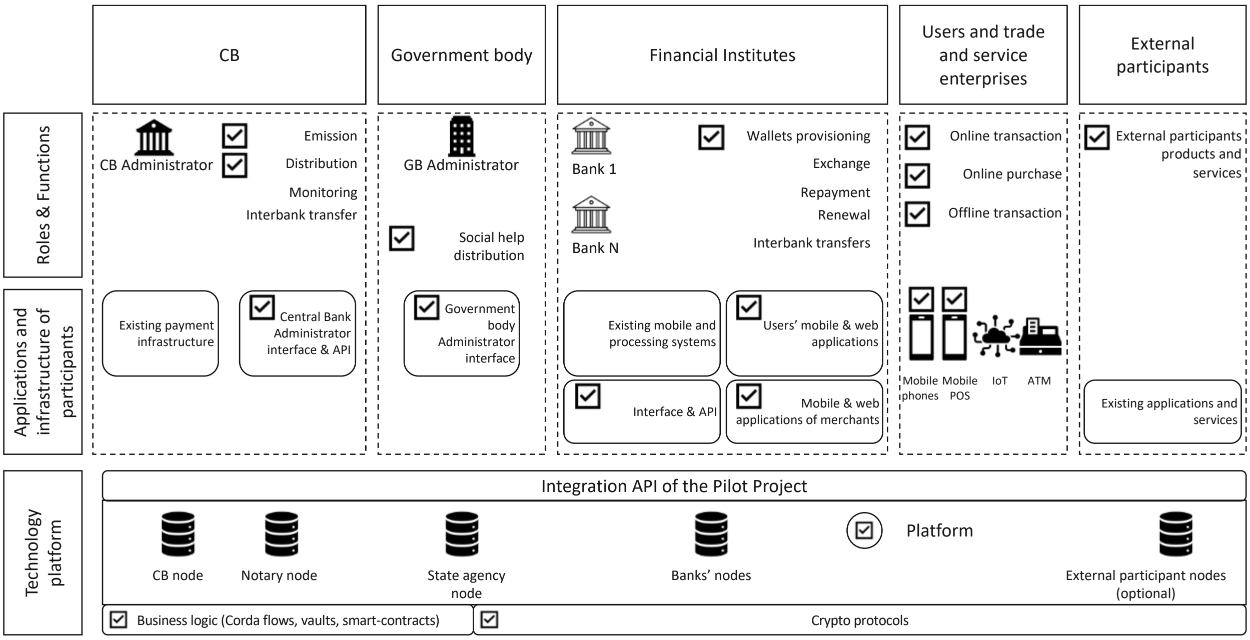

Fig. 1. Conceptual model of the platform.

IV. Result and Discussion

A. Application Architecture

Application architecture has two representations (Fig. 2):

– Functional architecture.
– System architecture.

This section outlines the requirements for the general landscape of applications or the functional architecture of the system, which includes requirements for the list of roles, systems, and interactions between them, while subsequent sections detail the environment for each component (Central Bank, Government Entity, Second-Layer Bank (SLB)).

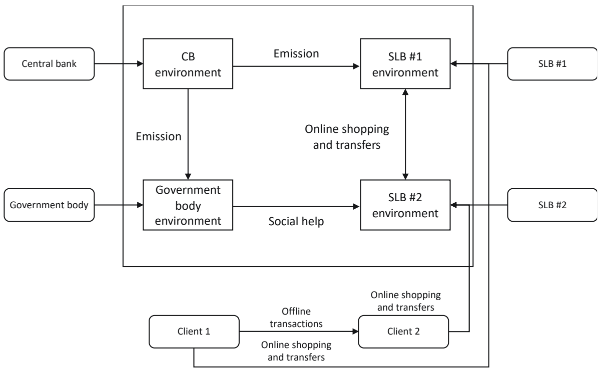

Fig. 2. General landscape of platform applications (functional architecture).

B. Functional Environment of the Central Bank

Functional environment of the Central Bank includes prototypes of the following systems (Fig. 3):

– Central Bank employee web application - user interface.
– DLT subsystem of the Central Bank.
– Notary node (Notary Subsystem).

