Project Thesis: Offline Payment Requirements for Central Bank Digital Currencies

Atangana Olivier

Supervisors Prof. Lyes Khoukhi
Institution: University of Caen

1 Abstract

In the context of the global digitization of financial transactions marked by the decline in cash usage, central bank-issued digital currencies (CBDCs) have emerged as a major innovation. However, although CBDCs aim to revolutionize the payment industry in its technical, sociological, and economic aspects, the obstacles and pitfalls related to their deployment remain numerous. Among these challenges is offline payment. This thesis proposes to examine the offline payment requirements for CBDCs, particularly by developing a payment framework that emphasizes the need to ensure the security, privacy, and accessibility of transactions without a central network connection. Subsequently, the research objectives are threefold: first, to ensure the security of offline transactions by preventing frauds such as double spending and double incoming; second, to guarantee privacy by developing protocols that maintain the confidentiality of transaction data and sensitive user information; and finally, to create a solution that integrates seamlessly with existing payment systems and is capable of adapting to modern infrastructures, allowing for transparent synchronization of transactions. Furthermore, the research methodology will first involve inventorying and evaluating the relevance and limitations of current CBDC technologies concerning offline payments. Then, investigate and exploit modern cryptography protocols on privacy protection. Finally, develop and test a viable offline payment solution using advanced technologies such as blind signatures and the zk-SNARK protocol. Ultimately, the key results include the development of an

innovative robust payment protocol ensuring confidentiality, authenticity of transactions, and thus addressing the concerns of users and regulators.

2 Project Description

2.1 Context and Problem Statement

The last decade has been marked by the emergence of digital technologies such as smartphones, Cloud Computing, blockchain, and artificial intelligence. Subsequently, the growing adoption of these digital technologies heuristically revolutionizes and transforms multiple domains of daily life, including payment systems with the advent of central bank digital currencies. Thus, CBDCs, which are a digitization of fiat currency, are developing within the orbit of the technological transition movement inherent in the global economy, marked by a preferential option for digital transactions. Following the 2008 financial crisis, which was succeeded by the all-around flourishing of cryptocurrencies and the emergence of the coronavirus pandemic, many countries and organizations accelerated their digital transformation to align with electronic payment systems. Nearly 80% of payments were made via smartphone in 2021 in China [1]. In the proliferation of digital currencies, the digital issuance trend of CBDCs, given its advantages in terms of speed, cost, trust, and stability, is a real opportunity and a guarantee of safety for public and private financial actors [2]. Hence, CBDCs are a credible alternative to the volatility of cryptocurrencies and a complementary option for electronic payment in an economic context undergoing full digital transition. The multiple initiatives and research projects like the digital euro, E-CNY, E-Krona, E-Naira, etc., implemented by contributions from academic, governmental, and private institutions sufficiently demonstrate the growing interest in CBDCs.

However, although CBDCs offer great promises, their deployment involves facing a plurality of complex challenges, notably security, privacy, interoperability, and offline transactions. The latter aspect implies that the payer and the beneficiary are not connected to the internet or a central network when the transaction is carried out [3]. Ensuring security, efficiency, and confidentiality while complying with regulatory constraints on anti-money laundering (AML) and countering the financing of terrorism (CFT) is crucial for the widespread adoption of CBDCs.

2.2 Motivation

The main motivation of this thesis lies in addressing the challenges related to offline payments for CBDCs by establishing a wallet that offers the possibility of maintaining a cash-like experience and improving financial inclusion, access, and resilience, particularly in regions where internet access is non-existent, limited, or intermittent. The detailed motivations underlying this research are as follows:

2.2.1 Security of Offline Transactions

The security requirements when considering implementing the offline payment function for digital currencies are defined in terms of protection against Double Spending. It is crucial for offline payments to avoid the risk of double spending, where the same unit of digital currency could be spent multiple times before synchronization with the central network. Another requirement is unforgeability because digital currency should not only aspire to replicate the properties of cash but also be better than cash, implying protection against counterfeiting. Currently, digital currencies are more susceptible to counterfeiting than hard currency. The security of offline payments also underscores the importance of verifiability, as the adopted payment protocol must ensure the recording and non-falsification of transactions. For optimal security, non-repudiation is also necessary, guaranteeing that the receiver has received authentic digital currency during the payment. Additionally, other features such as protection against DDoS attacks and post-quantum attacks can be considered.

