

This is the final peer-reviewed accepted manuscript of:

*Compliance Design Options for Offline CBDCs: Balancing Privacy and AML/CFT*

**Conference Proceedings:** IEEE International Conference on Blockchain and Cryptocurrency (ICBC) 2024

**Author:** Panagiotis Michapoloulos, Odunayo Olowookere, Nadia Pocher, Johannes Sedlmeir, Andreas Veneris, Poonam Puri

**Publisher:** IEEE

The final published version will be available online at:

<https://doi.org/10.1109/ICBC59979.2024.10634398>

### Rights / License:


© 2024 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. For all terms of use and more information see the publisher's website:


[https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/author\\_version\\_faq.pdf](https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/author_version_faq.pdf)

*This item was downloaded from OrbiLu University of Luxembourg – <https://orbilu.uni.lu/>*

***When citing, please refer to the published version.***

# Compliance Design Options for Offline CBDCs: Balancing Privacy and AML/CFT<sup>\*\*</sup>

Panagiotis Michalopoulos<sup>\*</sup>, Odunayo Olowookere<sup>†</sup>, Nadia Pocher<sup>‡</sup> ,

Johannes Sedlmeir<sup>‡</sup> , Andreas Veneris<sup>\*§</sup>, Poonam Puri<sup>†</sup>

<sup>\*</sup> Department of Electrical and Computer Engineering, University of Toronto

p.michalopoulos@mail.utoronto.ca, veneris@eecg.toronto.edu

<sup>§</sup> Department of Computer Science, University of Toronto

<sup>†</sup> Osgoode Hall Law School, York University

odunayoolowookere@osgoode.yorku.ca, ppuri@osgoode.yorku.ca

<sup>‡</sup> Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg

nadia.pocher@uni.lu, johannes.sedlmeir@uni.lu

**Abstract**—Many central banks are researching and piloting digital versions of fiat money, specifically retail Central Bank Digital Currencies (CBDCs). Core to these systems’ design is the ability to perform transactions even without network connectivity. Due to the lack of direct involvement of third parties in these offline transfers, various regulatory requirements that are key in the financial space need to be accommodated. This paper deploys a compliance-by-design approach to evaluate technologies that can balance privacy with anti-money laundering and counter-terrorism financing (AML/CFT) measures. It classifies privacy design options and corresponding technical building blocks for offline CBDCs, along with their impact on AML/CFT measures, and outlines commonalities and differences between offline and online solutions. As such, it provides a conceptual framework for further techno-legal assessments and implementations.

**Index Terms**—Anonymity, central bank digital currencies, compliance by design, offline payments, privacy, secure hardware

## I. INTRODUCTION

Over the past years, more than 90% of central banks have started active investigations into digital versions of fiat money [1], [2]. This large-scale interest in retail central bank digital currencies (CBDCs) is driven by various factors, including the desire to (1) uphold the effectiveness of monetary policy while the use of cash decreases and interest in private money (e.g., stablecoins and other crypto-assets) continues to grow; (2) improve transaction efficiency and modernize central bank money; (3) ensure system resilience and accessibility; and (4) improve financial inclusion [3]–[6].

Amidst various design options central to current explorations, there is a growing focus on the potential for transferring CBDC funds independently of Internet connectivity [7], [8]. *Offline CBDC transactions*, colloquially known as *proximity payments* [9], ensure access to payment functionalities in the absence of a reliable network connection (e.g., in remote areas) or during broader system failures (e.g., caused by natural disasters) [3], [7]. Despite the ostensible benefits in terms of reliability and financial inclusion, offline functionalities pose challenges that add to the overall regulatory questions in the context of CBDCs. One particular tension emerges with regard to privacy. On the one hand, end users may expect offline transactions to provide a level of privacy similar to physical cash. Indeed, public polls indicate strong privacy guarantees to

be a desirable characteristic [6], [10]. On the other hand, such designs should not allow to circumvent anti-money laundering and counter-terrorism financing (AML/CFT) regulations or to facilitate tax evasion [11]–[14]. Hence, solutions must address the tension between end users’ privacy requirements and transparency and accountability measures required to deter illicit activities [10]. One effective approach is to move beyond merely identifying the regulatory impact of technology (or vice versa) and instead adopt *inherently* compliant solutions [15]. Leveraging the approach known as compliance-by-design [15], this paper focuses on the *privacy-transparency trade-offs* associated with offline CBDCs. We provide guidelines on how CBDC systems with offline functionality can reach set AML/CFT design goals by expanding on existing classifications of offline CBDC functionalities [7]. This paper additionally contributes the following:

- An analysis of the advantages and shortcomings of established and emerging technologies for balancing the privacy-transparency trade-off in offline CBDC payments.
- A classification of privacy design options for offline CBDCs, including potential interactions with online systems.
- An analysis of the impact of technical design choices on AML/CFT duties such as know your customer (KYC) and transaction monitoring, as well as of how said design choices align with the AML/CFT *risk-based approach*.

Our findings confirm that offline CBDC transactions with existing hardware and software technology solutions introduce additional degrees of flexibility to privacy-related designs that can even emulate the privacy features of physical cash.

In the remainder of this paper, Sec. II introduces CBDCs, the motivation for offline functionality, the technologies that can be leveraged to implement offline CBDCs, and our problem assumptions. Sec. III discusses offline CBDC transactions and the steps involved in the payment process. Sec. IV examines AML/CFT duties and the notion of compliance-by-design. Sec. V presents various design options for offline CBDCs and analyzes their privacy and AML/CFT impact. Sec. VI elaborates on limitations and on future cross-disciplinary research on the topic. Sec. VII concludes the paper.

## II. BACKGROUND

### A. Central Bank Digital Currencies

A core classification of CBDCs distinguishes between *wholesale* and *retail* systems. The former caters to financial

<sup>\*\*</sup>This paper will be presented at the 2024 IEEE International Conference on Blockchain and Cryptocurrency (ICBC). ©2024 IEEE

institutions and interbank transactions, while the latter delivers digital cash directly to the public. This work focuses on retail CBDCs that embody a novel form of central bank money. They are a liability of the central bank, denominated in an established unit of account and functioning as both a medium of exchange and a store of value [16]. Retail CBDC is a form of fiat money that can coexist with other forms of central bank money (e.g., physical cash, bank reserves), and with commercial bank and e-money [5], [12]. Retail CBDC systems can be *one-tier*, i.e., end-users interact directly with the central bank, or *two-tier*, i.e., intermediaries facilitate access to the CBDC also in terms of distribution [5], [11]. Most CBDC explorations and pilots focus on the second option.

Another common classification for CBDCs distinguishes between *token-based* and *account-based* structures [17], [18]. Tokens are representations of the currency units to be directly exchanged and may (but need not) involve custodians who hold tokens on behalf of end-users. Account-based systems are typically associated with some kind of identity verification and the notion of balances, thus requiring a third party for bookkeeping [19]. However, this classification is not unique (e.g., account updates can be represented as spending a token and receiving a new one [14]) and reportedly also falls short in covering the features of many potential CBDC designs [20].

