A Prototype for Privacy-preserving and Compliant Offline CBDC Transactions

Panagiotis Michalopoulos*, Anthony Mack*, Cameron Clark*, Linus Chen*, Johannes Sedlmeir†, Andreas Veneris*‡
* Department of Electrical and Computer Engineering, University of Toronto, Toronto, Canada
{p.michalopoulos, anthony.mack, camo.clark, linus.chen}@mail.utoronto.ca, veneris@eecg.toronto.edu
‡ Department of Computer Science, University of Toronto
† Department of Information Systems, University of Münster, Münster, Germany
johannes.sedlmeir@wi.uni-muenster.de

***Abstract*—Blockchain technology has spawned a vast ecosystem of digital currencies with Central Bank Digital Currencies (CBDCs) – digital forms of fiat currency – being one of them. An important feature of digital currencies is facilitating transactions without network connectivity, which can enhance the scalability of cryptocurrencies and the privacy of CBDC users. However, in the case of CBDCs, this characteristic also introduces new regulatory challenges, particularly when it comes to applying established Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) frameworks. This paper introduces a prototype for offline digital currency payments, equally applicable to cryptocurrencies and CBDCs, that leverages Secure Elements (SEs), Zero-Knowledge Proofs (ZKPs), and digital credentials to address the tension between safeguarding user privacy and ensuring regulatory compliance. The proposed system is validated through a performance evaluation. The results demonstrate that the prototype can be flexibly adapted to different regulatory environments to accommodate various tiers of privacy, with a transaction latency below 5 seconds, thus comparable to real-life commercial payment systems.**

***Index Terms*—CBDC, offline payment, privacy, secure hardware, zero-knowledge**

I. Introduction

The emergence of blockchain has catalyzed the digitalization of payment services [1] through the creation of cryptocurrencies, such as stablecoins [2], representing a significant shift in the global financial landscape. This shift, primarily led by private entities, has created concerns among central banks over private control of payment infrastructures, financial stability, and monetary sovereignty [1], [3]. To maintain the effectiveness of their tools in providing financial stability, central banks are actively investigating [4] digital versions of fiat money, known as *Central Bank Digital Currencies (CBDCs)* [3] and the potential of incorporating blockchain and distributed ledger technologies in their designs [5], [6].

An important feature for both cryptocurrencies and CBDCs is the ability to perform value transfers between parties without requiring a connection to an online ledger or other network infrastructure [7]–[13]. For the former, this functionality can assist in addressing the scalability problem of blockchains [13], while for the latter it ensures payment accessibility during network outages or in regions with limited connectivity, inclusion of under-banked populations, and enhances system resilience during disasters or infrastructure failures [7], [14].

However, *offline CBDCs* also introduce unique regulatory challenges. Their potential to offer transactions without any connectivity (*i.e.,* communication via a third party authority) gives them a level of privacy comparable to that of physical cash. As such, ensuring compliance with Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) regulations becomes a challenge, creating an apparent *trade-off* between privacy and transparency. For instance, real-time transaction screening and monitoring that could uncover illicit activities are not straightforward procedures in such offline scenarios [15]. Additionally, the lack of identification of transacting partners in cash payments today complicates AML/CFT compliance as it effectively anonymizes counterparties and impedes the traceability of monetary flows. Therefore, the question of how digital identity mechanisms can be integrated into offline CBDC systems in a way that enables compliance while preserving user privacy arises as an additional challenge.

This paper addresses these intertwined challenges by arguing for a *compliant-by-design* hardware/software platform [15], [16]. This scheme aims to create inherently compliant payment instruments with digital identity mechanisms. To that end, we introduce an open-source[1] implementation of an offline CBDC prototype that leverages secure hardware and Zero-Knowledge Proofs (ZKPs) to offer regulatory-compliant and privacy-preserving offline transactions. Secure hardware is used to correctly execute an offline payment protocol and to enforce regulatory measures (*e.g.,* holding limits and transaction tracking). Meanwhile, ZKPs allow for privacy-preserving identity verification and compliance checks, such as conditional payments based on user attributes stored within and outside the SE (*e.g.,* age-restricted purchases). The proposed system remains relevant to cryptocurrencies, since similar compliance requirements could prove equally important for cryptocurrencies and decentralized finance [17], [18].

