

DOI: <https://doi.org/10.34069/AI/2023.69.09.6>

How to Cite:

Hudima, T., Kamyshanskyi, V., Dmytrenko, T., & Shmyhov, M. (2023). Optimal CBDC design for Ukraine through the lens of privacy and security. *Amazonia Investiga*, 12(69), 73-83. <https://doi.org/10.34069/AI/2023.69.09.6>

Optimal CBDC design for Ukraine through the lens of privacy and security

Оптимальний дизайн CBDC для України через призму конфіденційності та безпеки

Received: July 30, 2023

Accepted: September 25, 2023

Written by:

Tetiana Hudima¹ <https://orcid.org/0000-0003-1509-5180>**Vladyslav Kamyshanskyi²** <https://orcid.org/0000-0003-4220-8339>**Tetiana Dmytrenko³** <https://orcid.org/0000-0002-2632-2986>**Mykhailo Shmyhov⁴** <https://orcid.org/0009-0002-0492-326X>

Abstract

The growing popularity of cryptocurrencies has put on the agenda the need to develop an alternative and more regulated digital currency design, including a central bank digital currency (CBDC). The objective of the study is to formulate proposals for the development of the optimal design of the CBDC of Ukraine. The study is based on a review of the literature on digital currencies, cryptocurrencies and legislation on personal data protection, payment security and financial supervision. The implementation of the CBDC in Ukraine is associated with numerous technical and legal risks, including: privacy and data security risks; complications of financial monitoring; contradictions with national and international legislation; banks disintermediation risks.

To prevent these risks, a CBDC design is proposed that is compatible with national and international legislation, ensures data privacy and security, facilitates financial tracking, and reduces the risks of disintermediation.

The development of the CBDC in Ukraine could have a significant impact on the country's financial system. However, it is essential that the

Анотація

Зростання популярності криптовалют поставило на порядок денний необхідність розробки альтернативного та більш регульованого дизайну цифрової валюти, зокрема цифрової валюти центрального банку (CBDC). Метою дослідження є формування пропозицій щодо розробки оптимального дизайну CBDC України. Дослідження базується на огляді літератури про цифрові валюти, криптовалюти та законодавства про захист персональних даних, безпеку платежів і фінансовий моніторинг. Впровадження CBDC в Україні пов'язане з численними технічними та юридичними ризиками, серед яких: ризики конфіденційності та безпеки даних; ускладнення фінансового моніторингу; протиріччя національного та міжнародного законодавства; ризики дезінтермедіації банків. Щоб запобігти цим ризикам, пропонується дизайн CBDC, який є сумісним з національним і міжнародним законодавством, а також здатний забезпечити конфіденційність і безпеку даних; полегшити фінансове відстеження; зменшити ризики дезінтермедіації.

¹ Doctor of Science (Law), Senior Researcher, Deputy Head of Department, SO «V. Mamutov Institute of economic and legal research of NAS of Ukraine», Kyiv, Ukraine.  WoS Researcher ID: AAB-6450-2021

² PhD student (Law), SO «V. Mamutov Institute of economic and legal research of NAS of Ukraine», Kyiv, Ukraine.  WoS Researcher ID: JDV-9858-2023

³ PhD in Economics, Head of the Department of International Finance and Financial Security, Academy of Financial Management, Kyiv; OSCE AML Consultant, Vienna, Austria.  WoS Researcher ID: JDW-0367-2023

⁴ PhD student (Law), SO «V. Mamutov Institute of economic and legal research of NAS of Ukraine», Kyiv, Ukraine.  WoS Researcher ID: JDW-0773-2023

design of the CBDC is carefully considered to mitigate potential risks.

Keywords: central bank, central bank digital currency, distributed ledger technology, General Data Protection Regulation, payment system.

Introduction

Against the backdrop of the growing popularity of cryptocurrencies and the increasing interest of central banks in developing Central Bank Digital Currencies (CBDCs), the imperative for faster, cheaper, more transparent, inclusive, and secure payment services becomes paramount. As highlighted by the Financial Stability Board's reports in 2020, these priorities are crucial for fostering economic growth, supporting international trade, facilitating global development, and ensuring financial inclusion (FSB, 2020a; FSB, 2020b). The rapid replacement of electronic money by cryptocurrencies in international settlements has prompted central banks worldwide to explore and implement CBDCs as an alternative instrument. The Atlantic Council's CBDC Tracker reveals that as of July 2023, 130 countries, representing over 95 percent of global GDP, are actively considering the introduction of CBDCs, with 11 already launched and 21 engaged in pilot projects, including Ukraine (Atlantic Council, 2023).

The analysis of CBDC pilot projects in countries such as Sweden, China, Norway, and others underscores a critical challenge - balancing the imperative of data privacy and security in payments, as mandated by international documents like the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR), with the concurrent need for robust financial monitoring. This issue is particularly pronounced as regulators, including those in Ukraine, consider the adoption of distributed ledger technology (DLT) as the foundational infrastructure for CBDCs, presenting an alternative to cryptocurrencies. However, aligning such approaches with existing legal and regulatory frameworks, both at the national and international levels, poses complexities, especially within the European Union (EU).