### B. Motivations for the Offline Functionality

There is broad consensus on the significance of offline functionality in CBDC systems [21]. Representing a self-contained digital ecosystem, CBDCs are meant to stand as a modern counterpart to physical cash [22]. Evidently, central banks are actively exploring [23], [24] or piloting [8], [25] various designs. Offline CBDCs align with a myriad of system goals, heralding a paradigm shift in the realm of central banking objectives [7]. These goals include:

- *System resilience and accessibility*: Facilitating payments during connectivity or system disruptions, or in regions with communication infrastructure deficiencies.
- *Financial inclusion and accessibility*: Promoting access to financial services in underserved communities (e.g., the unbanked, individuals with no access to networking resources).
- *Lower transaction costs & enhanced scalability*: Reducing the load on online CBDC ledger systems, potentially increasing efficiency and cost savings. This is especially relevant for low-value and high-frequency transactions.
- *User privacy*: A level of privacy akin to physical cash. This becomes especially pertinent as the use of cash diminishes in favor of digital payments [7], [10]. The absence of a fully private digital alternative to cash raises concerns about the lack of access to *fully confidential transactions*.
- *User experience & trust*: Replicating features of cash to provide a familiar user experience and instill public confidence.

### C. Technical Building Blocks

In the following, we present hardware and software-based technologies that could be used to implement offline CBDCs. Notably, these can be combined to build a variety of solutions that we cannot cover in this paper due to space limitations.

1) *Secure Elements (SEs)*: SEs are tamper-resistant platforms commonly found in smart cards (e.g., chip-and-PIN or signature bank cards, mobile phone SIM cards, biometric passports) [26], but also as stand-alone chips in some phones [27]. They comprise a secure microprocessor resistant to both

software and physical attacks accompanied by small amounts (i.e., hundreds of KBs) of RAM and persistent memory in the form of electrically erasable programmable read-only memory (EEPROM) or, more recently, flash memory [28]. SEs are capable of hosting different applications whose relative isolation is guaranteed by the underlying secure operating system, with popular examples being JavaCard and MULTOS [29].

SEs can provide the highest levels of integrity and confidentiality and they are frequently certified against the Common Criteria EAL and FIPS 140-2 [30] specifications for use in environments with particularly high security requirements. Further, they can be provisioned ensuring that applications and data are installed in the SE during manufacturing time in a secure way, preventing tampering attempts [31]. However, due to the general need to reduce the possible attack surface (i.e., a system's components that can be used by an attacker [32]), SEs usually remain low on computational capabilities [28] and offer only highly restricted functionalities (e.g., only selected cryptographic operations and limited secure storage).

2) *Trusted Execution Environments (TEEs)*: TEEs are secure areas of a microprocessor that offer increased integrity and confidentiality of the code executed and data stored or processed in them [33]. More specifically, a TEE is implemented through the synergy of hardware and software components of the processor that isolate and protect it from the rest of the unsecured machine and the untrusted operating system running on it [34], [35]. As TEEs are part of a larger general-purpose processor, they have a wider range of computational capabilities when compared to SEs. In particular, they are able to flexibly execute arbitrary programs, named trusted applications (TAs), with low performance overhead [35]. Further, their ability for remote attestation, through which they can demonstrate that the code being executed was untampered [36], makes them compelling solutions for applications with increased security requirements, such as mobile payments. TEEs offer some valuable features which SEs do not support, for instance, network connectivity and time-keeping capabilities [37]. Moreover, TEEs can have dedicated access to peripherals (e.g., sensors), ensuring the integrity of the exchanged information [38].

On the other hand, TEEs suffer from a wide range of vulnerabilities [39], [40]. These can be software-based, architectural, and hardware-based, with the latter encompassing what is known as side-channel attacks. The first category exploits implementation flaws in the software running on the unsecured or trusted environment; the second takes advantage of design flaws in the TEE architecture; and the last category manipulates hardware components of the platform, such as caches. To address these problems, one can design hybrid secure applications where an SE is reserved for the most security-critical operations and the TEE assumes a supportive role for more complex and less critical data and computations.

3) *Zero-Knowledge Proofs (ZKPs)*: ZKPs are defined as those proofs that reveal nothing beyond the correctness of the proposition in question [41]. ZKPs allow a prover to demonstrate that they executed a public algorithm on a private input (which is only accessible to the prover and not shared with the verifier) with a public output (result) [33]. Thus, they provide, similarly to TEEs but by software-based means, *computational integrity* for arbitrary programs and *confidentiality* of the private input with respect to the verifier [33], [41]. However, unlike SEs and TEEs, ZKPs do not provide *confidentiality* and toward the prover, i.e., the prover can access all the data

underlying the corresponding computation.

Advantages of ZKPs include their independence from any underlying secure hardware, and, thus, from the corresponding manufacturers (as compared to SEs and TEEs), with their security guarantees being derived from cryptographic primitives. On the other hand, ZKPs suffer from complexity. For instance, common bug patterns [42] and side-channel attacks have been reported on ZKPs [43]. Further, as opposed to TEEs, general-purpose ZKPs involve a significant prover overhead, although continuous improvements are being made in this front [14]. Many of these ZKP implementations also require a “trusted setup” that relies on at least one honest party for integrity guarantees, yet, there are also variants that do not [33], [44].

#### D. Balancing Compliance Requirements

If CBDCs are intended to mirror the user experience of coins and banknotes, the system should include accessibility options that differ from the management of a traditional bank account [11]. The privacy of payment systems is also consistently ranked as a top priority for citizens in public surveys [10]. Therefore, the design goal of providing offline functionalities is intertwined with that of offering end-users a level of privacy similar to that of physical cash [45]. However, the inherent anonymity of cash and other bearer instruments (e.g., anonymous e-money), notoriously impacts financial integrity and crime [46]. In particular, this anonymity hinders the identifiability of payer and payee and the traceability of the associated flows, e.g., by means of graph analyses [47]. This challenge led to compliance standards and restrictions for transactions involving cash [48]. These restrictions can consist of limits on the purchase of specific types of goods or services, cross-border transfers, and the denomination of banknotes, as well as daily or monthly turnover limitations for individuals.

The effectiveness of these restrictions may diminish if CBDCs eliminate some physical limitations of cash. For instance, malicious entities may abuse the fact that digital proofs of proximity are difficult to implement [49], [50], and disguise a remote payment as a proximity payment to benefit from potentially less strict compliance rules for offline transactions. Consequently, offline CBDCs striving to replicate the anonymity of cash while surmounting its physical limitations may raise concerns similar to the online setting, thus necessitating some restrictions. Hence, an adequate design of usage controls and end-user privacy is vital, implying a fundamental *trade-off* between access to the means of payment and accountability. As outlined in Sec. IV, this trade-off has to be considered with particular care for offline functionalities.