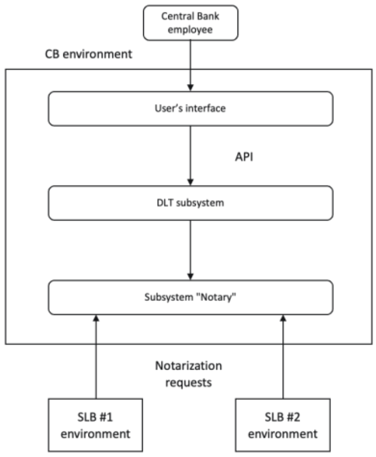

Fig. 3. Functional environment of the central bank.

C. Functional Environment of Second-Tier Banks

Functional environment of the bank includes prototypes of the following systems (Fig. 4):

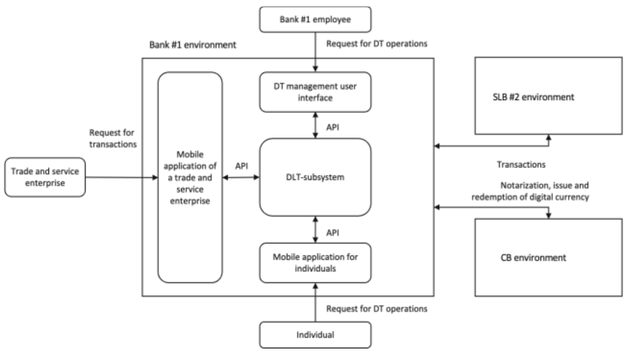

Fig. 4. Functional environment of the second-layer bank.

– SLB employee web application—user interface for central heating management;
– DLT subsystem of the bank.

– Mobile application physical faces;
– Mobile application of the trade and service enterprise.

D. Functional Environment of the Government Entity

The involvement of a governmental entity is essential for piloting the functionality of smart contract programmability and oracle properties. Practical application lies, for instance, in dispensing social assistance to citizens of the country. The functional environment of the Governmental Organization includes prototypes of the following systems (Fig. 5):

– Web application of a government agency employee - user interface.
– DLT subsystem of the Government entity.

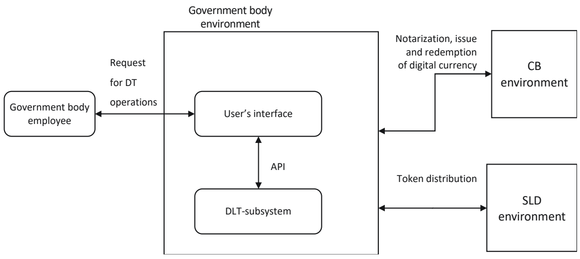

Fig. 5. Functional environment of the government agency.

E. System Architecture

The section outlines the list of system requirements for the functional blocks, principles of their interaction, and the stack of utilized technologies. Non-DLT application interaction services are implemented within the concept of microservices and REpresentational State Transfer Application Programming Interface (RestfulAPI), thus enabling reusability in the event of migration to the target architecture of participants. The Database Management System (DBMS) and application logic of the backend-level infrastructure participants are dependent on the stack of the Pilot Project. Consequently, there are no provisions for reusing these components in the event of migration to another stack.

The distributed ledger is to be implemented based on the technological platform of R3 Corda, utilizing PostgreSQL as the database, GraphQL as the application server engine, developing web applications on Vue.js, and mobile applications on the Android OS (using Kotlin).

In Fig. 6, the System Architecture of the Participant's Target Solution is presented. The term "participant" refers to the environment of any of the participants (from the perspective of the system architecture in the pilot, they should be identical).