Розвиток CBDC в Україні може мати значний вплив на фінансову систему країни. Однак дуже важливо, щоб дизайн CBDC був розроблений таким чином, щоб зменшити потенційні ризики.

Ключові слова: центральний банк, цифрова валюта центрального банку, технологія розподіленого реєстру, Загальний регламент захисту даних, платіжна система.

This dilemma necessitates further research and the formulation of proposals for the development of the Ukrainian CBDC design. This is particularly important in view of the Association Agreement between the EU and its Member States, of the one part, and Ukraine, of the other part (the "Association Agreement") as well as Ukraine's recently acquired status as an EU candidate country.

The article aims to contribute to this discourse by formulating recommendations for the optimal design of Ukraine's CBDC, considering the intricacies of international and national legislation on personal data protection, ensuring payment confidentiality and security, and complying with financial monitoring regulations. As the digital financial landscape continues to evolve, addressing these concerns is not only pivotal for safeguarding the rights and privacy of citizens but also for upholding the stability and integrity of the financial systems intertwined with global and regional economic frameworks.

Theoretical Framework or Literature Review

In general, the relevance of the issue of introducing a CBDC into the payment system is only growing. According to some experts, this will help strengthen financial stability and monetary policy, improve payment systems, and promote financial inclusion (Boar & Wehrli, 2021). Economic and legal research and the experience of other countries in this area can ensure the formation of scientific and practical reasonable extraordinary solutions, the implementation of which will contribute to positive transformations in the process of further digitalization of the payment market in Ukraine at the legislative level and in practice.

A growing number of publications focus on two fundamental questions. The first is how should retail digital money be issued by central banks and whether physical cash could be replaced by CBDCs (Brunnermeier, James, & Landau, 2019;

Chernyshova, Voznyakovs'ka, & Bashlay, 2021; Keister & Sanches, 2021; Shapoval, 2020). On the other hand, it is about the systemic implications of such a currency and how to deal with the associated risks and instability they may cause (Allen, Gu, & Jagtiani, 2022; Brunnermeier et al., 2019; Belke & Beretta, 2020; Fernández-Villaverde et al., 2020; Hrytsay, 2022; Khodakevich, Ponomarenko, & Urvantseva, 2022; Niepelt, 2018; Veneris et al., 2021).

Scientists note that CBDCs can have different designs (Allen et al., 2020; Auer & Boehme, 2021; Kiff et al., 2020). The role of the central bank and other payment market participants in the such currency ecosystem depends on the choice of a particular design. CBDCs can be issued and distributed directly by the central bank (direct design) or by authorized financial institutions (intermediary design). As for the technological basis of digital currency, it can be based on a centralized or distributed ledger technologies (DLT). In the case of a centralized ledger, the central bank controls and manages the CBDC system. In the opposite case (distributed ledger), data processing, storage and management functions are delegated to authorized financial institutions in the private or public sector (Gross et al., 2021).

Most central banks have launched CBDC pilots to find arguments in favor of choosing DLT for its launch (Sethaput & Innet, 2023; Sethaput & Innet, 2021).

However, in order to develop an optimal design for CBDCs, central banks must strike a balance between data protection and the individual's right to privacy, on the one hand, and the public interest in combating terrorist financing and money laundering, on the other. There are risks that a fully anonymous digital currency will make it impossible for anti-money laundering regulations (AML) regulators to exercise control, while a partially or fully transparent one could be used by governments as a surveillance tool. In addition, such a design choice is inconsistent with the fundamental rights to data protection and information privacy mentioned above (Ballaschk & Paulick, 2021; Islam & In, 2022; Fanti & Pocher, 2022; Auer et al., 2023); Tsang, Yang, & Chen, 2022; Tronnier, 2021).

For example, Charles Hoskinson (2022), the founder of Cardano, sees CBDC as a tool for controlling the population and considers it the most dangerous innovation in monetary policy. The same opinion is shared by researchers at the

American Institute for Economic Research. "Meeting the threat of an authoritarian rival by using dangerous social control technologies is completely contrary to society. According to experts, it would be more appropriate to invest in improving the payment system rather than replacing it with CBDC, which will give the government unprecedented control over financial transactions" (Salter, 2022). At the same time, more and more scholars point out the risks of the banking system's disintermediation (Eren, Jackson, & Lombardo, 2022; Banet & Lebeau, 2022; Changi et al., 2022).

Pollock (2018, p. 11), in his speech to the Subcommittee on Monetary Policy and Trade of the Committee on Financial Services of the United States House of Representatives, noted that disintermediation, in turn, would lead to even greater risks: unfair competition, abuse of regulatory powers to enhance one's own advantages, etc. The same concerns were expressed by Carstens A. (2019), Mancini-Griffoli et al., (2019), Bindseil U. (2020). According to Carrat (2018, p. 7) "the risk of excessive disintermediation would be mitigated by making any new form of central bank money more like cash and less like deposits".