#### E. Underlying Assumptions

This paper makes the following assumptions:

- 1) It strictly considers retail CBDCs where offline payments have emerged as particularly relevant for the domain;
- 2) Its AML/CFT analysis is based on the Recommendations of the Financial Action Task Force (FATF) [48]. Besides those international standards, it remains jurisdiction-agnostic;
- 3) It assumes that the offline CBDC design safeguards foundational security requirements, such as no double-spending, unforgeability, and non-repudiation [13], [24];
- 4) It neither addresses the issues of scalability [51] and interoperability [52] of offline CBDC systems nor does it consider applications of homomorphic encryption [53];

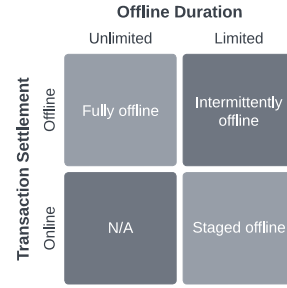


Fig. 1. Different types of offline CBDC transactions

- 5) It scrutinizes privacy measures from end users’ perspective, and transparency measures from the regulator’s perspective.

### III. OFFLINE CBDC TRANSACTIONS

The definition of ‘offline’ payment turns out to be quite nuanced. At its core, it denotes payments made in the absence of a connection to an online ledger. However, this definition undergoes refinement when exploring various models of offline transactions. While some define an offline transaction as one where participants lack any network access, others narrow the criteria to transactions that necessitate access to telecom servers (but not the Internet). Additional constraints (e.g., no access to external power sources) can be introduced [8].

#### A. BIS Classification of Offline CBDC Transactions

The Bank for International Settlements (BIS) delineates three categories of offline CBDC transactions [7], which we also adopt in this paper. Fig. 1 offers an overview of their key characteristics, with detailed descriptions as set out below:

- *Fully offline*: This system enables payments without the need for a direct ledger connection, ensuring instant offline value exchange between purses and transaction settlement, with no temporal restrictions on staying offline for both parties. That is, the payee can immediately spend the received funds.
- *Intermittently offline*: This setup allows the payer and payee to complete only a limited set of payments fully offline. Similarly to ‘fully offline’, transactions are settled offline and received funds can be spent. However, risk parameters will eventually limit further transactions, requiring occasional synchronization of end-users’ wallets with the central online system for continued functionality. The online system makes use of an additional ledger to keep track of the users’ offline balances or transaction logs.
- *Staged offline*: Here, the payer and payee do not need to connect to a ledger system for value exchange between purses to occur, but the payee cannot spend the transferred value until they connect to an additional online ledger (similarly to ‘intermittently offline’) for online settlement.

#### B. Offline CBDC Transactions and User Onboarding

Offline CBDC functionality could depart significantly from existing offline payment methods like payment cards equipped with Europay, Mastercard, and Visa (EMV) chips and magnetic stripe technology. This departure is rooted in the operational dynamics of offline CBDC payments: In contrast to payment cards featuring EMV chips, which operate by verifying end-user credentials to connect them with third-party banking services, offline CBDC payments can provide

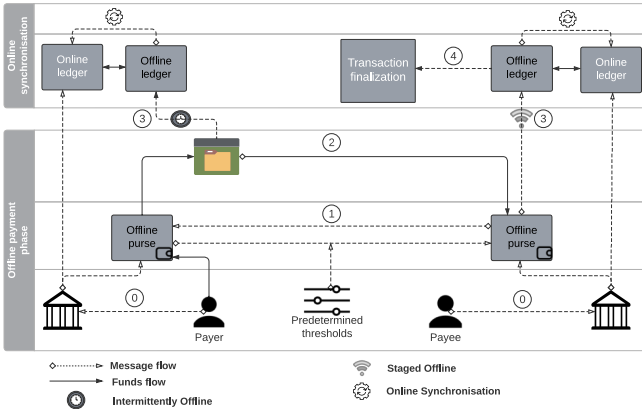


Fig. 2. Offline CBDC payment cycle

a more versatile and self-reliant approach [22]. The primary distinction emerges from the potential for offline CBDCs to mimic existing payment card systems or establish a self-reliant ecosystem equipped with technologies that facilitate offline transactions and enable users to manage their accounts [22].

We now examine the various phases of the offline CBDC payment process and gain an initial understanding of their operation (see Fig. 2). Before CBDC transactions can be conducted, users go through step ①, where *user onboarding* takes place. The foundation of any payment or electronic funds transfer system often involves an onboarding process, which includes tasks like user registration, KYC, and other identity validation methods. A comprehensive KYC process is key in the context of AML/CFT compliance. Within a CBDC ecosystem that imposes limits (e.g., balances, turnover, etc.), the aim is to ensure authenticity and to make sure users cannot enroll multiple times [14]. In Sec. V, we further discuss how a strong device binding established through the KYC may be key to achieving a plausible implementation of a high-privacy option also for offline CBDCs. The following offline CBDC payment process comprises the two phases of ‘offline payment’ and ‘online synchronization’ [7].

### C. The Offline Payment Phase

This phase consists of the following two stages:

1) *Transaction initiation and confirmation:* It takes place during step ①, which begins with the users initiating an ‘eligible’ transaction via their certified devices, assigning appropriate roles to devices (payer/payee), and authorizing the transaction. Concurrently, a strict identity verification process (including user authentication and mutual device verification) builds the foundation of the overall reliability and integrity of the offline CBDC payment system. It is achieved through a secure communication protocol involving the following steps: (1) Each user proves control of their device by providing a PIN or biometrics as a protection against device theft or unauthorized use. (2) The devices prove to each other through the use of digital certificates that they originate from trusted manufacturers and/or have been authorized to participate in the offline CBDC system. (3) The devices prove that the software they run can be trusted and has not been tampered with.

To execute the authentication protocol, devices can be provisioned with a cryptographic keypair for signing messages and proving ownership of their certificates. The public key

can also function as a pseudonymous identifier for the device; however, in settings that maximize privacy, many devices may obtain the same keypair from the manufacturer [54]. Further, a participation certificate signed by the central bank of a regulatory authority may be necessary. Verification of such certificates requires that devices are pre-loaded with a list of appropriate certificate authorities (CAs) or a minimal PKI from which such lists can be fetched or updated.

2) *Offline transaction settlement:* Once these steps are successfully completed, trust between the devices has been established and the transaction process can continue with executing the value exchange protocol. During step ②, devices agree on the amount to be transferred and ensure the atomicity of the transaction. For instance, both devices’ local balances may be updated, or the payer’s wallet may send unique serial numbers corresponding to coins to the payee and delete them subsequently. Offline value exchange from the payer to the payee occurs after user confirmation and successful mutual authentication. Finally, key transaction details, including sender and recipient information (e.g., device identifiers), transaction amounts, timestamps, and metadata, are recorded in the local storage of the user’s device. For instance, SEs can be used to store the funds, identity information of the user, and transaction details. In parallel, they can enforce basic AML/CFT rules based on pre-loaded risk parameters.