In more detail, the paper's contributions include:

- a proof-of-concept offline CBDC implementation that demonstrates how digital identity attestations can be combined with monetary functions while maintaining privacy and enforcing specific regulatory constraints; and,
- a performance evaluation of the prototype that demonstrates that transaction latency remains below 5 seconds, which is comparable to modern payment systems today, thus confirming the real-life viability of the solution on resource-constrained devices.

II. Background and Related Work

A. Central Bank Digital Currencies

CBDCs are the equivalent of "digital fiat money" as – unlike "commercial bank money" – they represent a liability of the central bank. As such, they serve as an alternative form of base money, next to physical cash and reserve accounts of the private sector maintained at the central bank [19]–[21]. Retail CBDCs – the focus of this paper – are intended for use by the public and can be administered (*e.g.,* account opening)

[1] https://github.com/Veneris-Group/offline-cbdc-prototype

directly by the central bank, giving rise to a *one-tier* model, or administration can be delegated to Financial Institutions (FIs), such as commerical banks, in a *two-tier* model [19] – the latter resembling the financial practice today. Another common – yet contested [15] – classification distinguishes CBDCs between *token-based* and *account-based* [22], [23]. Token-based systems function through the exchange of verifiable cryptographic tokens with a predefined value. Acount-based systems typically depend on some form of identity verification, such as Know-Your-Customer (KYC) procedures, and make use of account balances.

B. Offline CBDC transactions

Offline transactions are payments made in the absence of a connection to an online ledger [7]. Following the classification of offline CBDC systems by the Bank for International Settlements [7], [15], the proposed system falls under the *intermittently offline* category. As such, received funds are available for re-spending but limits to the duration a device can remain offline are imposed through the requirement for periodic synchronization with the online CBDC system.

Current offline CBDC proposals [8]–[12] rely on secure hardware [11], [12] or a combination of secure hardware and cryptographic primitives [8]–[10]. Compared to [11], [12], which do not touch upon compliance, this paper focuses on a solution that enables regulatory compliance in a privacy-preserving way. Compared to [10], which uses custom hardware and physical unclonable functions, we focus on commercial-off-the-shelf smartcards to demonstrate the feasibility of our system on hardware used by the existing payments infrastructure. The works closest to ours are [8] and [9]. In [9], ZKPs are used to provide a private and compliant offline CBDC system that detects double-spenders in case of an SE compromise. In contrast, while acknowledging the potential vulnerabilities of SEs, this paper focuses on the implementation details pertaining to the SE and provides a prototype that could be used as a testbed for further explorations. It also approaches regulatory compliance through the integration of digital identity attestations to the CBDC system. In [8], a system based on an SE combined with a cryptographic protocol to enable private offline token-based CBDC transactions and double spender detection is presented. In comparison, we put an emphasis on addressing the trade-off between compliance and privacy through an account-based approach. Finally, compared to [8], [9], our proposed system exhibits a constant payment latency that does not increase with transaction or token history, and regulatory flexibility since the same firmware adapts to different AML/CFT risk-tiers.

C. AML/CFT in payment systems

AML/CFT regulations aim to safeguard the financial system by preventing criminals from hiding the origins of illegal funds through the assignment of responsibilities to regulated entities (*e.g.,* FIs) [24]. For offline CBDCs, such AML/CFT responsibilities can include, among others [15]: *(i)* KYC by identifying clients and verifying their identity; *(ii)* the association of transactions to user identities; *(iii)* the enforcement of offline usage limits (*e.g.,* thresholds on transaction amount, turnover, or balance); *(iv)* the storing of offline transactions; and *(v)* the automatic or manual monitoring of offline transactions (*e.g.,* transaction tracking, graph analysis).

III. Solution Overview

The proposed system enables users to transact offline in a compliant way. Following are the system's main entities and operations. The section concludes with a discussion of the system's privacy features, supported through the add-on use of ZKPs. A detailed description accompanied by a security analysis can be found in [].

A. Entities

1) Central bank and FIs: Without loss of generality, we assume a two-tiered CBDC system. The central bank issues the CBDC and oversees the operation of the system. FIs interact with the users of the CBDC by performing the necessary KYC procedures and holding users' accounts.