In any case, "central banks should not put a brake on innovations just for the sake of it". But this does not mean that it is necessary "to rush ahead disregarding all traffic conditions. First, they should make sure that innovations set the right course for the economy, for businesses, for citizens, for society as a whole" (Carstens, 2019, p. 10).

As rightly noted Santaolalla Montoya (2023) "centralized digital currencies should be very well regulated, precisely so that they are not abused by the executive authorities or central banks. The European Data Protection Regulation must be strictly enforced".

Quite interesting in this vein is the work "Central bank digital currency: Principles for technical implementation", in which the authors presented an overview of some of the principles of a CBDC. This paper particularly emphasizes the key requirements of privacy protection and interoperability (Duffie, Mathieson, & Pilav, 2021).

Pocher and Veneris (2021) in their paper "Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFTS Scheme" offer a technical and legal taxonomy of

approaches to balancing privacy and transparency in CBDCs without violating accountability and anti-money laundering and counter-terrorist financing requirements in the United States of America (USA). Some proposals of the researcher may be applicable in resolving the question regarding the choice of the optimal CBDC design for Ukraine.

In general, while acknowledging the importance of existing scientific developments in this area, it should be noted that some scientific aspects of the general issue of choosing a CBDC design in Ukraine that would meet the requirements of international and national legislation on personal data protection, data privacy and security of payments, as well as legislation on financial monitoring have not yet been detailed. Accordingly, the above has led to the need for the proposed research.

Methodology

To attain the article's aim and uphold the scientific rigor of the research outcomes, a methodological framework encompassing hermeneutic, comparative, and generalizing methods was applied.

The choice of China, Sweden, and Norway as the focus of the study was deliberate and based on several criteria. China, represented by the People's Bank of China (PBoC), was selected due to its leadership in developing central bank digital currencies (CBDCs), as evidenced by its extensive pilot project reaching 260 million people and encompassing various scenarios, such as public transit, stimulus payments, and e-commerce (Atlantic Council, 2023). Transactions using China's digital yuan hit 1.8 trillion yuan (\$249.33 billion) at end-June 2023, marking a jump from over 100 billion yuan as of August last year (Wee, 2023). The inclusion of China provides a comprehensive understanding of a leading CBDC initiative on a large scale.

Sweden and Norway were chosen because they are progressive EU countries actively piloting CBDCs, not only at the national level but also in collaboration through projects like Icebreaker, involving Israel and the Bank for International Settlements (Atlantic Council, 2023). The participation of these Nordic countries in the Icebreaker project is unique and allows for an exploration of cross-border retail payments using CBDC. Furthermore, the intermediary design based on DLT in the CBDCs of Sweden and Norway contrasts with China's approach,

offering valuable insights into diverse design strategies.

Hermeneutic and comparative methods facilitated the analysis and comparison of international experiences, including data from CBDC pilot projects in Sweden, China, and Norway. This involved an in-depth examination of reports on the implementation of these projects, along with an exploration of international and national acts/documents governing legal regulations, data protection, financial monitoring, and related aspects.

Data collection involved accessing reports, legal documents, and official publications from the People's Bank of China, the Riksbank, the Central Bank of Norway, and relevant international organizations. Comparative analysis was conducted to identify commonalities and differences in CBDC designs and implementations. Conclusions, recommendations, and suggestions were formulated through a process of generalization based on the insights gained from the analysis of these diverse experiences.

Results and discussion

The general principles of the issuance and use of digital money of the National Bank of Ukraine (NBU) in Ukraine and its distinction from electronic money were officially established by the Law of Ukraine "On Payment Services" dated June 30, 2021 (this law is the result of the implementation of European legislation - author's note). According to paragraph 96 of Article 1 of this law, "digital money of the NBU is an electronic form of the currency of Ukraine, the issuer of which is the NBU".

At the same time, it should be noted that the Law of Ukraine "On Payment Services" is rather declarative in its approach to regulating the specifics of issuing and using digital currency. In particular, the legal act notes that the procedure for issuing and storing digital money, as well as the specifics of payment transactions using digital money, should be determined by the NBU's regulations (Article 62 of the Law of Ukraine "On Payment Services").

Despite the two-year period for the adoption and existence of the Law of Ukraine "On Payment Services" further steps to implement the above article by the regulator are rather slow. Thus, the NBU presented the draft concept of the e-hryvnia - the digital money of the National Bank of Ukraine - to representatives of banks, non-bank

financial institutions and the virtual asset market for discussion and feedback only on November 28, 2022 (NBU, 2022).

The regulator is currently considering and working on the following possible uses of the e-hryvnia, which will determine its design and main characteristics: e-hryvnia for retail cashless payments; cross-border payments and operation with virtual assets (NBU, 2022).

At the same time, as noted above, the innovation of introducing the e-hryvnia (CBDC) may lead to a number of positive and negative consequences. On the one hand, it will help to optimize financial monitoring, accessibility of payments, transaction speed, reduce the cost of international transfers, fight corruption through transparency of transactions, etc., and on the other hand, it will threaten the data privacy and security of payments.