### D. The Online Synchronization Phase

1) *Offline-online data synchronisation:* At step ③, when users regain network connectivity, the data stored in the device’s local storage, such as the purse’s current balance and transaction logs, are synchronized with the offline ledger. This procedure may involve some proof of ownership of the corresponding (KYCed) online ledger account. At the same time, maintenance tasks (e.g., system updates, risk parameter updates, reconciliation between ledgers) can be carried out.

2) *Transaction finalization:* Step ④ occurs only for the staged offline case. Transactions are settled online and the corresponding funds become available to the payee to be spent either online or offline. Additionally, data may be exchanged between the online and offline ledger, in accordance with the transaction’s specific needs. These may be subject to additional verification processes to increase trust in offline transactions (e.g., redemption of a coin on an unspent online list, similar to some payer-anonymous e-cash transactions [13]).

## IV. COMPLIANCE BY DESIGN AND AML/CFT

### A. AML/CFT Framework and CBDC Systems

AML/CFT laws, regulations, and procedures protect financial integrity by preventing criminals from concealing the origin of illicit funds. To this end, the framework imposes duties on actors known as regulated entities, which include financial institutions, professionals (e.g., lawyers and notaries), real estate agents, and crypto-asset service providers, among others. The FATF coordinates the international efforts in its standard-setter capacity [48], and the EU is currently strengthening the regime through a major reform [55]. AML/CFT measures are both preventive and repressive, and duties imposed on regulated entities encompass licensing, customer due diligence (CDD) including KYC (i.e., the identification of customers and the verification of their identity, including checks of personal and business information according to given criteria), ongoing monitoring (e.g., transaction monitoring and screening), and



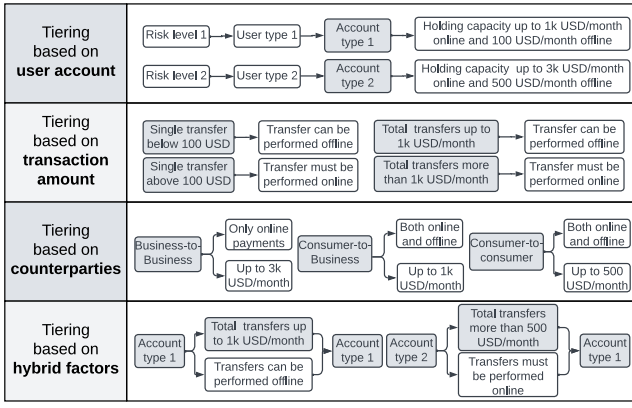


Fig. 3. Types of accounts and transaction tiering and examples

record retention [56]. Most of these obligations are informed by the *risk-based approach*: the entity must identify, verify, and understand the specific risks to which it is exposed and take proportionate mitigating measures [48]. The final objective is to inform the authorities of any suspicion of illicit deeds by filing a suspicious transaction report.

The AML/CFT dimension is at the core of CBDC experiments. Monitoring and limiting the use of physical cash are widespread means to combat money laundering, terrorist financing, and tax evasion [15]. In the CBDC space, the goal is to avoid threats to the existing safeguards and establish AML/CFT competencies in multi-stakeholder systems. Within a two-tier structure with distributors in charge of end-user relationships and compliance checks (similar to commercial banks and e-money institutions today), the role of distributors is a major design choice [57] because it relates to giving access to payment data not only to regulatory and supervisory bodies but also to private actors (as with commercial bank money and e-money today). The risk is amplified by the foreseen potential of CBDCs to intrude into the private lives of individuals [58], [59]—e.g., payment history datasets generated by commercial payments platforms [15], [60].

### B. Compliance-by-Design and Tiered CBDC Options

To be compliant means achieving and demonstrating conformity with given regulatory constraints, such as laws, regulations, and standards [61]. While certain checks are increasingly automated to reduce costs and improve accuracy [47], compliance itself is a granular concept that is not fully translatable into binary requirements [61]. Specific aspects can, however, be streamlined into the technology design process. This proactive approach first emerged with privacy-by-design [62] and evolved into compliance-by-design, where compliance is embeddable into technology [63]. When technology design is leveraged for compliance purposes, it requires preliminary engineering and standard setting [15]. The complexity of compliance standards could influence technology solutions. For instance, integrating sanctions checks may be simpler than embedding AML/CFT checks: sanctions compliance, operating within a rules-based system for individual transactions, involves compiling lists and ensuring that the technology adopts and applies sanctions restrictions [64]. In contrast, AML/CFT compliance operates within a risk-based system, navigating nuanced scenarios affecting collections of transac-

tions, defining risk parameters, and balancing diverse regulatory requirements (e.g., privacy-transparency trade-offs) [11].

CBDC investigations must balance diverse regulatory requirements. Concerning privacy and transparency, CBDCs can be designed to accommodate multiple options [14], [57]. Most CBDC projects offer both some degree of privacy for end-users and some transparency to authorities by means of a composite system [15]. The integration of different trade-offs within the same system can rely on ‘access tiering’, which means the features offered by the CBDC system can vary depending on the attributes of a given account or transaction [65]. This can be done for a variety of purposes, such as privacy, security, financial inclusion, and an AML/CFT risk-based approach. Tiering can be based on the user account (e.g., between two less risky accounts as per a level of CDD), transaction amount thresholds (e.g., transfers can be facilitated below a certain amount), counter-party types (e.g., business-to-business, business-to-consumer, and consumer-to-consumer), and other hybrid factors (e.g., total turnover transacted between two accounts in a certain time window exceeds a certain amount) [65]. Managing these trade-offs gives rise to a spectrum of design options. In this work, we focus on classifying those related to offline CBDCs. Any movement of a specific solution along the spectrum is based on tiering offline transactions, by imposing various limits including on the amounts, frequency, or transaction types for offline transfers. Accordingly, a lower tier set of transactions of only small monetary value—albeit not as small as to disrupt usability—may be compatible with the offline option while a higher tier, such as transfers of significant value, may require online capabilities. In Fig. 3, we depict possible examples of transaction tiering in the context of offline capabilities.

### C. AML/CFT Design Choices for an Offline CBDC System

Three overarching CBDC design angles highlighted in [57] exert a considerable impact on AML/CFT compliance: *user access* (identity management), *daily end-user experience* (wallet and account management), and *CBDC distribution* (system management). In terms of access, identity-related information can be managed in different ways, and the stakeholders may be granted various levels of visibility into end-user information. This gives rise to a spectrum, ranging from a high level of privacy for all transactions with respect to any stakeholder, crossing the visibility of selected data for selected transactions to selected stakeholders, up to a high degree of transparency of all transactions with respect to any stakeholder [57]. Often, offline functionality represents a way to offer end-users a certain degree of capability to exchange money privately in a way that resembles their experience with physical cash [65].

