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

(Anonymous submission)

***Abstract*—An increasing number of central banks are actively researching and piloting digital versions of fiat money, specifically retail Central Bank Digital Currency (CBDC) systems. 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, the need arises to leverage technology to accommodate various regulatory requirements that are key in the financial space. This paper deploys a compliance-by-design approach to evaluate technologies that are useful to balance privacy with anti-money laundering and counter-terrorism financing (AML/CFT) measures. Ultimately, it provides a classification of privacy design options and corresponding technical building blocks for offline CBDCs, along with their impact on AML/CFT measures. It also outlines commonalities and differences between offline and privacy-focused online solutions and 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 continues to grow (including stablecoins and other crypto-assets); (2) improve transaction efficiency and modernize central bank money; (3) ensure system resilience and accessibility in the face of communication deficiencies/outages; and (4) improve financial inclusion [3]–[8].

Amidst various design options central to current explorations, there is a growing focus on the potential for transferring CBDC funds independently of internet connectivity [9], [10]. *Offline CBDC transactions*, colloquially known as *proximity payments* [11], 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], [9]. 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 in the context of 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 [12], [13]. On the other hand, this expectation should not serve as a possible means to circumvent Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) regulations and/or to facilitate tax evasion [14]–[17]. Hence, solutions must be crafted to address the tension between the privacy requirements of end-users and the transparency and accountability measures required to deter illicit activities [12]. One effective approach is to move beyond merely identifying the regulatory impact of technology (or vice versa) and instead adopt *inherently* compliant solutions [18]. Leveraging the approach known as compliance-by-design [18], this paper focuses on the *privacy-transparency trade-offs* associated with offline CBDCs. By doing so, we provide guidelines on how CBDC systems with offline functionality can reach set AML/CFT design goals. We achieve this by expanding on existing classifications of offline CBDC functionalities [9]. This paper additionally contributes the following:

- An analysis of how established and emerging technologies can enable offline CBDC payments along with the advantages and shortcomings of balancing the privacy-transparency trade-off.
- A classification of privacy design options that can be achieved in offline CBDCs with current technology, taking into account the potential interaction 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.

Our findings confirm that offline transactions with existing hardware/software technology solutions have the potential to introduce additional degrees of flexibility to the privacy-related design choices that can emulate the privacy features of physical cash in CBDC systems.

The remainder of this paper is organized as follows. Sec. II introduces CBDCs, the motivation for their offline functionality, the technologies that can be leveraged to implement offline CBDCs, and our problem assumptions. Sec. III discusses offline CBDCs in their technical options and the different 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, their integration into a potential online system and analyzes their privacy and AML/CFT impact. Sec. VI elaborates on our findings and limitations. Sec. VII concludes the paper and lays foundations for future cross-disciplinary research on the topic.

II. Background

A. Central Bank Digital Currencies

A fundamental classification of CBDCs lies in the distinction between *wholesale* and *retail* systems. The former caters to financial institutions and interbank transactions, while the latter delivers digital cash directly to the public. This work focuses on retail CBDCs that embody a novel digital form of central bank money. They are a liability of the central bank, denominated in an established unit of account, functioning as both a medium of exchange and a store of value [19]. In essence, a retail CBDC is a fiat currency that can coexist with

other forms of central bank money (e.g., physical cash and bank reserves), and with commercial bank and e-money [7], [15]. Additionally, 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 [7], [14]. Admittedly, the majority of explorations and pilots conducted by central banks focus on the second option.

Another common classification for CBDCs distinguishes *token-based* and *account-based* structures [4], [20]. 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 [21]. However, this classification is not unique (e.g., account updates can be represented as spending a token and receiving a new one [17]) and reportedly also falls short in covering the features of many potential CBDC designs [22].