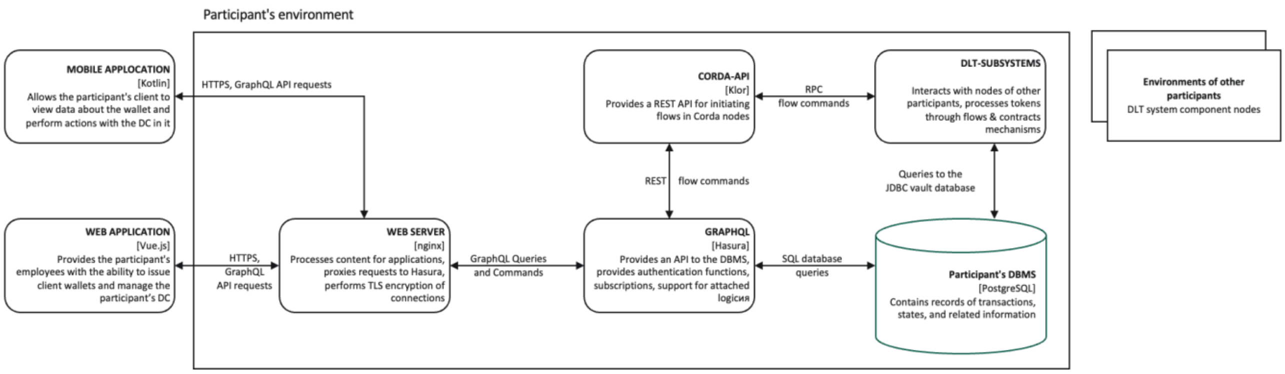

Fig. 6. System architecture of the participant.

F. DLT Architecture

Within the scope of developing DLT architecture in a distributed ledger, two types of interactions were implemented:

– Interaction of a Corda node with other Corda nodes via the Advanced Message Queuing Protocol (AMQP) protocol;
– Interaction of a node with external systems through the Corda API via RPC.

At Corda level The API implements methods for initiating vault[3] requests and flows[4], in in turn, interacting with smart contracts and verifying the results of transactions. The Corda node must include the following blocks:

– the node's core, which provides basic services for flows and contracts[5], as well as an interface for interaction with other nodes and the outside world;
– A "flow state machine," responsible for executing flows;
– A "vault," containing records of transactions, states, and other artifacts.

[3] Vault is a repository of records of transactions, states and related information. It represents a collection of database storage (for example, PostgreSQL), vault Query API and environment, as well as data

[4] Flows are automated processes built on Corda. Presented as a sequence of steps for a corda node, which determines how to perform a particular operation (for example, an emission operation).

[5] Contracts—contracts that define the rules for validating transactions. In accordance with these rules, a transaction can be recognized as valid (and be executed in this case) or invalid (in which case the transaction is not executed). Can be implemented in Java or Kotlin.

In the core of a node, contracts can be implemented to define rules or execution scenarios for transactions. For instance, these contracts may conduct verification of transactions executed by participants in accordance with blacklists and, based on the verification outcomes, either block or permit the transaction execution.

The architecture of a DLT node (Corda node) is depicted in Fig. 7.

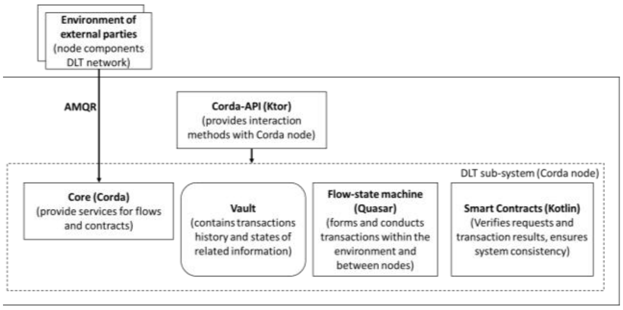

Fig. 7. DLT architecture.

G. DLT Structure

The R3 Corda platform offers the following functional capabilities:

– Nodes of participants: encompassing the implementation of interaction protocols and contracts.
– Notary node: used to ensure linearity of the transaction history, which, in particular, is necessary to solve the problem of double spending.

The platform must comply with the enterprise level, which includes following requirements:

– Enterprise-level database support;
– Network security system (firewall) and Hardware Security Module (HSM) support;
– Performance/stress testing tools.

The technology platform includes a custom consensus mechanism other than Proof-of-Work, Proof-of-Stake and similar.

H. Interaction Principles between DLT Nodes

The notarial node and participant nodes can exchange messages directly with each other using the standard secure AMQP protocol, thus ensuring data privacy and eliminating the need for a shared registry.

Participant nodes can interact with each other by transmitting messages via the AMQP protocol in cases of transactions occurring between participants. In each transaction between participants, there is additional interaction with the "Notary" node.

To execute transactions, the principle of consensus regarding the accuracy and uniqueness of transactions in the registry must be achieved. Consensus of accuracy is ensured by verifying the transaction by each participating party. This verification involves not only the current transaction but also the entire chain of transactions that led to its creation. Upon successful transaction verification, the party (DLT node) signs the transaction.