2) Users: System participants maintain an account with an FI, possess a *secure device* equipped with an SE, and install a *wallet application* on their mobile phone. The SE can be embedded in their phone or be separate in the form of a smart card that communicates with the wallet application through the NFC interface of the phone. Without loss of generality, in this paper we assume the latter. Currently, only some smartphones incorporate embedded SEs, and even for these, programmability remains restricted. Although smartphone manufacturers like Google and Apple are beginning to provide limited API access to their SEs [25], [26], which may allow for smartphone implementations, choosing a smart card allows lowering the barrier to entry to the offline system for users who do not own a niche smartphone or with no smartphone at all.

Since SEs are passive elements, i.e., they do not have their own power supply, the phone combined with the wallet application functions as the *user terminal* for the secure device. It provides power, handles the user interface and communication with the secure element, and facilitates the communication between the secure devices of the two users.

3) Public key infrastructure: Every device is assigned a *participation certificate*, which authorizes it to operate inside the system and assigns its role (*i.e.,* either a secure device, a user terminal, or an FI terminal) that is used to restrict access to the secure device's API. For instance, only an FI terminal can initiate the withdrawal protocol. We assume a single *certificate authority* (CA) – *e.g.,* the central bank – signs all certificates and that the cryptographic keypair of each certificate is unique per SE to ensure that compromise of a single key cannot help impersonate any other secure device, and to enable enhanced accountability measures. To eliminate single points of failure, the CA could be replaced by a distributed ledger. In addition, short-lived certificates (*e.g.,* updated in every online synchronization) could prove beneficial for limiting fraudulent devices in the system.

B. Operations

Consider users Alice ("A", the *receiver*) and Bob ("B", the *sender*) who wish to transact offline. If $i \in \{A, B\}$ is the user, let d_i denote the user's secure device (*i.e.,* the smart card), and w_i the wallet application installed on their phone.

1) Setup: During initial setup, user i undergoes a one-time KYC procedure with a designated institution (such as a government agency or an FI). After successful KYC verification of the user, the designated institution requests the certificate authority to create and sign the device's participation certificate c_i – thus, certifying that the device is authorized to participate in transactions inside the system. The certificate is

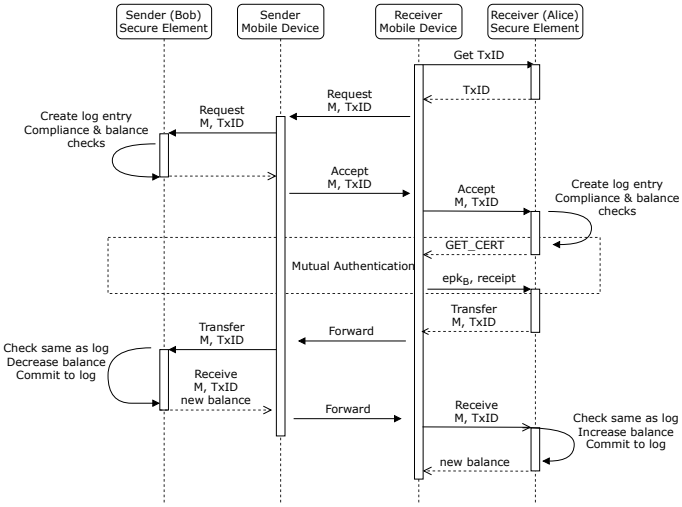

Fig. 1: The offline payment protocol

stored in d_i along with the authority's public key. Finally, the wallet application is also assigned its own separate certificate (created and signed by the certificate authority) which is used for authenticating itself to the secure device and other wallets.

2) Mutual authentication: The mutual authentication protocol [27], [28] is used as a subroutine by the other operations to establish a secure and authenticated communication channel that ensures message confidentiality and integrity, as well as to establish the legitimacy of the transacting parties. Mutual authentication consists of two phases: *certificate exchange* and *key establishment*. During the first, both parties authenticate to each other and verify that they are communicating with authorized devices within the jurisdictional "CBDC perimeter". This step also enables the SE to determine which operations of its API can be invoked by the counterparty. In the second phase, devices negotiate and derive a shared secret which is used to create session-specific symmetric cryptography keys that encrypt and verify all subsequent communication.