B. Motivations for the Offline Functionality

Within the global conversation about digital currencies, there is consensus on the significance of offline functionality in CBDC systems [23]. Representing a self-contained digital ecosystem, CBDCs are meant to stand as a modern counterpart to physical cash [24]. Evidently, central banks, attuned to the transformative potential, are actively engaged in exploring [25], [26] or piloting [10], [27], [28] various designs. In this dynamic pursuit, offline CBDCs align with a myriad of system goals, heralding a paradigm shift in the realm of central banking objectives [9]. These goals include:

- *System resilience and accessibility:* Facilitating payments during connectivity/system disruptions, or in regions with communication infrastructure deficiencies.
- *Financial inclusion and accessibility:* Promoting access to financial services in underserved communities (such as, the unbanked, aboriginals, and individuals with no access to the required computing/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 facilitating low-value and high-frequency peer-to-peer 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 [9], [12]. The absence of a fully private digital alternative to cash raises concerns about the potential extinction of *fully confidential transactions* in the evolving landscape of electronic payments.
- *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 hardware/software solutions that cannot be exhaustively considered 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) [29], but also as stand-alone chips in some phones [30]. 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 EEPROM (Electrically Erasable Programmable Read-Only Memory) or, more recently, flash memory [31]. 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 [32].

SEs can provide the highest levels of integrity and confidentiality and they are frequently certified against the Common Criteria EAL and FIPS 140-2 [33] 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 [34]. 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 to gain access to confidential data [35]), among others, SEs usually remain low on computational capabilities [31] and offer only highly restricted functionalities (i.e., 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 [36]. 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 [37], [38]. 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 [38]. Further, their ability for remote attestation, through which they can demonstrate that the code being executed can be trusted to be untampered [39], [40], makes them compelling solutions for applications with increased security requirements, such as mobile payments. TEEs also offer additional valuable features which SEs do not support, like network connectivity and time-keeping capabilities. As such, TEEs can have dedicated access to peripherals (e.g., sensors) through a trusted path ensuring the integrity of the exchanged information.

On the other hand, TEEs suffer from a wide range of vulnerabilities [36], [41], [42]. 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 advantages of design flaws in the TEE architecture; and the last category leverages hardware components of the platform, such as caches, by manipulating them to compromise the TEE's security. Finally, due to the high privilege level in which TEEs execute, if they are compromised then the unsecured OS can also be compromised regardless of lack of vulnerabilities of its own [41]. 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 [43]. ZKPs allow a prover to demonstrate that they executed a publicly known algorithm on a private input (which is only accessible to the prover and not shared with the verifier) with a public output (result) [36]. Thus, they provide, similarly to TEEs but through software-based means, *computational integrity* for arbitrary programs and *confidentiality* of the private input with respect to the verifier [36], [43]. However, unlike SEs and TEEs, ZKPs do not provide *confidentiality* and *integrity* toward the prover, i.e., the prover can access all the data underlying the corresponding computation, and arbitrarily modify variables when the legitimacy of modifications is not checked by an online verifier.

Advantages of ZKPs include their independence from any underlying secure hardware, and, by extension, from the corresponding industrial manufacturers (as compared to SEs and TEEs), with their security guarantees being derived organically from cryptographic primitives [17]. While many ZKP implementations require a coordination-intensive trusted setup that relies on at least one honest party for integrity guarantees, there are also variants that do not [36], [44]. Further, as opposed to TEEs, ZKPs involve a significant prover overhead, although continuous improvements are being made in this front [17].

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 [14]. More so, the privacy of payment systems is consistently ranked as a top priority for citizens in public surveys [12]. 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 such as anonymous e-money, notoriously impacts financial integrity and crime [46]. In particular, this anonymity hinders the identifiability of payer and payee and also the traceability of the associated flows, e.g., by means of graph analyses [47]. This challenge led to the imposition of 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, as well as daily or monthly turnover limitations for individuals. Moreover, there are restrictions on cross-border transfers and the denomination of banknotes.