Before moving to identify the AML/CFT specifics of various technical options for offline functionality, we list below the AML/CFT elements that inform the CBDC offline payment cycle. In particular, the system will define whether:

- to transact offline, end-users need to undergo KYC;
- the offline functionality is part of a broader CBDC system that includes online capabilities;
- offline transactions are associated with end-user identity;
- offline transactions are considered in addition to online ones for AML/CFT purposes/thresholds;
- offline transactions are stored or there is any other form of record-keeping of corresponding compliance material;

- there are limits imposed to the capability to transact offline and, if so, which ones—e.g., thresholds on transaction amount, turnover, balance;
- there is automated or manual monitoring for transactions performed offline and, if so, which one—e.g., transaction tracking, graph analysis;
- there is transaction screening—i.e., an opportunity to screen transactions in real-time before approval and to block them when identified as risky or illicit;
- it is possible to blacklist payers and/or payees; and,
- it is possible to tailor the offline functionality to individual customers or groups thereof—e.g., counterparty tiering.

These AML/CFT capabilities of an offline CBDC can be supported by various hardware and software technology options, but not by all of them. As described in Sec.V, different models can uphold the robustness of the AML/CFT safeguards while diminishing end-user privacy, albeit this is often more nuanced. For instance, although an initial KYC and strong identity binding are foreseen by many models, ZKPs can prevent the association of certain transactions (e.g., below a given threshold) with the end-user identity [14].

#### V. A SPECTRUM OF OFFLINE PRIVACY OPTIONS

In this section, we outline different models of offline CBDC functionality, ranging from the solutions that provide the highest level of privacy to those that provide the highest degree of transparency. As the operator of the online ledger can control read permissions for stakeholders, we will exclusively focus on privacy with respect to this stakeholder, i.e., which data provided by the end-user is directly accessible to the online ledger [19]. For each model, we describe a potential technology stack and elaborate on repercussions in terms of the key AML/CFT dimensions for offline functionalities (as outlined in Sec. IV). Fig. 4 features a summary of our findings.

##### A. Fully Offline with no KYC

The first model into consideration is a fully offline solution (i.e., independent of an online ledger) that does not require users to have an account with financial institutions. Arguably, this solution supports the highest level of privacy, with the objective of emulating the privacy standards akin to physical cash. These solutions can be enabled by technologies such as payment cards equipped with SEs. In case ‘indistinguishable’ SEs are used (i.e., batches of cards that carry the same keypairs for chip authentication [54]), end-user anonymity can be provided even with respect to the transacting counterparty. In our analysis, we consider this highest privacy level as a hypothetical construct. The model acts as a yardstick against which other privacy-centric concepts and solutions should be assessed, rather than being intended for immediate adoption or practical implementation by central banks.

Unsurprisingly, this technological scenario offers minimal capabilities in terms of compliance (see Fig. 4). While the proposed payment instrument can be subject to scarce oversight during usage by end-users who are not identified, it also cannot support the majority of compliance checks. Regulation could treat these instruments like today’s existing anonymous gift/prepaid cards or vouchers, which are known to pose a challenge to AML/CFT compliance [66]. Hence, they would be subject to strict limits in terms of balance and turnover capacity or reloadability. For instance, in the EU, AML/CFT measures are particularly strict with limiting functionalities of

		Fully Offline No KYC	Fully Offline with KYC	Intermittently Offline I	Intermittently Offline II	Staged Offline
AML/CFT	Thresholds	✓	✓	✓	✓	✓
	KYC	×	✓	✓	✓	✓
	Balance tracking	×	×	✓	✓	✓
	Transaction tracking	×	×	×	✓	✓
	Transaction screening	×	×	×	×	✓
Technologies	SE	✓	✓	✓	×	×
	TEE	×	✓	✓	✓	✓
	ZKP	×	✓	✓	/	/

Fig. 4. Offline design models for privacy and AML/CFT compliance

anonymous prepaid/gift cards: they must not be reloadable and are subject to balance (and, therefore, also transaction) limits of 150 € per month [67]. In the context of offline CBDCs, such types of restrictions can be enforced by the SEs.

##### B. Fully Offline with KYC

In this second case, we consider a fully offline solution that can operate independently of an online ledger and where the involved devices (typically, two mobile phones) are associated with their corresponding user’s identity through an initial KYC. Users could top up their balance to be spent offline using an online account or anonymously at an ATM, similar to previous proposals for online CBDCs with cash-like privacy features [14]. In contrast to the previous hypothetical model, this design is of more practical application. A characteristic of this design model, which differentiates it from the following ones, is that there is no mandatory synchronization with the online ledger, which here is being used only as a mechanism for depositing funds to the offline purse.

This model can be implemented with SEs or TEEs, since both technologies support threshold-based compliance mechanisms. SEs can effectively enforce counter-based thresholds (e.g., transaction limits or cumulative expenditure). TEEs enable more complex, temporal thresholds, albeit with some complexities in implementation. Furthermore, both SEs and TEEs offer the capacity for ‘over-the-air’ updates [68] for outdated risk parameters. Therefore, TEEs seem to not confer a significant advantage at this level. If the online ledger is ‘transparent’ and does not employ any privacy-enhancing technologies, it offers privacy assurances comparable to a prepaid card in combination with a bank account, and the AML/CFT treatment can also be foreseen as similar. On the other hand, if the online ledger provides high privacy guarantees, such as TEEs or ZKPs to construct proofs as in [14], and topping up is done anonymously at an ATM, it offers the highest privacy assurances.

At the offline level, compliance measures can remain minimal and limited to predefined balance and turnover thresholds. Leveraging the KYC process, turnover thresholds can now be enforced on a per-individual basis, rather than on a per-device basis. In this context, *all-or-nothing non-transferability* plays an essential role [14], particularly when the online ledger is not

transparent: if it is easy for illicit actors to get access to many individuals' devices for offline payments (e.g., by means of theft, blackmailing, or bribing), they can circumvent balance and turnover limits and, hence, render AML/CFT measures ineffective. While the need to get access to a device and the PIN to unlock it already makes theft more difficult, it can be argued that this alone may not deter active sharing. This is especially true when considering the existence of numerous alternative means of payment that will not be abolished with the adoption of a CBDC. One natural way of increasing the barrier to sharing devices and access credentials is the connection to a strongly bound national identity, as foreseen, for instance, through the EU digital identity wallet [14], [69]. This form of identification and authentication inhibits sharing, heightening both the drawbacks of passing the device and the accountability risks for actions associated with this identity [14]. To mitigate such risks, verification of access to a corresponding digital identity in offline payments (via SEs or TEEs) can be implemented, potentially coupled with occasional revocation checks via synchronized revocation lists.