These issues are global in nature. An analysis of publicly available reports from both the EU (European Central Bank, 2022) and the United States on the introduction of digital currency allows us to identify the most pressing issues in this area. These include the expediency of involving intermediaries; compliance with the laws on financial monitoring (AML), identification (Know Your Customer policy (KYC)) and confidentiality of information, if a decision is made to issue a CBDC based on well-known DLT, such as blockchain technology etc. (U.S. Department of the Treasury, 2022).

In addition, issues regarding the choice of (1) a centralized or decentralized design of the digital currency ledger; (2) determining the entities that will be able to access the identity and transaction data in the CBDC system and the exceptional conditions under which they may be accessed; (3) the features of CBDC system in response to data leaks, cyber threats, etc., and compliance with data leaks notification requirements (both nationally and internationally) remain unresolved. As for the expediency of engaging intermediaries, it should be noted that there are different approaches in this area. Out of the twenty-one countries that have launched a CBDC pilot, only ten have clearly chosen the intermediary design, while the rest are still considering the advantages and risks of the relevant design as opposed to a non-intermediary design (Atlantic Council, 2023). Among the striking examples of the intermediary design are the CBDC pilot projects of China, Norway, Sweden, and other countries.

"E-CNY adopts two-tier operation whereby the PBoC is responsible for issuance and disposal, inter-institution connect and wallet ecosystem management. Additionally, it prudently selects commercial banks with certain strengths in capital and technology as authorized operators to take the lead in providing e-CNY exchange services. Other commercial banks and institutions, under the PBoC's centralized management, give full play to their creativity, and collectively provide services for e-CNY circulation" (People's Bank of China, 2021, p. 8).

In turn, the intermediary design in Sweden is presented as follows. At the first level, the Riksbank issues or buys back e-krona from selected intermediaries in the network, such as banks (Handelsbanken or Tietoevry). At the second level, the intermediaries will distribute the e-krona to end users by providing them with alias that are used as network addresses for CBDC payments.

Participants will be able to receive or redeem digital currency by debiting or replenishing reserves held directly by the participants or through a representative in the Riksbank's real-time money transfer system, known in Sweden as RIX. In the test design, the participants' e-krona node in the network is integrated with their internal accounting and payment systems. Handelsbanken has implemented its e-krona node in its own IT environment, while the Tietoevry e-krona node is hosted in the Riksbank's IT environment (Sveriges Riksbank, 2022). Nevertheless, clients of both banks were able to conduct transactions in the common e-krona network."

The Corda network design chosen by the Swedish central bank, in which information is shared with central banks, financial regulators, and financial intermediaries only on a need-to-know basis, provides a level of data privacy similar to the two-tier design used by central banks today. To prevent double spending in this design, specialists track incoming and outgoing transaction data and risks of double spending by noting transaction identifiers (Meher, 2020).

As for Norway's practice, CBDC is also planned to be distributed under a two-tier architecture: Norges Bank will issue CBDC to banks, which will then credit it (CBDC) to the accounts of their clients (end users). However, there are conflicting opinions on this intermediary design at the regulator's level (Syrstad, 2023).

However, a design that allows banks (or a part of them) to retain the function of intermediaries connecting the central bank and holders of the CBDC accounts seems more acceptable anyway. After all, it will guarantee that the balance between the availability of confidential information and the protection of private interests is not compromised. It will comply with the current legislation on: (1) financial monitoring, according to which banks, authorized payment system operators and others are subjects of primary financial monitoring, and the NBU is the subject of state financial monitoring in this case (Article 6 of the Law of Ukraine "On Prevention and Counteraction to Legalization (Laundering) of Proceeds of Crime, Terrorist Financing and Financing of the Proliferation of Weapons of Mass Destruction"); (2) storage and procedure for dissemination of personal data (Articles 14-16 of the Law of Ukraine "On Protection of Personal Data"). The fact that the practice of implementing compliance programs by banks to ensure compliance with all international and national requirements for data privacy and security has been developed over the years strengthens the argument in this direction. In other words, such institutions already have the experience and reliable infrastructure to verify account holders and suspicious transactions for compliance with KYC/AML requirements. In the case when the NBU assumes the responsibility for opening and maintaining CBDC accounts or chooses another centralized institution for this aim, there is a need to develop and implement data protection and financial privacy programs to ensure the security of new account holders from scratch. A more practical approach on the part of the regulator in this case is to use the private sector for these functions.

In view of the above, Ukraine should avoid disintermediation when developing a CBDC design. The experience of Sweden, where selected intermediary financial institutions are connected to a large CBDC network, but through their own IT infrastructure rather than the NBU's IT infrastructure, is relevant here. In addition, the legislative developments in Norway on the technical support for the issuance and circulation of this type of currency are useful for application at the national level.

In the future, the NBU should further investigate whether the national CBDC design can operate using different types of DLTs and at the same time comply with national and international requirements for data privacy and personal data protection.

The issues of determining the range of entities that will have access to identification data; the circumstances under which such access is possible; and the specifics of managing access to information (in particular, to protect CBDC system participants from unlawful disclosure of their personal and financial information or legal liability related to access to data) are of great importance in this case.