3) Withdraw & deposit: Users can withdraw funds from their account to their secure device or deposit funds from their secure device to their account. First, a secure session is established between the seucre device and the FI terminal, then the terminal sends the appropriate command (`<Withdraw>` or `<Deposit>`) to the secure device, which in turn verifies it, checks if regulatory constraints are satisfied (*e.g.,* balance/transaction limits), and modifies the balance accordingly.

4) Offline payment: The offline payment protocol between Alice and Bob depicted in Fig. 1 is divided into two stages: *payment initiation* and *value exchange*. During the first stage (`<Request>` and `<Accept>` commands), the two parties use their wallet applications to initialize the transaction identifier TxID, agree upon the payment amount $\mathcal{M}$ and roles (*i.e.*, who is the sender and who is the receiver), and authorize the transaction. In parallel, their secure devices check that: *(i)* the offline balance is sufficient; *(ii)* the requested amount does not exceed single-transaction limits; and *(iii)* cumulative transaction limits are not exceeded. If successful, pending transaction entries are created in the secure logs of both devices. During the second stage (`<Transfer>` and `<Receive>` commands), the funds move between the devices through appropriate balance and log updates. Specifically, they check that the payment details match the pending transaction log entry and will atomically: *(i)* update their balances and *(ii)* mark the transaction as completed in their logs.

5) Retransmission mechanism: To address potential communication interruptions that may lead to transaction failures and inconsistent state, the retransmission mechanism allows devices to repeat the last transaction. Specifically, if communication is lost after d_B decrements its balance but before d_A increments its own, then the retransmission protocol can used. The wallet application of Alice issues a `<Retransmit>` command to d_A, which checks if the command can be serviced. Then a new secure session is established and the value exchange phase is repeated, but without d_B reducing its balance.

6) Online synchronization: Intermittently offline systems keep track of the current state of the secure device by recording the offline balance in a separate ledger on the online CBDC system called the *offline ledger* [7]. Further, they can retrieve transaction metadata from secure devices that could be used to detect anomalies and potential instances of fraud [7]. As such, and depending on the compliance requirements of the system, some or all of the following actions take place before every withdraw or deposit operation: *(i)* the balance history of the device is shared with the offline ledger, *(ii)* the transaction log, locally stored in the device, is shared with the online system to enable more thorough compliance checks, and *(iii)* the risk parameters (*e.g.,* balance, turnover limits) on the card are reset and – if necessary – updated to new values.

C. Privacy preservation through ZKPs

In this section, we describe how ZKPs can be combined with Verifiable Credentials (VCs) [29] – secure and verifiable digital representations of documents attesting identity attributes (*e.g.,* IDs) – to enable the privacy features of the system.

1) Verifiable transactions: The offline payment protocol (see Sec. III-B4) can be extended by embedding conditions during the payment initiation phase through which the receiver can request a ZKP on an attribute of the sender (*e.g.,* age) as an extra condition to accept the payment. If the payer satisfies the condition(s), they append a ZKP to their `<Accept>` response.

The provided ZKP attests that the payer: *(i)* posses a valid VC signed by the certificate authority; *(ii)* has control over the public key included in the VC; and *(iii)* the VC contains an attribute whose value is above a threshold. We note that the proof is verified by w_A and not by d_A, since these kind of conditions are not directly related to the security of the payment system, and thus, not a concern to the SE. Therefore, the wallet's software can more flexibly accommodate changes in regulation or complex logic as compared to the applet running on the SE. Moreover, the corresponding VCs and cryptographic keys may not be directly accessible to the SE, as some regulated wallets require a separate secure device for managing the private keys corresponding to the VCs.