#### C. Hybrid: Intermittently Offline and High Privacy

As outlined in Sec. III, this model ('Intermittently Offline I' in Fig. 4) for offline CBDC transactions necessitates periodic synchronization with the online CBDC ledger to ensure continued functionality. In this context, in addition to the KYC process and the threshold-based mechanisms described above, we anticipate the potential inclusion of *balance tracking* as an additional AML/CFT feature. This feature would enable the online ledger to access the balance of the purse at specific points in time. To safeguard end-user privacy, balance tracking could be done in a privacy-preserving manner, i.e., certain limits would be enforced through TEEs or ZKPs. Similar to the previous two designs, compliance measures could also be established through counter-based mechanisms, leveraging SEs or TEEs. These checks could be expanded by time-based mandatory synchronization enforcements with TEEs.

#### D. Hybrid: Intermittently Offline and Lower Privacy

At a lower privacy level, we consider an intermittently offline solution equipped with stricter thresholds, more frequent synchronization requirements, and enhanced capabilities to monitor offline payments. Beyond balance tracking, the online ledger receives information about actual transactions, including timestamps and transacting parties, through *transaction tracking*. While privacy-preserving disclosure is feasible for balances, this may not be viable for transaction details, especially if they are intended for online computations like transaction graph analyses. Since the online system requires access to the original data for such computations, solutions such as ZKPs may not be helpful. Regarding the technology stack that can be leveraged in this scenario, we note that transaction monitoring requires a substantial amount of storage on the offline CBDC-enabled device. It follows that, due to the limited storage capacity of SEs and the enhanced computational and storage capabilities of TEEs, TEEs may emerge as a more apt solution.

#### E. Hybrid: Staged Offline

A staged offline approach, where received funds remain unusable until synchronization, provides the opportunity to conduct online AML/CFT checks before the settlement of a

transaction (e.g., transaction screening). A transaction flagging mechanism could potentially be set in place for the cases where unusual behaviour is observed by the system. The transaction would be logged in the online system and flagged for further inspection. In case a regulatory offence is detected, transactions could be reversed, where the online account of the payer is debited with the reversed amount and the payee's offline device is instructed to forfeit the funds. At the same time, all the compliance measures from previous models are also available, leading to a layered approach favoring transparency and more sophisticated AML/CFT measures. Here, the usage of ZKPs can help reduce the amount of information that needs to be disclosed. Much like in the previous design model, TEEs also emerge as a suitable alternative choice.

### VI. LIMITATIONS AND OPEN QUESTIONS

From our analysis of the privacy and AML/CFT impact of different models supporting offline functionality in CBDC systems, we pinpointed several open issues as avenues for future work. Concurrently, we identify limitations to the approach and methodology deployed in this paper. As our research suggests a strong interconnection between these limitations and open issues, we outline both aspects below.

First, we conduct our research at a point in time where there is *no real-life functioning offline CBDC payment framework*. Unlike investigations into online payment systems, the absence of a standardized model requires speculation, underscoring the nascent nature of offline CBDCs. Although some jurisdictions have started pilot stages for the offline component of their respective CBDC projects, these initiatives remain incomplete, thus constraining the depth of our analysis. Further implementation and evaluation of the proposed design options remain intriguing open issues for future work.

Second, in this paper, the analysis remains *jurisdiction agnostic*, prioritizing overarching regulatory principles over jurisdiction-specific AML/CFT rules. While acknowledging this limitation, we recognize the importance of a nuanced approach considering factors like specifics of the FATF Recommendations, jurisdictional peculiarities of criminal justice systems, commercial dispute resolution mechanisms, and domestic policies on illicit financial activities. Relying on FATF's Recommendations ensures alignment with globally recognized principles, forming a realistic foundation for the analysis. Yet, a jurisdiction-specific focus is essential for a comprehensive design that ensures compliance while preserving privacy. Alternatively, one could focus on the cross-border dimension and additional challenges posed by regulatory divergences [12].

Third, the *dynamic and fragmented regulatory fields* relevant to our field of research are constantly in flux. This condition introduces complexities, particularly concerning privacy considerations with offline CBDCs. The evolving landscape of these regulations across jurisdictions poses challenges in predicting the precise impact on privacy within the context of offline CBDCs. The intricate interplay between privacy, digital identity laws, data protection laws, AML/CFT standards, and the unique attributes of CBDCs necessitates ongoing scrutiny.

Fourth, the regulatory repercussions of offline functionality of CBDC systems go far *beyond the AML/CFT dimension*. By focusing on the interrelation between privacy and AML/CFT considerations, we intentionally left out a thorough exploration of broader repercussions, such as implications to monetary



policy and central bank law [11]. In addition, specific frameworks tied to financial sanctions, such as those outlined by the Office of Foreign Assets Control (OFAC) but also the different financial restrictive measures imposed by the EU, introduce an added layer of complexity. While our paper provides insights into AML/CFT implications and a brief mention of sanctions, a more expansive analysis is needed to comprehensively address the diverse range of sanctions-related frameworks impacting offline CBDCs.

Fifth, the regulatory strategy of introducing limits on the amounts, frequency, or transaction types is still positioned within the risk-based AML/CFT framework. As standalone solutions, thresholds may not be able to provide the flexibility needed to fully mirror an inherently principle-based framework. Considering the regular deployment of this approach for cash transfers and prepaid cards, we consider this element as an open issue rather than a limitation of our study.

Lastly, this work does not consider the effects of further cryptographic primitives (e.g., homomorphic encryption) to complement the presented technologies. Such primitives can allow performing checks by the ledger operators while preserving the confidentiality of the underlying data. It also just touches the surface of the important issue of *data protection* in offline CBDC payment transactions. These topics constitute additional avenues for future techno-legal research.

## VII. CONCLUSION

Similarly to the challenges faced when designing privacy-focused online retail CBDCs, the increasing focus on supporting offline functionalities requires balancing various financial regulatory requirements. In this paper, we adopt a compliance-by-design approach, evaluating a set of hardware and software technologies for balancing privacy compliance. Specifically, we provide a classification of privacy design options and corresponding technical building blocks for offline CBDCs.

Our findings reveal that supporting offline transactions introduces additional degrees of freedom to the privacy design options of CBDCs. A fully offline CBDC appears to maximize privacy but compromises transaction monitoring and other essential risk management approaches. On the other hand, different flavors of online CBDCs with support for offline transactions essentially offer the same spectrum of privacy as fully online solutions, from full transparency to cash-like privacy. A full transaction graph analysis with the techniques we consider is only possible with high degrees of transparency that includes detailed reporting of offline payments to the online ledger in synchronization phases. However, using TEEs or ZKPs on the online layer in combination with the reporting of selected transaction data from offline transactions enables a substantial set of risk mitigation measures without compromising privacy. As such, we believe that this work serves as a valuable resource for CBDC system architects, delineating commonalities and differences between offline and privacy-focused online solutions. Additionally, it establishes a conceptual framework for techno-legal assessments and implementations in the evolving landscape of CBDCs as central banks explore the redefinition of the very essence of cash.