Consensus of uniqueness is ensured by the notarial node ("Notary" node). Consensus of uniqueness implies that no input data of the transaction has been used previously in any other transaction. Where the input data of the transaction refers to references to states obtained as a result of previous transactions. In the Platform, the input data of the transaction must be references to "tokens." In such a case, for example, if the "tokens" have been previously spent, the notarial node will not confirm the transaction. A situation where input data has already been used leads to double spending. In the event such a situation is detected by the notarial node, the transaction is not executed. All participants of the transaction receive notification of the rejection of the transaction by the notarial node.

The platform also provides for the possibility of clustering notarial nodes to enhance network availability and fault tolerance.

I. Functional Features of DLT

The implementation of a distributed registry must ensure the availability of digital securities tokens and operations with them properties defined on the basis of the previous article.

Thus, the Platform in the context of a distributed registry has the following properties:

– Access to wallets based on tokens. Compliance with international Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT) requirements is ensured to block illegal transactions. Participants have the ability to halt transaction recording in the registry to facilitate the implementation of these features.
– Anonymity of transactions—achieved through disclosure of CBDC owner data only to the bank serving the CBDC owner [23–25].
– Ability to operate in short-term offline mode.
– Ability to conduct transactions for different categories of CBDC: two types of CBDC are implemented: regular and programmable.

V. Conclusion

This article showcases the latest developments in the field of building high-transaction systems based on distributed ledgers. The pilot platform described in this article and the implemented mechanisms have demonstrated the feasibility of using the proposed methods. The core of the pilot platform, with certain enhancements, can be reused in industrial projects as it represents a set of fundamental tested Distributed Ledger Technology (DLT) tools: consensus mechanisms, transactions, token creation, transaction lifecycle support, etc.

The global architecture developed based on advanced global developments by leading central banks in prominent countries (China, Sweden, Switzerland) encompasses the most comprehensive list of layers and components necessary for implementing a secure and high-transaction DLT system for central banks.

However, some of the mechanisms implemented within the pilot platform require further refinement and testing for stability, security, and resilience. Primarily, this pertains to the length of the transaction chain stored in the token. Increasing the length with each cycle exponentially decreases transaction speed. A potential solution could involve trimming part of the chain and transferring the token to the central bank node (similar to creating a new token and removing the old one). The second critical issue requiring additional investigation is the memory limitation of devices to 5.6 KB, which complicates storing a large transaction history on the medium and impedes the creation of a large graph of online transactions. Methods to address these problems will be researched and tested as part of ongoing scientific research.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Georgii Rulev conducted research on application architecture, functional environment of Central Bank, second-tier bank, government entity and system architecture. Vasilii Krikunov conducted research on DLT architecture and structure, interaction principles between nodes and functional feature of DLT. All authors had approved the final version.

ACKNOWLEDGMENT

The authors wish to thank Moscow Institute of Physics and Technology for support during the research.

REFERENCES

[1] R3 Sandbox for Digital Currencies. [Online]. Available: https://www.r3.com/digital-currency-sandbox/

[2] S. Scorer. (2017). Central Bank Digital Currency: DLT, or not DLT? That is the question. [Online]. Available: https://bankunderground.co.uk/2017/06/05/central-bank-digital-currency-dlt-or-not-dlt-that-is-the-question/

[3] S. Allen, S. Čapkun, I. Eyal, G. Fanti, B. A. Ford, J. Grimmelmann, F. Zhang *et al*., "Design choices for central bank digital currency: Policy and technical considerations," National Bureau of Economic Research, No. w27634, 2020.

[4] What we learned from our DLT capability study. A Q&A with DTCC's Jennifer Peve. [Online]. Available: https://www.dtcc.com/dtcc-connection/articles/2018/november/08/what-we-learned-from-our-dlt-capability-study

[5] J. Polge, J. Robert, and Y. L. Traon, "Permissioned blockchain frameworks in the industry: A comparison," *ICT Express*, vol. 7, no. 2, pp. 229–233, 2021.

[6] R. Han, G. Shapiro, V. Gramoli, and X. Xu, "On the performance of distributed ledgers for internet of things," *Internet of Things*, vol. 10, 100087, 2020.