The effectiveness of these restrictions can diminish with CBDCs, primarily because CBDCs could 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 degree of anonymity of cash payments while surmounting its physical limitations may raise concerns similar to the online setting, thus necessitating some restrictions, e.g., on turnover [17]. Hence, an adequate design of usage controls and end-user privacy is vital and this process involves a *trade-off* between access to the means of payment and maintaining accountability. As outlined in Sec. IV, this trade-off has to be considered with particular care when it comes to offline functionalities.

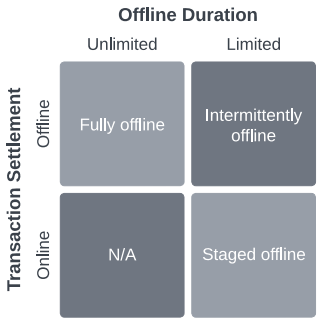

Fig. 1. Different types of offline CBDC transactions

E. Underlying Assumptions

This paper makes the following assumptions:

1) It strictly considers retail CBDCs where offline functionality has 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 int'l 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 [16], [26];
4) It neither addresses the issues of scalability and interoperability of offline CBDC systems [51], [52] nor does it consider applications of homomorphic encryption [53];
5) It scrutinizes privacy measures from the end user's perspective, and transparency ones from the regulator's capacity to match end-user identity with actual transaction details.

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). Similarly, additional constraints, such as completing transactions without relying on an external power source, can be introduced [10].

A. BIS Classification of Offline CBDC Transactions

In [9], the Bank for International Settlements delineated three categories of offline CBDC transactions that are also adopted as a classification for offline CBDC functionality in this paper. Fig. 1 offers an overview of their primary 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.

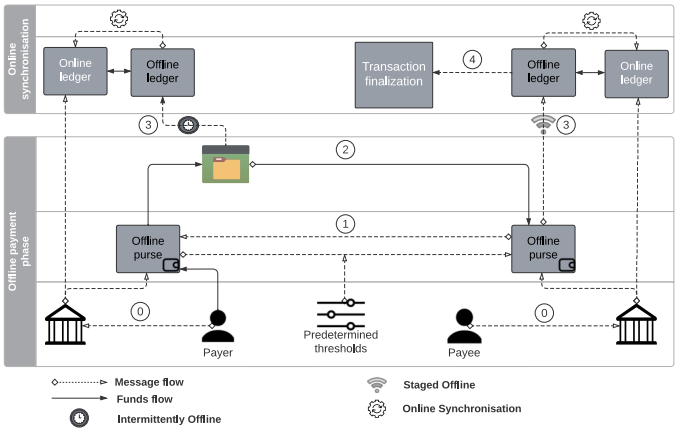

Fig. 2. Offline CBDC Payment Cycle

- *Intermittently offline*: This setup allows the payer and payee to complete only a limited set of payments fully offline. Similarly to above, transactions are settled offline and the funds are available for spending. Risk parameters will eventually limit further transactions, requiring occasional synchronization with the central system in which end-users synchronize their wallets online for continued functionality. The online system makes use of a separate ledger to keep track of the user's offline balance and/or transaction logs.
- *Staged offline*: Here, the payer and payee do not need to connect to a ledger system for a value exchange between purses to occur, but the payee cannot spend the transferred value until they connect to the ledger for online settlement. Similarly to intermittently offline, an additional ledger is needed beyond the online CBDC system to provide continued offline payment functionality.

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 conventional 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 in order to connect them with third-party banking services, offline CBDC payments can provide a more versatile and self-reliant approach [24]. The primary distinction emerges from the potential for offline CBDCs to either mimic existing payment card systems or establish a self-reliant ecosystem equipped with the requisite technologies to autonomously facilitate offline transactions as well as to enable users to manage their accounts [24]. We now proceed to examine the various phases of the offline CBDC payment process and gain an initial understanding of their operation, also illustrated in Fig. 2.