2) Anonymous withdrawals: The mutual authentication protocol with the FI during CBDC withdrawal can be modified to allow for privacy-preserving withdrawals, where the user exchanges physical cash for CBDCs at an FI terminal, similarly to previous CBDC proposals [30]. Specifically, the secure device does not provide its certificate – thereby protecting the user's identity – but instead it uses a ZKP generated by the wallet application, which attests to the following: *(i)* it possesses a valid VC signed by the certificate authority; *(ii)* it has control over the public key included in the VC by using

TABLE I: End-to-end latencies of the basic operations for variants $V.1$ and $V.2$

	V.1					V.2				
	Withdraw		Deposit		Payment (ms)	Withdraw		Deposit		Payment (ms)
Log size	Bal. (ms)	Trans. (ms)	Bal. (ms)	Trans. (ms)		Bal. (ms)	Trans. (ms)	Bal. (ms)	Trans. (ms)	
$n = 0$	2165		2114		4791	1738		1673		3949
$n = 1$	2488	2526	2528	2572	4813	2080	2105	2083	2114	3961
$n = 4$	2556	3007	2557	3014	4792	2123	2559	2135	2606	3954
$n = 10$	2612	3587	2637	3638	4788	2189	3195	2211	3186	3945

it to produce a signature on the cryptographic material used for producing the shared secret.

3) On the privacy and transparency conundrum: The proposed system allows the realization of different trade-off levels between privacy and transparency [15], [16]. Specifically, if the CBDC system has provisions for anonymous withdrawals and no transaction and balance tracking are required, then the prototype can ensure the anonymity of the user toward the FI. If balance reporting is enforced, a moderately private version is possible, in which the FI can obtain transaction amounts but cannot link multiple transactions to the same user. Finally, when both balance and transaction monitoring are implemented, the user has a low degree of privacy (in case of anonymous withdrawals) or no privacy at all.

IV. Prototype Evaluation

Implementation-wise, the prototype uses Elliptic Curve Cryptography with keys defined over the secp256r1 curve. AES-256 is used for session keys, with a key derivative function based on the ANSI X9.63 standard. SHA-256 is used for hashing, and certificates follow the format specified in [27]. Experiments use two ACOSJ 95K smart cards (Java Card 3.0.4, Global Platform 2.2.1) as secure devices and simulated user and FI terminals on a computer with an Intel i7-10750H processor and 32 GBs of RAM running Windows 11.

We consider three compliance cases. The first ("compliance-free") does not have any online synchronization constraints, while the second and third implement balance and transaction tracking, respectively. To further study the impact of the mutual authentication protocol on the performance of the system, we implement two variants of the prototype: *V.1* and *V.2*. The first executes the mutual authentication protocol as described in Sec. III-B2, whereas the second explores a trade-off between security and performance. Under this variant, the shared secret remains the same across sessions, while a nonce is used as a source of randomness to ensure unique session keys. Therefore, if the shared secret is compromised, forward secrecy may no longer be guaranteed [28].

Table I features an overview of the average latencies over five iterations for the main operations of the system for variants $V.1$ and $V.2$. We conduct experiments for varying values of n, where n is the number of transactions to be synchronized with the FI. We note that for $n = 0$, we effectively have the compliance-free case. We observe that $V.2$ mirrors $V.1$ in behavior but with lower latencies overall, owing to the reduced impact of the alternative mutual authentication scheme. Specifically, withdrawals and deposits exhibit similar latency trends, increasing with n, while payment latency remains constant at around 4.8 seconds for $V.1$ and 3.9 seconds for $V.2$, irrespective of n. Between the different types of compliance, transaction tracking is more expensive, reaching 3.6 seconds and 3.2 seconds, due to the larger amount of data to be synchronized. For both variants, payment latency remains comparable with modern payment systems.

TABLE II: Detailed latencies for the sub-operations of the protocols ($n = 10$)

		V.1		V.2	
	Operation	Bal. (ms)	Trans. (ms)	Bal. (ms)	Trans. (ms)
Withdr.	Mut. auth.	1652	1656	1231	1231
	Synch.	528	1192	526	1214
	Withdr.	300	296	302	300
Deposit	Mut. auth.	1690	1696	1245	1246
	Synch.	521	1516	533	1512
	Dep.	298	295	300	300
Offline trans.	Init.	495		492	
	Mut. auth.	3491		2626	
	Val. exch.	673		692	