[7] Monetary Authority of Singapore and Accenture. Project Ubin: Central Bank Digital Money using Distributed Ledger Technology. [Online]. Available: https://www.mas.gov.sg/schemes-and-initiatives/project-ubin

[8] R. Auer, G. Cornelli, and J. Frost, "Rise of the central bank digital currencies: Drivers, approaches and technologies," *International Journal of Central Banking*, 2023. https://www.bis.org/publ/work880.htm

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

[10] K. Georgieva. (Feb. 9, 2022). The future of money: Gearing up for central bank digital currency. [Online]. Available: https://www.imf.org/en/News/Articles/2022/02/09/sp020922-the-future-of-money-gearing-up-for-central-bank-digital-currency

[11] Z. Mngomezulu, S. Rimer, K. Ouahada, and A. Ndjiongue, "A review of Bluetooth and NFC for financial applications," in *Proc. Sixth International Conference on Advances in Computing, Control and Networking*, 2017, pp. 48–51.

[12] I. S. Igboanusi, K. P. Dirgantoro, J. M. Lee, and D. S. Kim, "Blockchain side implementation of Pure Wallet (PW): An offline transaction architecture," *ICT Express*, vol. 7, issue 3, pp. 327–334, 2021.

[13] A. A. Omilabu, O. O. Olusanya, A. A. Adebare, F. Ibitowa, and O. B. Longe, "Comparative analysis of Wi-Fi, Bluetooth & Xender wireless technology applications," *Computing*, vol. 8, no. 4, 2017.

[14] S. Noether and A. Mackenzie, "Ring confidential transactions," *Ledger*, vol. 1, pp. 1–18, 2016.

[15] R. Metere and C. Dong, "Automated cryptographic analysis of the pedersen commitment scheme," in *Proc. International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, Springer, 2017, pp. 275–287.

[16] E. A. Opare and K. Kim, "A compendium of practices for central bank digital currencies for Multinational financial infrastructures," *IEEE Access*, vol. 8, pp. 110810–110847, 2020.

[17] M. Klein, J. Gross, and P. Sandner, "The digital Euro and the role of DLT for central bank digital currencies," FSBC Working Paper, Frankfurt School Blockchain Centre, 2020.

[18] Accenture. (2017). The (R)evolution of Money: Blockchain Empowered Digital Currencies. [Online]. Available: https://www.accenture.com/t20171116T025715Z__w__/us-en/_acnmedia/PDF-63/Accenture-Evolution-Money-Blockchain-Digital-Currencies.pdf#zoom=50

[19] Accenture. (2020). The (R)evolution of Money II: Blockchain Empowered Bank Digital Currencies. [Online]. Available: https://www.accenture.com/us-en/insights/blockchain/evolution-money

[20] Digtal Dollar Foundation and Accenture. (2020). The Digital Dollar Project. [Online]. Available: http://digitaldollarproject.org/wp-content/uploads/2021/05/Digital-Dollar-Project-Whitepaper_vF_7_13_20.pdf

[21] Riksbank and Accenture. (February 2020). The Riksbank's e-krona pilot (2018–2021). [Online]. Available: https://www.riksbank.se/globalassets/media/rapporter/e-krona/2019/the-riksbanks-e-krona-pilot.pdf

[22] World Economic Forum. (2021). Digital Currency Governance Consortium. White Paper Series. Compendium Report. [Online]. Available: https://www.weforum.org/communities/digital-currency-governance-consortium/

[23] Accenture. (2018). Connecting ecosystems: Blockchain integration. [Online]. Available: https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-3/pdf/pdf-88/accenture-20180514-blockchain-interoperability-pov.pdf

[24] Accenture and DTCC. (2019). Governing DLT Networks, DLT Governance for Private Permissioned Networks. [Online]. Available: https://www.accenture.com/content/dam/accenture/final/a-com-migration/pdf/pdf-2/Accenture-Governing-DLT-Networks.pdf

[25] ECB and Accenture. (2019). Exploring anonymity in central bank digital currencies with European Central Bank. [Online]. Available: https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.mipinfocus191217.en.pdf

Copyright © 2025 by the authors. This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited (CC BY 4.0).