Before CBDC transactions can be conducted, users go through step ⓪ (Fig. 2), 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. 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 [17]. A comprehensive KYC process is key in the context of AML/CFT compliance. In Sec.V, this paper further discusses how a strong device or hardware binding established through the KYC may be key to achieve a plausible implementation of a high-privacy option also for offline CBDCs [17]. Relying on [9], the following offline CBDC payment process comprises the two phases of 'offline payment' and 'online synchronization'.

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 said 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 needs to prove 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.

In order for the authentication protocol to be executed, devices can be provisioned with a cryptographic keypair for signing the exchanged messages and in particular 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 the appropriate certificate authorities' (CAs) certificates or the existence of a minimal PKI from which the CA can be fetched/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 of the value to be transferred and ensure the atomicity of the transaction. For instance, both devices' local balances may be updated, or the payer may send unique serial numbers corresponding to coins to the payee and delete them in the payer's wallet. 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 or names), 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 current balance of the purse and transaction logs, are synchronized with the offline ledger. This procedure involves some proof of ownership of the corresponding (KYCed) online ledger account. At the same time, maintenance tasks (e.g., system updates, risk parameter update, reconciliation between ledgers, etc.) can be carried out.

2) Transaction finalization: Step ④ occurs only for the staged offline case during which the transaction is settled online and the 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 [16]).

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 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. While monitoring and limiting the use of physical cash are widespread means to combat money laundering, terrorist financing, and tax evasion [18], the goal in the CBDC space is to avoid threats to the existing safeguards against financial crime, while establishing AML/CFT competences in CBDC systems which include various stakeholders. 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. The risk is amplified by the foreseen potential of CBDCs to intrude into the private life of individuals [58], [59] – e.g., payment history datasets generated by commercial payments platforms [18], [60].

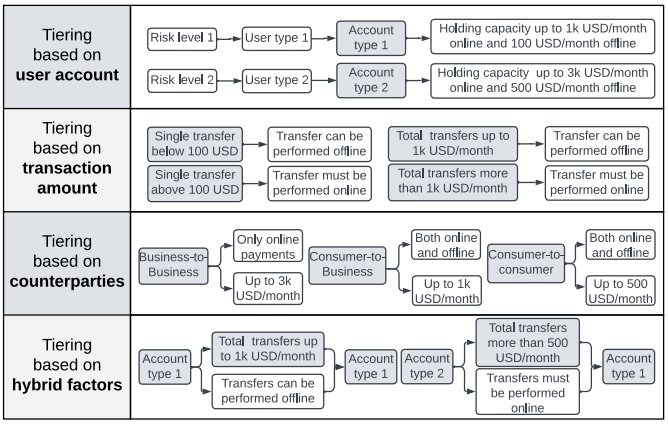

Fig. 3. Types of Account and Transaction Tiering and Examples

B. Compliance-by-Design and Tiered CBDC Options

To be compliant means achieving and demonstrating conformity with given regulatory constraints – e.g., 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 [18]. 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, 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, addressing privacy-transparency trade-offs, defining risk parameters, and balancing diverse regulatory requirements [14].

In CBDC investigations, a need has emerged to balance diverse regulatory requirements. Concerning privacy and transparency, CBDCs can be designed to accommodate multiple options [17], [57]. In fact, most CBDC projects offer both some degree of privacy for end-users and some degree of transparency to authorities by offering a composite system [18]. 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), counterparty 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 grounded on the classification of 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 participants of the CBDC system 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, the offline functionality of the system 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 we move to identifying the AML/CFT specifics of various technical options in terms of offline functionality, we list below the AML/CFT elements that inform the CBDC offline payment cycle functionality. 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., possibility to screen transactions real-time before approval and block them when identified as risky or illicit;
- it is possible to blocklist 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 [17].

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 the online ledger, i.e., which data provided by the end-user is directly accessible to the operator of the online ledger [21]. For each model, we describe the possible technology stack they can leverage, and elaborate on their repercussions in terms of the key AML/CFT dimensions for offline functionalities as outlined in Sec. IV. We provide a summarized depiction of our findings in Fig. 4.