2.2.2 Privacy of Transaction Data

Preserving privacy is an essential aspect of CBDC deployment. A survey conducted by the ECB revealed that privacy is a prized feature by users and payment system actors [4]. Given that users are increasingly concerned about the confidentiality of their financial transactions, payment professionals are working to offer privacy-based solutions [5]. The clear objective is for CBDCs to guarantee that transaction data remains private and protected against profiling risks and undue surveillance, such as citizen surveillance and dataveillance orchestrated by Big Data. Furthermore, leveraging privacy-enhancing technologies within the cryptographic paradigm allows overcoming challenges

inherent to preserving user privacy. Thus, the use of privacy-enhancing technologies such as blind signatures, zk-SNARK, and homomorphic encryption ensures that transactions remain confidential while ensuring their validity and authenticity [6].

2.2.3 Financial Inclusion

Driven by the wings of accessibility and resilience, the CBDC revolution implies enabling greater access to financial services, particularly for unbanked or underbanked populations. In this vein, offline payment is an interesting option as it provides a reliable digital payment method without dependence on continuous online infrastructure. Moreover, offline transactions offer resilience against network outages and service interruptions, ensuring continuity of financial operations even in the absence of connectivity. Additionally, deploying offline mode is favorably received in areas where internet connectivity is absent or intermittent, such as rural areas and regions with insufficient network infrastructure.

2.2.4 Interoperability and Integration

First, by ensuring compatibility with existing systems. CBDCs should not be seen through the lens of adversity but through the lens of complementarity with existing payment methods. Implementing offline payment solutions requires seamless integration into central banking systems and interoperability with existing and modern payment infrastructures such as blockchain. Second, it is crucial to ensure data synchronization. Maintaining the integrity and accuracy of financial records is crucial for verifiability and audit purposes. Therefore, ensuring effective and secure synchronization of transaction data once connectivity is restored is important.

Overall, this thesis aims to address these motivations by developing a secure and confidential offline payment framework for CBDCs, using advanced technologies such as blind signatures and zk-SNARK. This research on offline payment requirements for CBDCs aims to contribute to the evolution of digital payment systems by establishing robust and reliable solutions for offline transactions.

3 Literature Review

3.1 Synthesis of Some Existing Works on Offline CBDC Payments

A plethora of serious work has been done to define the characteristics, issuance, reception, and recording modalities of CBDCs as well as their deployment infrastructure. Research on offline payment functions has garnered significant attention since the emergence of electronic money. Despite this interest, few protocols or frameworks exist for offline CBDC payments in the current landscape [4]. Below, we mention some relevant works that have already been done on this subject:

The Offline Payment System (OPS) protocol proposed in [5] establishes a two-tier certificate infrastructure set up by a delegated financial authority. It employs cryptographic algorithms, enabling secure payments from Alice to Bob without Bob needing a security device. However, it may not fully meet the requirements of non-falsification and DDoS attack prevention.

Furthermore, an extension of OPS employing an ISO/IEC 7816-compatible smart card and an NFC interface addresses these issues by setting transaction time limits and using cryptographic keys on the smart card [6]. Another proposal employs a One-Time Programm (OTP) for each monetary unit, to ensure confidentiality, anonymity, and programmability [7]. However, vulnerabilities exist during OTP transmission and framework forgery risks. Among these vulnerabilities are attacks by intercepting data transmitted via NFC, exploiting transaction time limits to conduct denial-of-service attacks, smart card cloning, weaknesses in cryptographic key management, and risks of transaction data forgery.