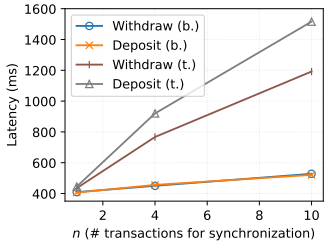

Fig. 2: Latency of the *synchronize* sub-operation for $V.1$ for various n

Table II lists the average latencies for the sub-operations of withdrawal, deposit, and payment for $n = 10$. Here, we observe that the most expensive operation is the establishment of a secure channel between the participants, reaching 3.5 seconds (72.9 % of the total latency) for payments under the $V.1$ variant. This indicates a clear bottleneck of the system and an avenue for future improvements. The next most expensive operation is the synchronization in the transaction tracking case taking as much as 1.5 seconds.

In Fig. 2, we examine the impact of n in the latency of the synchronize sub-operation for 1, 4, and 10 transactions under balance and transaction tracking for $V.1$. Latency increases with the number of transactions to be synchronized, and this increase is more prominent during transaction tracking.

V. Conclusion

As Central Banks look to redefine the very essence of cash with CBDCs, this paper presented a proof-of-concept implementation for offline digital currency transactions that balances the competing requirements between privacy and regulatory compliance. Its findings indicate that the proposed implementation safeguards payment integrity and that it is suitable for real-life daily use. Future work could include further strengthening the system against compromised devices and extending the performance evaluation.

REFERENCES

[1] T. Adrian and T. Mancini-Griffoli, "The Rise of Digital Money," Jul. 2019. [Online]. Available: https://www.imf.org/

[2] President of the United States, "Executive order 14178: Strengthening American leadership in digital financial technology," Federal Register, Vol. 90, No. 20, 31 January 2025, pp. 8647-8650. [Online]. Available: https://www.federalregister.gov/documents/2025/01/31/2025-02123/strengthening-american-leadership-in-digital-financial-technology

[3] A. Kosse and I. Mattei, "Making headway. Results of the 2022 BIS survey on central bank digital currencies and crypto," 2023. [Online]. Available: https://www.bis.org/publ/bppdf/bispap136.pdf

[4] Atlantic Council. Central bank digital currency tracker. [Online]. Available: https://www.atlanticcouncil.org/cbdctracker/

[5] "A proposal for a retail central bank digital currency (CBDC) architecture," Bank for International Settlements, Tech. Rep., Dec. 2024. [Online]. Available: https://www.bis.org/publ/othp89.htm

[6] "Central banks and distributed ledger technology: How are central banks exploring blockchain today?" World Economic Forum, Tech. Rep., Mar. 2019. [Online]. Available: https://www3.weforum.org/docs/WEF_Central_Bank_Activity_in_Blockchain_DLT.pdf

[7] "Project polaris: A handbook for offline payments with CBDC," Bank for International Settlements, Tech. Rep., May 2023. [Online]. Available: https://www.bis.org/publ/othp64.htm

[8] E. Androulaki, A. D. Caro, K. E. Khiyaoui, R. Gay, R. Mercer, and A. Sorniotti, "Secure and privacy-preserving CBDC offline payments using a secure element," Cryptology ePrint Archive, Paper 2024/1746, Oct. 2024. [Online]. Available: https://eprint.iacr.org/2024/1746/20241025:114406

[9] C. Beer, S. Zingg, K. Kostiainen, K. Wüst, V. Capkun, and S. Capkun, "Payoff: A regulated central bank digital currency with private offline payments," Aug. 2024.

[10] B. Bean, C. Minwalla, E. E. Tsiropoulou, and J. Plusquellic, "Puf-based digital money with propagation-of-provenance and offline transfers between two parties," *J. Emerg. Technol. Comput. Syst.*, vol. 20, no. 3, Aug. 2024. [Online]. Available: https://doi.org/10.1145/3663676

[11] M. Christodorescu, W. C. Gu, R. Kumaresan, M. Minaei, M. Ozdayi, B. Price, S. Raghuraman, M. Saad, C. Sheffield, M. Xu, and M. Zamani, "Towards a two-tier hierarchical infrastructure: An offline payment system for central bank digital currencies," Dec. 2020.

[12] B. Yang, Y. Zhang, and D. Tong, *DOT-M: A Dual Offline Transaction Scheme of Central Bank Digital Currency for Trusted Mobile Devices*. Springer Nature Switzerland, 2022, pp. 233–248.