When developing a national digital currency design, the NBU will face a choice: whether the system should operate in (1) a centralized registry maintained by a single authority, or (2) a decentralized registry maintained and modified by all participants connected to the CBDC network. If the decentralized design is chosen, the central bank will have to decide whether access to the ledger and the history of the ledger will be public or private; permissioned or permissionless. In the case of a public ledger, the information in it will be publicly accessible to all members involved in the CBDC network (including end users); a private ledger will be accessible only to a selected subgroup of private business entities.

In general, CBDC systems can be "permissioned" (operated by a group of permissioned entities), "permissionless" (managed by a structure of system participants) and the combination of above. The main focus when choosing a CBDC design is not on the use of DLT itself, but on the system management structure regardless of the technology applied. If the structure has no trusted entities, permissionless systems show efficiency in making possible transactions without establishing trust relationships with third parties. Detailed drawbacks of permissionless design for CBDC are shown in report of the Office of Science and Technology Policy (USA) "Technical Evaluation for a US Central Bank Digital Currency System" (The White House, 2022).

Returning again to the pilot projects of the above countries, it should be noted that the Chinese CBDC project is an illustration of an operating design of a centralized ledger managed by the PBoC, using the concept of "controlled anonymity" to ensure the confidentiality of transactions. This method ensures that transactions remain private to those outside the system, with the exception of the PBoC, which can track the movement of electronic payments in digital currency, and the link between addresses and user identification is known to the central bank only through the KYC process.

However, the regulator takes additional measures to protect against unlawful state surveillance by using firewalls for any information related to CBDC, appointing special personnel to manage the information and prohibiting all arbitrary information requests (Ross, 2023).

Unlike China's CBDC project, the Swedish and Norwegian projects are examples of a DLT operating design using the Corda and Ethereum platforms, respectively.

In particular, e-krona "transactions are not recorded in a central database, but in the nodes of the participants directly involved in the transaction" (Sveriges Riksbank, 2022, p. 5). E-currency wallet holders - transaction initiator, in short, have access to the public digital ledger of e-currencies and can make changes to it. At the same time, this approach has raised concerns, including from the Swedish central bank. It is unclear how the exchange of information based on DLT/blockchain technology will be correlated with existing legislation on financial confidentiality and data protection. It is likely that the data accompanying a transaction in the transaction history will be considered personal data and subject to financial privacy protection. Therefore, legislative changes and/or information security measures may be required (Sveriges Riksbank, 2022). To ensure full compliance of the e-krona pilot system with data protection legislation, it is advisable to hold joint consultations between the Swedish and European Union data protection authorities on how DLT/blockchain technology relates to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation (GDPR)).

Ukraine is also considering the possibility of issuing and circulating e-hryvnia based on the DLT operating design (Stellar) (Atlantic Council, 2023). To date, the central bank has no official finalized information on the national design of the digital currency. However, if the NBU decides to issue and circulate the e-hryvnia based on the Stellar distributed ledger operating design, Ukraine will also face issues of its security and compliance with data protection legislation. This has been repeatedly emphasized in the scientific literature. Sandner (2019) in his article "How Should Companies Choose a Specific Blockchain Framework?" notes that aspects of the GDPR remain unclear for DLTs

such as Ethereum, Stellar, Corda, etc. In terms of security, Ethereum is superior to all others in terms of resilience due to the fact that it exists as a public system.

These issues were investigated by the European Parliament's Research Service back in 2019. The analysis identified the following main critical contradictions between DLT and GDPR. First, the GDPR provides for the existence of at least one natural or legal person - a data controller - to whom data subjects can address to protect their rights under EU data protection law. In contrast, DLT replaces the single responsible entity with several entities, which "prevents the distribution of responsibility and accountability". Secondly, the GDPR contains a provision that data can be changed or erased if necessary to comply with legal requirements, in particular Articles 16 and 17 of the GDPR. Instead, "it is because of DLT's append-only nature that the modification and erasure of data that is required by the GDPR under some circumstances cannot straightforwardly be implemented" (European Parliament, 2019, p. 3).

This raises the question of whether it is possible to create a national CBDC design based on DLT in a way that does not contradict the requirements of national and international privacy legislation. As is well known, digital assets, which central banks are trying to develop their own currencies against, are attractive to citizens, businesses, and others because of the ability to conduct direct and instant transactions in an anonymous manner, as well as the ability to track and verify transactions through a public ledger.

However, the approach of creating a national CBDC design based on DLT with complete anonymity of transactions in such a currency may conflict with national legislation, in particular the Law of Ukraine "On Prevention and Counteraction to Legalization (Laundering) of Proceeds of Crime, Terrorist Financing and Financing of the Proliferation of Weapons of Mass Destruction". The requirement for permissioned operators to report suspicious transactions makes it impossible to develop a CBDC system that operates on the basis of a decentralized public ledger with complete anonymity of identification data.