In [8], a flexible, programmable two-tier architecture solution requiring a secure Tamper Resistant Element (TRE) to counter hardware attacks is proposed, offering various transaction scenarios and adaptable confidentiality levels. However, the integration of blockchain introduces de-anonymization risks. In [9], the aim is to evaluate the feasibility and effectiveness of an offline CBDC as a digital alternative to cash, focusing on potential benefits and associated challenges. The results indicate that while offline CBDCs can offer some security and inclusivity advantages, they face several major limitations. Despite potential benefits, the practical implementation of offline CBDCs encounters several obstacles. Among the main limitations are the need for sufficient demand for widespread adoption, the difficulty of replicating all

cash characteristics, increased fraud risks, and technical challenges related to frequent online synchronization.

3.2 Identifying Gaps in the Current Literature

Numerous solutions are being explored in the field of digital currencies, with various levels of experimentation underway [10]. On the one hand, there are already operational solutions, but they do not fully meet the criteria sought by central banks, particularly the European Central Bank (ECB). On the other hand, pilots and studies show the feasibility of network-free payments using secure embedded systems like smart cards and smartphones. However, they still raise issues such as fraud risk assessment and transaction consolidation. Each solution presents advantages and disadvantages in its current state, as described in [11].

Multiple layers of protection are necessary to promote resilience and maintain a secure CBDC system. Although any form of CBDC carries certain risks, the offline functionality introduces new dangers, particularly internet disconnection and the introduction of physical hardware accessible to malicious actors [12]. Threats can seem similar to those faced by an online system, such as attempts to increase funds without authorization, spending the same funds more than once (double spending), duplicating devices, or altering limits [13].

In [14], the challenges related to privacy and offline transactions in the context of CBDCs are analyzed while exploring existing solutions and proposing new approaches. The study highlights the difficulties encountered in preserving user privacy and establishing effective offline transactions in CBDC systems. However, despite the importance of these aspects, several limitations have been identified. Regarding privacy, it is crucial to find a balance between protecting user data and compliance requirements while considering risks associated with data collection. Additionally, implementing offline transactions poses technical and security challenges, and there is a gap between the perception of their importance by central banks and researchers. Although solutions such as using hash chains have been proposed, unresolved questions remain concerning risk management and interoperability with existing systems. Future work could involve extending existing prototypes, exploring new methods of privacy preservation, and evaluating the impact of proposed solutions on user experience and overall system security.

4 Methodology

This thesis aims to ensure optimal security and confidentiality for the flow of CBDC payment transactions in offline mode. To achieve this, the research methodology relies on the dynamics of three action verbs: understand, analyze, and implement. Specifically, it involves immersing oneself in the latest research advances on offline CBDC projects through literature studies, participation in seminars, and technological monitoring on the subject. Then, in the analysis phase, it is necessary to identify the shortcomings and challenges of current CBDC solutions and examine the relevance of modern technologies used for offline payments involving digital currencies.

Finally, it will be essential to implement a viable offline payment solution for the CBDC ecosystem. This final aspect will be structured into three moments: developing the solution by establishing a payment protocol, testing and validation, which will involve testing the developed solution in a simulated environment to verify its effectiveness and security. Finally, ensuring the integration of solutions with existing payment infrastructures by developing APIs and synchronization interfaces.

5 Research Axes

Offline transactions of Central Bank Digital Currencies (CBDCs) represent a major innovation in the digital payment ecosystem, given their contributions to resilience and financial inclusion. However, for the implementation of offline CBDC payment solutions, it is imperative to address security, confidentiality, and interoperability challenges. Consequently, this thesis aims to respond to these motivations by defining the technical characteristics of an electronic currency based on a secure and resilient infrastructure. In other words, defining an operational system capable of ensuring offline payment when the central infrastructure is unavailable or when network quality is degraded while guaranteeing transaction security, traceability, and the authenticity of the issuer. In this vein, this thesis proposes to contribute through four research axes:

5.1 Definition of the characteristics of the electronic wallet

It is the matrix of electronic currency, in all its contours and with its security constraints. This assumes initially ensuring the security services of a traditional computer system, namely integrity, non-repudiation, access control, confidentiality, availability, identity, and authentication. The latter service will be particularly important as it will be necessary to ensure the identity of the buyer or prove the issuer's identity during payment. This is where the expertise of the FIME biometrics laboratory, in collaboration with the GREYC laboratory's Electronic and Biometrics team specializing in the evaluation of behavioral biometrics, will be of great contribution. Indeed, biometric authentication linked to payment is increasingly popular in the market and even required by new regulations on electronic payment. Additionally, it will be necessary to integrate a feature to protect against double spending and a hardware and/or software privacy protection module. This is one of the reasons why research on CBDCs related to Distributed Ledger Technologies (DLTs), which prioritize privacy, is significantly developing.