## ACKNOWLEDGMENTS

The authors acknowledge various comments and insights by Cyrus Minwalla (Bank of Canada), Yaya Fanusie (Center for a New American Security and former CIA counterterrorism

analyst), and the anonymous reviewers that helped improve the content and presentation of this work.

The contributions of Nadia Pocher and Johannes Sedlmeir were funded by the Luxembourg National Research Fund (FNR), grant reference NCER22/IS/16570468/NCER-FT (CryptoReg) and grant reference 16326754 (PABLO), as well as by PayPal-FNR, PEARL grant reference 13342933/Gilbert Fridgen. For the purpose of open access, and in fulfillment of the obligations arising from the grant agreements, the authors have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

## REFERENCES

- [1] 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>
- [2] Atlantic Council. Central bank digital currency tracker. [Online]. Available: <https://www.atlanticcouncil.org/cbdctracker/>
- [3] Bank for International Settlements, "Central bank digital currencies: foundational principles and core features," 2020. [Online]. Available: <https://www.bis.org/publ/othp33.htm>
- [4] Bank of Canada, "Contingency planning for a central bank digital currency," 2020. [Online]. Available: <https://www.bankofcanada.ca/2020/02/contingency-planning-central-bank-digital-currency/>
- [5] S. Allen, S. Capkun, I. Eyal, G. Fanti, B. Ford, J. Grimmelmann, A. Juels, K. Kostiaainen, S. John, A. Miller, E. Prasad, K. Wüst, and F. Zhang, "Design choices for central bank digital currency: Policy and technical considerations," 2020. [Online]. Available: <https://www.nber.org/papers/w27634>
- [6] Bank of Canada, "A Digital Canadian Dollar: What we heard 2020–23 and what comes next," 2023. [Online]. Available: <https://www.bankofcanada.ca/digitaldollar/a-digital-canadian-dollar-what-we-heard-2020-23-and-what-comes-next/>
- [7] Bank for International Settlements, "Project Polaris: Handbook for offline payments with CBDC," 2023. [Online]. Available: <https://www.bis.org/publ/othp64.htm>
- [8] B. Brodsky, A. Dubey, and D. Tercero Lucas, "Enabling offline payments in an online world. A practical guide to offline payment design," 2023. [Online]. Available: <https://www.lipisadvisors.com/whitepapers>
- [9] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro," 2023. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0369>
- [10] S. Choi, B. Kim, Y.-S. Kim, and O. Kwon, "Central bank digital currency and privacy: A randomized survey experiment," 2023. [Online]. Available: <https://www.bis.org/publ/work1147.htm>
- [11] N. Pocher and A. Veneris, *Central bank digital currencies*. Springer, 2022, pp. 463–501.
- [12] 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](https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Privacy_in_cross-border_digital_currency_-_A_transatlantic_approach_-_pdf)
- [13] Bank for International Settlements, "Project Tourbillon – exploring privacy, security and scalability for CBDCs," 2023. [Online]. Available: <https://www.bis.org/publ/othp80.htm>
- [14] 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](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3891121)
- [15] 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.
- [16] Committee on Payments and Market Infrastructures, "Central bank digital currencies," 2018. [Online]. Available: <https://www.bis.org/cpmi/publ/d174.htm>
- [17] R. Auer, G. Cornelli, and J. Frost, "Rise of the central bank digital currencies: drivers, approaches and technologies," 2020. [Online]. Available: <https://www.bis.org/publ/work880.htm>
- [18] 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>
- [19] G. Goodell, H. D. Al-Nakib, and P. Tasca, "A digital currency architecture for privacy and owner-custodianship," *Future Internet*, vol. 13, no. 5, p. 130, 2021.