A national CBDC design could be created on the basis of a centralized registry, similar to the way Ukraine's payment system is currently operating. Only selected financial institutions would have access to the transaction register and registry history in order to comply with legal

requirements, including personal data protection. Under such conditions, the legal risks associated with DLT will be levelled. At the same time, this approach may limit the ability to fully incorporate the latest features in areas such as encryption and programming, which may limit innovation but also arguably better protect consumers, investors and businesses (The White House, 2022). In view of the above, it can be concluded that a centralised approach (centralised design) would be a better option for Ukraine.

Alternatively, the NBU could consider creating a CBDC design based on a private and permissioned DLT, where details of digital currency transactions would be available to permissioned financial institutions. At the same time, the identifying data of CBDC transactions must be available to such institutions in order to comply with legal requirements, in particular with respect to financial monitoring, using highly secure cryptographic technology. Thus, permissioned financial institutions may assign a randomly generated alias to each end-user account after identifying the person at the account opening stage. This alias will be displayed in the private ledger for a while. As a result, information on the amount of the transaction associated with randomly generated account alias will be available to the relevant institutions (similar to the concept of e-krona pseudonyms) (Sveriges Riksbank, 2022). Under normal circumstances, such transactions will not be traceable to end users. However, in the event when it is identified that information is related to suspected money laundering, terrorist financing and/or financing of the proliferation of weapons of mass destruction and/or other illegal financial transactions, authorized financial institutions should be able to match anonymous pseudonym information with a specific account holder. The NBU could consider a number of approaches to securely block alias and at the same time allow for identification data matching. The World Economic Forum's Digital Currency Governance Consortium White Paper Series will be useful in this case. They present possible "cryptography methods, with examples of how they could be used to enhance privacy in CBDCs". These include: zero-knowledge proofs, symmetric key cryptography, public-key (asymmetric-key) cryptography, multi-party computation, differential privacy, and homomorphic encryption (WEF, 2021).

Discussion

Implementing CBDC in practice may lead to a number of risks related to data privacy, security of payments (Islam & In, 2022; Fanti & Pocher, 2022; Auer et al., 2023; Tsang et al., 2022), unprecedented control over financial transactions by government agencies (Salter, 2022), disintermediation of the banking system (Eren et al., 2022; Banet & Lebeau, 2022; Chang et al., 2022) etc. As a result, the NBU should take a more careful approach to optimizing these risks. Given the predominant approach of countries to implementing CBDCs based on various types of DLT, the above is of particular importance. Continuing the debate in this area it should be noted that the data privacy and security of payments issues raised by DLT are relatively new and very complex. And they will only become more complex as technology advances. In order to create a national CBDC design based on DLT and take advantage of all the benefits of this technology while complying with national and international legislative on payment privacy and security, it is advisable that Ukraine (represented by the NBU and other government authorities involved in the CBDC research project) actively engages in international dialogue and joint research on relevant issues. After all, a digital currency design that, for example, does not meet the requirements of European documents (in particular, the GDPR) will limit its use in the global payment system and will have a negative impact on the image of Ukraine as a future member of the European Union. In order to prevent such negative consequences for the country, the authors formulate the following proposals and conclusions.

Conclusions

Analysis of international approaches, drawing from reports on CBDC pilot projects in Sweden, China, and Norway, reveals potential negative consequences associated with CBDC implementation. These include data privacy and security risks, complications in financial monitoring, contradictions with current national and international legislation (such as GDPR and FATF recommendations), and the risks of disintermediation of banks. To mitigate these consequences, particularly in light of Ukraine's Association Agreement and its recent EU candidate status, it is imperative to expedite the harmonization of national legislation with international standards.

Addressing the technical features of Ukraine's CBDC design, it is recommended to proactively eliminate disintermediation risks by retaining private sector financial institutions as intermediaries. This approach, involving entities with robust data protection and security programs, ensures a balance between data privacy and the protection of private interests. Additionally, to align the technical design with international and national legislation, the proposal suggests operating the CBDC on a centralized ledger or, until common international legal approaches are established, on a private permissioned DLT. This necessitates intensified international participation by Ukraine to contribute to the resolution of pertinent issues. In summary, the proposed measures aim to ensure the seamless alignment of Ukraine's CBDC with legal and regulatory frameworks while safeguarding privacy, security, and financial stability.