5.2 Establishing the communication protocol between two electronic wallets

Cryptography knowledge will inevitably be necessary because any envisaged protocol must ensure transaction authenticity (obviously without overburdening the execution of the transaction itself) through encryption. Encryption tools such as asymmetric encryption, elliptic curve cryptography, and cryptographic signature are very interesting avenues. Furthermore, the development of quantum computing units implies planning, if not implementing, the possible integration of a post-quantum algorithm. Additionally, for the transmission of payment data (account-based or token-based), a study of protocols such as the NFC protocol, BLE protocol, or the use of QR codes with single or mutual authentication should be considered. For illustration, the payment card provider Visa currently implements the OPS (offline payment system) protocol, which allows point-to-point authorization during offline payments using open-source technology and a public key infrastructure.

5.3 Synchronization with the central network

The central network, for this purpose, is the central bank, the trusted third party, fund provider, and guarantor of the financial stability of the system. The main challenge will be to coexist offline and online electronic wallets, combine their exchanges so that fund transfer and recovery are achieved properly, simply, and transparently for the actors. Many CBDC-based architectures consider integrating an API to ensure the link between payment actors and central banks.

5.4 Fraud detection

The research will be complemented by studying the impact of an embedded artificial intelligence solution on fraud prevention. Cyber attackers and cyber fraudsters are competing in skill to compromise cryptocurrency systems. Consequently, as their techniques develop, innovation must provide a consequent response. In this case, to counter fraud techniques such as double spending, double incoming, replay, etc.

6 Contributions

The primary objective of this thesis is to propose a secure and confidential framework for offline payments using central bank digital currencies (CBDCs). Leveraging advanced technologies and a rigorous methodology, the expected results of this research can be summarized as follows:

6.1 Ensuring Security and Resilience

- **Currency Storage**: Unspent CBDC units should be protected against any theft or counterfeiting attempts by integrating a Trusted Execution Environment (TEE).

- **Double Spending and Replay Attack Prevention**: The combined development and implementation of digital signatures, blind signatures, and the zk-SNARK protocol will ensure that each unit of CBDC is not only authentic but can only be spent once in offline transactions. The zk-SNARK algorithm ensures that transactions can be verified without revealing sensitive information, guaranteeing that the same unit of currency cannot be used in multiple transactions.

- **Proactive Fraud Detection**: Integrating an embedded system based on a stochastic method as well as federated learning and biohashing within the proposed framework will ensure that illicit transactions are detected and, if necessary, canceled before their completion. The embedded AI model must itself be protected against any poisoning attack attempts by exploiting backdoor vulnerabilities.

6.2 Transaction Data Privacy

- **Privacy Protection**: The system will be based on privacy by design and by default. The use of blind signatures will maintain message confidentiality during the withdrawal and offline payment process, ensuring that neither the content of transactions nor the identities of the involved parties are exposed. The zk-SNARK protocol will be used to verify transactions confidentially, without requiring disclosure of sensitive information, thus protecting users from undue surveillance and tracking. The system must ensure end-to-end privacy (online/offline) even within the framework of integrating a blockchain. Balance updates will be done confidentially by exploiting homomorphic encryption.

- **Compliance with Privacy Regulations**: The proposed framework will comply with privacy and data protection standards, ensuring easier adoption and acceptance by users and regulators. By integrating privacy protection principles from the design phase and by default, the framework will address the growing concerns of users regarding the confidentiality of their financial transactions. For transparency needs, the system will be auditable by exploiting mechanisms compliant with contextual privacy.

6.3 Interoperability and Integration

- **Compatibility with Existing Systems**: Developing APIs and synchronization interfaces will facilitate the integration of the offline payment solution with existing centralized payment infrastructures. The proposed solution must be deployable in a heterogeneous environment, facilitating interoperability with current payment systems and modern systems through the establishment and integration of digital identity, thus allowing smoother adoption by financial institutions and users.