[13] W. Jie, W. Qiu, A. S. Voundi Koe, J. Li, Y. Wang, Y. Wu, J. Li, and Z. Zheng, "A secure and flexible blockchain-based offline payment protocol," *IEEE Transactions on Computers*, vol. 73, no. 2, pp. 408–421, Feb. 2024.

[14] "Central bank digital currencies: foundational principles and core features," Bank for International Settlements, Tech. Rep., Oct. 2020. [Online]. Available: https://www.bis.org/publ/othp33.htm

[15] P. Michalopoulos, O. Olowookere, N. Pocher, J. Sedlmeir, A. Veneris, and P. Puri, "Privacy and compliance design options in offline central bank digital currencies," *IEEE Transactions on Network and Service Management*, pp. 1–1, 2025.

[16] N. Pocher and A. Veneris, "Privacy and transparency in CBDCs: A regulation-by-design AML/CFT scheme," *IEEE Transactions on Network and Service Management*, vol. 19, no. 2, pp. 1776–1788, 2022.

[17] J. D. Duffie, O. Olowookere, and A. Veneris, "A note on privacy and compliance for stablecoins," 2025. [Online]. Available: https://ssrn.com/abstract=5242230

[18] X. Xiong, M. Huth, and W. Knottenbelt, "REGKYC: Supporting privacy and compliance enforcement for KYC in blockchains," Cryptology ePrint Archive, Paper 2025/579, 2025. [Online]. Available: https://eprint.iacr.org/2025/579

[19] S. Allen, S. Čapkun, I. Eyal, G. Fanti, B. Ford, J. Grimmelmann, A. Juels, K. Kostiainen, S. Meiklejohn, A. Miller, E. Prasad, K. Wüst, and F. Zhang, "Design choices for central bank digital currency: Policy and technical considerations," National Bureau Of Economic Research, Tech. Rep., Aug. 2020.

[20] C. Barontini and H. Holden, "Proceeding with caution - a survey on central bank digital currency," Bank for International Settlements, Tech. Rep., Jan. 2019. [Online]. Available: https://papers.ssrn.com/abstract=3331590

[21] G. Fanti and N. Pocher, "Privacy in cross-border digital currency: A transatlantic perspective," in *Frankfurt Forum on European-US GeoEconomics*, 2022. [Online]. Available: https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Privacy_in_cross-border_digital_currency-_A_transatlantic_approach__-.pdf

[22] R. Auer, G. Cornelli, and J. Frost, "Rise of the central bank digital currencies: drivers, approaches and technologies," Aug. 2020. [Online]. Available: https://www.bis.org/publ/work880.pdf

[23] A. Carstens, "Digital Currencies and the Future Monetary System," *Hoover Institution Policy Seminar*, vol. 89, no. 1, p. 17, 2021. [Online]. Available: https://www.bis.org/speeches/sp210127.pdf

[24] V. Schlatt, J. Sedlmeir, S. Feulner, and N. Urbach, "Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity," *Information & Management*, vol. 59, 2022.

[25] Developers can soon offer in-app NFC transactions using the Secure Element. [Online]. Available: https://nr.apple.com/dN9S3v5Wt1

[26] OMAPI Vendor Stable Interface. [Online]. Available: https://source.android.com/docs/security/features/open-mobile-api

[27] "Secure channel protocol '11'," GlobalPlatform, Tech. Rep., Jul. 2018. [Online]. Available: https://globalplatform.org/wp-content/uploads/2017/09/GPC_2_3_F_SCP11_v1.2_PublicRelease.pdf

[28] E. Barker, L. Chen, A. Roginsky, A. Vassilev, and R. Davis, "Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography," National Institute of Standards and Technology, Tech. Rep., Apr. 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/nist.sp.800-56Ar3.pdf

[29] M. Sporny, D. Longley, and D. Chadwick. (2022, Mar.) Verifiable Credentials data model v1.1. W3C. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[30] J. Gross, J. Sedlmeir, M. Babel, A. Bechtel, and B. Schellinger, "Designing a central bank digital currency with support for cash-like privacy," 2021. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891121