- [20] R. J. Garratt, M. J. Lee, B. Malone, and A. Martin, "Token-or account-based? A digital currency can be both," 2020. [Online]. Available: <https://ideas.repec.org/p/fip/fednls/88550.html>
- [21] J. Kiff, "Taking digital currencies offline," [Online]. Available: <https://www.imf.org/en/Publications/fandd/issues/2022/09/kiff-taking-digital-currencies-offline>
- [22] C. Minwalla, J. Miedema, S. Hernandez, and A. Sutton-Lalani, "A central bank digital currency for offline payments," 2023, Bank of Canada working paper 2023-2. [Online]. Available: <https://www.bankofcanada.ca/2023/02/staff-analytical-note-2023-2/>
- [23] H. Armelius, C. A. Claussen, and I. Hull, "On the possibility of a cash-like CBDC," 2021. [Online]. Available: <https://ideas.repec.org/p/zbw/esprep/231485.html>
- [24] Y. Chu, J. Lee, S. Kim, H. Kim, Y. Yoon, and H. Chung, "Review of offline payment function of CBDC considering security requirements," *Applied Sciences*, vol. 12, no. 9, p. 4488, 2022.
- [25] T. Alper, "Further details of 'offline' Chinese Digital Yuan 'hard wallet' emerge," 2021. [Online]. Available: <https://cryptonews.com/news/further-details-of-offline-chinese-digital-yuan-hard-wallet-8891.htm>
- [26] GlobalPlatform, "Introduction to secure elements," 2018. [Online]. Available: <https://globalplatform.wpengine.com/resource-publication/introduction-to-secure-elements/>
- [27] G. Alendal, S. Axelsson, and G. O. Dyrkolbotn, "Chip chop — smashing the mobile phone secure chip for fun and digital forensics," *Forensic Science International: Digital Investigation*, vol. 37, p. 301191, 2021.
- [28] K. Mayes, "An introduction to smart cards," in *Smart Cards, Tokens, Security and Applications*. Springer, 2017.
- [29] K. Markantonakis and R. N. Akram, "Multi-application smart card platforms and operating systems," in *Smart Cards, Tokens, Security and Applications*. Springer, 2017, pp. 59–92.
- [30] S. Skorobogatov, "Teardown and feasibility study of IronKey – the most secure USB Flash drive," 2021. [Online]. Available: <https://arxiv.org/abs/2110.14090>
- [31] GlobalPlatform, "Secure element protection profile," 2021. [Online]. Available: <https://www.commoncriteriaportal.org/files/ppfiles/CCN-C-C-PP-5-2021.pdf>
- [32] P. K. Manadhata and J. M. Wing, "An attack surface metric," *IEEE Transactions on Software Engineering*, vol. 37, no. 3, pp. 371–386, 2011.
- [33] G. M. Garrido, J. Sedlmeir, Ö. Uludağ, I. S. Alaoui, A. Luckow, and F. Matthes, "Revealing the landscape of privacy-enhancing technologies in the context of data markets for the IoT: A systematic literature review," *Journal of Network and Computer Applications*, vol. 207, p. 103465, 2022.
- [34] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2015.
- [35] GlobalPlatform, "Introduction to trusted execution environments," 2018. [Online]. Available: <https://globalplatform.wpengine.com/resource-publication/introduction-to-trusted-execution-environments/>
- [36] J. Ménétrey, C. Göttel, A. Khurshid, M. Pasin, P. Felber, V. Schiavoni, and S. Raza, "Attestation mechanisms for trusted execution environments demystified," in *Distributed Applications and Interoperable Systems*. Springer, 2022, pp. 95–113.
- [37] S. Cen and B. Zhang, "Trusted time and monotonic counters with Intel® Software Guard Extensions Platform Services," 2017. [Online]. Available: <https://cdrdv2-public.intel.com/671564/intel-sgx-platform-services.pdf>
- [38] M. Schneider, R. J. Masti, S. Shinde, S. Capkun, and R. Perez, "Sok: Hardware-supported trusted execution environments," May 2022.
- [39] A. Muñoz, R. Ríos, R. Román, and J. López, "A survey on the (in)security of trusted execution environments," *Computers & Security*, vol. 129, p. 103180, 2023.
- [40] D. Cerdeira, N. Santos, P. Fonseca, and S. Pinto, "SoK: Understanding the prevailing security vulnerabilities in TrustZone-assisted TEE systems," in *Symposium on Security and Privacy*. IEEE, 2020.
- [41] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on Computing*, vol. 18, no. 1, pp. 186–208, 1989.
- [42] S. Chaliasos, J. Ernstberger, D. Theodore, D. Wong, M. Jahanara, and B. Livshits, "SoK: What don't we know? Understanding security vulnerabilities in SNARKs," 2024. [Online]. Available: <https://arxiv.org/abs/2402.15293>
- [43] F. Tramèr, D. Boneh, and K. Paterson, "Remote Side-Channel attacks on anonymous transactions," in *29th USENIX Security Symposium*. USENIX Association, 2020, pp. 2739–2756. [Online]. Available: <https://www.usenix.org/conference/usenixsecurity20/presentation/tramer>
- [44] E. Ben-Sasson, I. Bentov, Y. Horesh, and M. Riabzev, "Scalable zero knowledge with no trusted setup," in *Annual International Cryptology Conference*. Springer, 2019, pp. 701–732.
- [45] B. Brodsky, A. Dubey, and D. Tercero Lucas, "Enabling offline payments in an online world. Privacy considerations," 2023. [Online]. Available: <https://www.lipisadvisors.com/whitepapers>
- [46] M. Riccardi and M. Levi, "Cash, crime and anti-money laundering," in *The Handbook of Criminal and Terrorism Financing Law*. Palgrave Macmillan, 2018.
- [47] N. Pocher, M. Zichichi, F. Merizzi, M. Z. Shafiq, and S. Ferretti, "Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics," *Electronic Markets*, vol. 33, no. 1, 2023.
- [48] Financial Action Task Force on Money Laundering, "The 40 Recommendations, published October 2004," [Online]. Available: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/The40recommendationspublishedoctober2004.html>
- [49] G. P. Hancke, "Distance-bounding for RFID: Effectiveness of 'terrorist fraud' in the presence of bit errors," in *International Conference on RFID-Technologies and Applications*, 2012, pp. 91–96.
- [50] A. Ranganathan and S. Capkun, "Are we really close? Verifying proximity in wireless systems," *IEEE Security & Privacy*, vol. 15, no. 3, pp. 52–58, 2017.
- [51] B. Brodsky, A. Dubey, and D. Tercero Lucas, "Enabling offline payments in an online world. Scalability," 2023. [Online]. Available: <https://www.lipisadvisors.com/whitepapers>
- [52] —, "Enabling offline payments in an online world. Interoperability," 2023. [Online]. Available: <https://www.lipisadvisors.com/whitepapers>
- [53] A. Chatterjee and K. M. M. Aung, *Fully Homomorphic Encryption in Real World Applications*. Springer, 2019.
- [54] A. Poller, U. Waldmann, S. Vowé, and S. Türppe, "Electronic identity cards for user authentication – promise and practice," *IEEE Security & Privacy Magazine*, vol. 10, no. 1, pp. 46–54, 2012.
- [55] European Commission, "Anti-money laundering and countering the financing of terrorism legislative package," 2021. [Online]. Available: [https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package\\_en](https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en)
- [56] 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.
- [57] L. de Lima and E. M. Salinas, "Retail central bank digital currency: From vision to design," 2022. [Online]. Available: <https://www.oliverwymanforum.com/content/dam/oliver-wyman/ow-forum/future-of-money/Retail-Central-Bank-Digital-Currency-From-Vision-to-Design.pdf>
- [58] Bank for International Settlements, "CBDCs: an opportunity for the monetary system," 2021. [Online]. Available: <https://www.bis.org/publ/arpdf/ar2021e3.pdf>
- [59] E. Rennie and S. Steele, "Privacy and emergency payments in a pandemic: How to think about privacy and a central bank digital currency," *Law, Technology and Humans*, vol. 3, no. 1, pp. 6–17, 2021.
- [60] R. J. Garratt and M. R. Van Oordt, "Privacy as a public good: a case for electronic cash," *Journal of Political Economy*, vol. 129, no. 7, pp. 2157–2180, 2021.
- [61] P. Casanovas, J. González-Conejero, and L. De Koker, "Legal compliance by design (LCbD) and through design (LCtD): Preliminary survey," *CEUR Workshop Proceedings*, vol. 2049, pp. 33–49, 2018.
- [62] A. Cavoukian, "Privacy by design," *Office of Information and Privacy Communication*, 2011.
- [63] K. Yeung, "Hypernudge: Big Data as a mode of regulation by design," *Information, Communication & Society*, vol. 20, no. 1, pp. 118–136, 2017.
- [64] M. Cipriani, L. S. Goldberg, and G. La Spada, "Financial sanctions, SWIFT, and the architecture of the international payment system," *Journal of Economic Perspectives*, vol. 37, no. 1, pp. 31–52, 2023.
- [65] T. W. House, "Technical design choices for a U.S. CBDC system," 2022. [Online]. Available: <https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Technical-Design-Choices-US-CBDC-System.pdf>
- [66] B. Custers, J.-J. Oerlemans, and R. Pool, "Laundering the profits of ransomware: Money laundering methods for vouchers and cryptocurrencies," *European Journal of Crime, Criminal Law and Criminal Justice*, vol. 28, no. 2, pp. 121–152, 2020.
- [67] European Commission, "Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC," 2015.
- [68] GlobalPlatform, "Confidential card content management," 2019. [Online]. Available: <https://globalplatform.org/specs-library/confidential-card-content-management-amendment-a-v1-2/>
- [69] S. Feulner, J. Sedlmeir, V. Schlatt, and N. Urbach, "Exploring the use of self-sovereign identity for event ticketing systems," *Electronic Markets*, vol. 32, pp. 1759–1777, 2022.