- **Effective Data Synchronization**: The framework will ensure transparent, secure, and double-import-free synchronization of transaction data

once network connectivity is restored, guaranteeing the coherence and integrity of financial records on offline and online wallets. The developed synchronization mechanisms will operate in a secure channel and minimize disruptions, ensuring that all transactions are correctly recorded and validated by the ledger.

6.4 Improved Accessibility

Offline payment solutions will be designed to operate on mid-cost devices to facilitate access to financial services for unbanked, underbanked, or marginalized population segments.

6.5 Practical Implications and Future Perspectives

- **Cost Reduction of Issuance**: The proposed framework will contribute to reducing the costs of CBDC issuance and transaction processing by the central network. Reducing dependence on cash will enable substantial savings for central banks and financial institutions.

- **Improvement of Sustainability**: The proposed framework will also consider sustainable development issues by proposing energy-efficient and low-cost consumption for each transaction.

7 Conclusion

In conclusion, this research will significantly contribute to the evolution of digital payment systems by proposing robust, secure, and confidential solutions for offline CBDC transactions. The expected results will have a major impact on financial inclusion, the resilience of payment systems, and the widespread adoption of CBDCs worldwide.

References

[1] Knoerich. "China's new digital currency: implications for renminbi internationalization and the US dollar. In: The (Near) Future of Central Bank Digital Currencies: Risks and Opportunities for the Global Economy and Society", Global Politics and Security (2021): 145-166.

[2] Ahmet Faruk Aysan, Farrukh Nawaz Kayani, "China's transition to a digital currency: does it threaten dollarization?" Asia and the Global Economy (2022).

[3] Bank for International Settlements (BIS), "BIS Handbook of Offline Payment," BIS Papers, No. 100, March 2023. [Online]

[4] European Central Bank, Eurosystem, https://www.ecb.europa.eu/pub/pdf/other/Eurosystem_report_on_the_public_consultation_on_a_digital_euro~539fa8cd8d.en.pdf

[5] Digital Euro Association, "Privacy and Central Bank Digital Currencies", Public Digital Euro Working Group, 2023.

[6] O. Atangana, M. Barbier, L. Khoukhi, and W. Royer, "Securing privacy in offline payment for retail central bank digital currencies: A comprehensive framework, Proceedings of the Conference on Blockchain and Cryptocurrency", Greece, vol. 2, pp. 25–32, October 2023.

[7] M. Christodorescu et al., "Towards a Two-Tier Hierarchical Infrastructure: An Offline Payment System for Central Bank Digital Currencies," arXiv 2012, arXiv:2012.08003.

[8] A. Dogan et al., "Smart Card Based Offline Payment System for Central Bank Digital Currencies," in Proceedings of the Conference on Blockchain and Cryptocurrency Congress (B2C' 2022), Barcelona, Spain, 9-11 November 2022, pp. 114-127.

[9] L. Mainetti et al., "A Sustainable Approach to Delivering Programmable Peer-to-Peer Offline Payments," Sensors, Vol. 23, Issue 2, 2023, 1336.

[10] Idemia, "Offline CBDC payments," IDEMIA, 2023.

[11] NURMINEN, Julia, SCHRECK, Johanna, et al. "Reining in the expectations of offline payments," 2023.

[12] CBDCTracker (2024), https://cbdctracker.org/, accessed: 2024-04-10.

[13] DARBHA, Sriram. "Archetypes for a retail CBDC," Bank of Canada, 2022.

[14] Armelius, H., C. A. Claussen, and I. Hull. “On the Possibility of a Cash-Like CBDC.” Sveriges Riksbank Staff Memo, 2021.

[15] MINWALLA, Cyrus, MIEDEMA, John, HERNANDEZ, Sebastian, et al. ”A central bank digital currency for offline payments,” Bank of Canada, 2023.

[16] LEE, Michael. ”Analyzing Issues of Privacy and Offline Transactions In Central Bank Digital Currencies,” 2023. Master’s thesis. University of Waterloo.