Bibliographic references

- Allen, F., Gu, X., & Jagtiani, J. (2022). Fintech, Cryptocurrencies, and CBDC: Financial structural transformation in China. *Journal of International Money and Finance*, 124, 102625. <https://doi.org/10.1016/j.jimonfin.2022.102625>
- Allen, S., Čapkun, S., Eyal, I., Fanti, G., Ford, B. A., Grimmelmann, J., ... & Zhang, F. (2020). Design Choices for Central Bank Digital Currency: policy and technical considerations (No. w27634). *National Bureau of Economic Research*. <https://doi.org/10.3386/w27634>
- Atlantic Council. (2023). Central Bank Digital Currency Tracker. Retrieved from: <https://www.atlanticcouncil.org/cbdctracker/>
- Auer, R., Böhme, R., Clark, J., & Demirag, D. (2023). Mapping the privacy landscape for Central Bank Digital Currencies. *Communications of the ACM*, 66(3), 46-53. <https://doi.org/10.1145/3579316>
- Auer, R., & Boehme, R. (2021). Central bank digital currency: The quest for minimally invasive technology (No. 948). *Bank for International Settlements*. <https://www.bis.org/publ/work948.pdf>
- Ballaschk, D., & Paulick, J. (2021). The public, the private and the secret: Thoughts on privacy in central bank digital currencies. *Journal of Payments Strategy & Systems*, 15(3), 277-286.
- Banet, J., & Lebeau, L. (2022). Central Bank Digital Currency: Financial inclusion vs disintermediation. *Federal Reserve Bank of Dallas, Working Papers*, 2218, 49. <https://doi.org/10.24149/wp2218>
- Belke, A., & Beretta, E. (2020). From cash to private and public digital currencies. the risk of financial instability and "Modern Monetary Middle Ages." *Economics and Business Letters*, 9(3), 189-196. <https://doi.org/10.17811/eb1.9.3.2020.189-196>
- Bindseil, U. (2020). Tiered CBDC and the financial system. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3513422>
- Boar, C., & Wehrli, A. (2021). Ready, steady, go? - Results of the third BID survey on central bank digital currency. *BIS Papers 114. Basel. Bank of International Settlements*. <https://www.bis.org/publ/bppdf/bispap114.pdf>
- Boar, C., & Wehrli, A. (2021). Ready, steady, go?-Results of the third BIS survey on central bank digital currency. *BIS papers*.
- Brunnermeier, M. K., James, H., & Landau, J. (2019). The digitalization of money. (No. w26300). National Bureau of Economic Research. <https://doi.org/10.3386/w26300>
- Carrat, R. J. (2018). *The future of Money: digital currency on monetary policy and trade of the committee on financial services U.S. House of Representatives Serial № 115-11. U.S. Government Publishing Office*. <https://acortar.link/dGhdPn>
- Carstens, A. (2019). *The future of money and payments*. Bank for International Settlements. <https://www.bis.org/speeches/sp190322.pdf>
- Changi, H., Grinberg, F., Gornicka, L., & Miccoli, M. (2022). Central Bank Digital Currency and Bank Disintermediation in a Portfolio Choice Model, 44. [File PDF]. <https://acortar.link/oPzyvG>
- Chernyshova, O., Voznyakovs'ka, K., & Bashlay, S. (2021). The global experience of the development of digital currencies of central banks and its implementation in Ukraine. *Economy and society*, 33. <https://doi.org/10.32782/2524-0072/2021-33-87>
- Duffie, D., Mathieson, K., & Pilav, D. (2021). Central bank digital currency: Principles for technical implementation. Available at SSRN 3837669. <https://doi.org/10.2139/ssrn.3837669>
- Eren, E., Jackson, T., & Lombardo, G. (2022). Efficient disintermediation with CBDC, 39. [File PDF]. Retrieved from: <https://acortar.link/QYaDTTr>
- European Central Bank. (2022). *Progress on the investigation phase of a digital euro – second report*. <https://acortar.link/WxRi25>

- European Parliament (2019). *Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?* <https://acortar.link/jN6C0i>
- Fanti, G., & Pocher, N. (2022). *Privacy in Cross-border Digital Currency. A Transatlantic Approach. In Frankfurt Forum on US-European GeoEconomics* (pp. 1-25). Atlantic Council.
- Fernández-Villaverde, J., Sanches, D., Schilling, L., & Uhlig, H. (2020). Central Bank Digital Currency: Central Banking for All?. *Review of Economic Dynamics*, 41, 225-242. <https://doi.org/10.3386/w26753>
- FSB (2020a). *Financial Stability Board, Enhancing Cross-Border Payments: Stage 1 Report to the G20*. <https://www.fsb.org/wp-content/uploads/P090420-1.pdf>
- FSB (2020b). *Financial Stability Board, Enhancing Cross-Border Payments: Stage 3 Roadmap*. <https://www.fsb.org/2020/10/enhancing-cross-border-payments-stage-3-roadmap/>
- Gross, J., Sedlmeir, J., Babel, M., Bechtel, A., & Schellinger, B. (2021). Designing a Central Bank Digital Currency with Support for Cash-like Privacy. [File PDF]. Retrieved from: <https://acortar.link/opFzPf>
- Hoskinson, C. (2022). Why CBDCs 'Are A Really Bad Idea. *Cardano Feed*. <https://acortar.link/fOaT0g>
- Hrytsay, S. O. (2022). Central Banks' digital currency – threats and challenges. *Actual Problems of Native Jurisprudence*, (1), 144-149. <https://doi.org/10.32782/392256>
- Islam, Md. M., & In, H. P. (2022). A privacy-preserving transparent central bank digital currency system based on consortium blockchain and unspent transaction outputs. *IEEE Transactions on Services Computing*, 16(4), 2372-2386. <https://doi.org/10.1109/tsc.2022.3226120>
- Keister, T., & Sanches, D. (2021). Should Central Banks issue digital currency? Working Paper. *Federal Reserve Bank of Philadelphia*. <https://doi.org/10.21799/frbp.wp.2021.37>
- Kiff, J., ALwazir, J., Davidovic, S., Farias, A., Khan, A., Khiaonarong, T., ... Zhou, Z. (2020). A survey of research on Retail Central Bank Digital Currency. *SSRN Electronic Journal*, 2020(104), 66. <https://doi.org/10.2139/ssrn.3652492>
- Khodakevich, S., Ponomarenko, K., & Urvantseva, S. (2022). Digital currencies of central banks: Essence and prospects of implementation. *Strategy of Economic Development of Ukraine*, 50, 71-81. <https://doi.org/10.33111/sedu.2022.50.071.081>
- Mancini-Griffoli, T., Peria, M. S., Agur, I., Ari, A., Kiff, J., Popescu, A., & Rochon, C. (2019). Casting light on Central Bank Digital Currency. *Oxford University Press*, 307-340. <https://doi.org/10.1093/oso/9780190077310.003.0012>
- Meher, A. (2020). Spending Corda State on Different Notaries. *Medium*. <https://acortar.link/2nUFlt>
- NBU (2022). *NBU Unveils E-hryvnia Concept to Payment Market and Virtual Asset Market Participants*. <https://acortar.link/5RFMnr>
- Niepert, D. (2018). Reserves for all? Central Bank digital currency, deposits, and their (non)-equivalence. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3254206>
- People's Bank of China. (2021). *Progress of Research & Development of E-CNY in China*, 3. <https://acortar.link/wafHvg>
- Pocher, N., & Veneris, A. (2021). Privacy and transparency in cbdc: A regulation-by-design AML/CFT scheme. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3759144>
- Pollock, A. J. (2018). The future of Money: digital currency on monetary policy and trade of the committee on financial services U.S. House of Representatives (Serial № 115–11). *U.S. Government publishing office*. <https://acortar.link/dGhdPn>
- Ross, R. (2023). Data Privacy and Security Implications of a US Central Bank Digital Currency (CBDC). *Seton Hall University. Advance online publication*. <https://acortar.link/lnMsmU>
- Salter, A. (2022). CBDC in the USA: Not Now, Not Ever. *Aier*. Retrieved from: <https://www.aier.org/article/cbdc-in-the-usa-not-now-not-ever/>
- Sandner, P. (2019) How Should Companies Select a Specific Blockchain Framework? *Medium*. Retrieved from: <https://acortar.link/EKWDbm>
- Santaolalla Montoya, C. (2023). Do central bank digital currencies (CBDC) protect the consumer or are they a mirage. *SSRN Electronic Journal*, p. 199-211. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4371075
- Sethaput, V., & Innet, S. (2021). Blockchain application for Central Bank Digital Currencies (CBDC). 2021 Third International Conference on Blockchain Computing and Applications (BCCA). *IEEE*. <https://doi.org/10.1109/bcca53669.2021.9657012>

- Sethaput, V., & Innet, S. (2023). Blockchain application for Central Bank Digital Currencies (CBDC). *Cluster Computing*, 26, 2183-2197. <https://doi.org/10.1007/s10586-022-03962-z>
- Shapoval, Y. (2020). Central Bank Digital Currencies: Experience of pilot projects and conclusions for the NBU. *Economy and Forecasting*, 2020(4), 97-115. <https://doi.org/10.15407/econforecast2020.04.097>
- Sveriges Riksbank. (2022). E-krona report phase 2022. [File PDF]. Retrieved from: <https://acortar.link/pJviER>
- Syrstad, H. (2023). Introduction of central bank digital currency – necessary legislative amendments. *Norges Bank*. <https://acortar.link/K82FPw>
- The White House. (2022). *Technical Evaluation for a US Central Bank Digital Currency System*. <https://acortar.link/Nvil8C>
- Tronnier, F. (2021). *Privacy in payment in the age of Central Bank Digital Currency*. In Privacy and Identity Management: 15th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Maribor, Slovenia, September 21–23, 2020, Revised Selected Papers 15 (pp. 96-114). Springer International Publishing. https://doi.org/10.1007/978-3-030-72465-8_6
- Tsang, C. Y., Yang, A. Y. P., & Chen, P. K. (2022). Disciplining Central Banks: Addressing the Privacy Concerns of CBDCs and Central Bank Independence. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.4253888>
- U.S. Department of the Treasury (2022). *The Future of Money and Payments: Report Pursuant to Section 4(b) of Executive Order 14607*, 51. <https://acortar.link/PB5dGJ>
- Veneris, A., Park, A., Long, F., & Puri, P. (2021). Central Bank Digital Loonie: Canadian cash for a new global economy. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3770024>
- Wee, R. (2023). China's digital yuan transactions seeing strong momentum, says cbank Gov Yi. *Reuters*. <https://acortar.link/VsWcNd>
- WEF (2021). *Privacy and Confidentiality Options for Central Bank Digital Currency*. *World Economic Forum, Digital Currency Governance Consortium White Paper Series*, 5. <https://acortar.link/ufD53a>