A. Fully offline with no KYC

The first model into consideration is a fully offline solution 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 here being to emulate 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 (e.g., 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. In a nutshell, its model relevance acts as a yardstick against which other privacy-centric concepts and solutions should be assessed, rather than intended for immediate adoption or practical implementation by central banks.

Unsurprisingly, this technological scenario offers minimal capabilities in terms of compliance. 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 as today's existing anonymous gift/prepaid cards/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, turnover capacity, and (im)possibility to reload the payment instrument. We emphasize that in the EU, for instance, AML/CFT measures are particularly strict with limiting functionalities of anonymous prepaid/gift cards: they must not be reloadable and they are subject to balance (and, therefore, 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 [17]. In contrast to the previous hypothetical model, this design is of more practical application. Finally, 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 it does not employ any privacy-preserving technologies, it offers privacy assurances comparable to those of a prepaid card in combination with a bank account, and the possible AML/CFT treatment can also be foreseen as similar. If the online ledger provides high privacy guarantees, such as TEEs or ZKPs to construct proofs as in [17], and topping up is done 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 [17], 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 [17], [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 [17]. To mitigate such risks, verification of access to a corresponding digital identity in offline payments (via SEs or TEEs) can be implemented, coupled with occasional revocation checks (with synchronized revocation lists).

C. Hybrid: Intermittently offline and high privacy

This model (corresponding to 'Intermittently Offline I' in Fig. 4) for offline CBDC transactions adopts an intermittently offline approach. As outlined in Section III, this option 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.

		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

To safeguard the privacy of end-users, the balance tracking could be done in a privacy-preserving manner with the assistance of TEEs or ZKPs. Similar to the previous two designs, compliance measures in this model could be established through counter-based mechanisms, leveraging SEs or TEEs. These checks, however, could be expanded through time-based mandatory synchronization enforcement, which can be introduced through 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 payment activities. In addition to balance tracking, *transaction tracking* also takes place through which the online ledger receives information about actual transactions, including timestamps and transacting parties. While privacy-preserving disclosure is feasible for balances, this may not be viable for transaction details, especially if they are intended for further online computations like transaction graph analysis. Since the online system requires access to the original data for such computations, solutions such as ZKPs that do not reveal private data cannot be leveraged.

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, then transaction reversal could occur, 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 and much like the previous design model, TEEs emerge as one suitable choice.

VI. Limitations and open questions

From our analysis of the privacy and AML/CFT impact of different models that support 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 thus outline both of them below.

Firstly, we are conducting 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.

Next, the analysis presented here remains *jurisdiction agnostic*, prioritizing overarching regulatory principles over jurisdiction-specific AML/CFT regulations. While acknowledging this limitation, we recognize the importance of a nuanced analysis considering factors like specifics of FATF Recommendations, jurisdictional peculiarities of criminal justice systems, and domestic policies on illicit financial activities. Relying on FATF's Recommendations ensures alignment with globally recognized principles, forming a realistic foundational basis for the analysis. However, a jurisdiction-specific focus is essential for a comprehensive techno-regulatory design that ensures compliance while preserving privacy. Alternatively, one could focus on the cross-border dimension and additional challenges posed by said regulatory divergences [15].

Thirdly, 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 as these frameworks continue to evolve.

Relatedly, 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, in our work we intentionally left out a thorough exploration of broader repercussions, such as implications to monetary policy and central bank law [14]. 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.

Lastly, 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.

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-related design options of CBDCs. A fully offline CBDC appears to maximize privacy but compromises transaction monitoring and other essential risk management approaches impossible. 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 the implementation of 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 ongoing techno-legal assessments and implementations in the rapidly evolving landscape of CBDCs as central banks explore redefining the very essence of cash.

This work does not consider the effects of cryptographic primitives (such as homomorphic encryption) to complement the technology solutions presented here. Such primitives can assist in performing checks offline (e.g., overnight by the central bank and/or other CBDC intermediaries) while fully preserving the confidentiality of the underlying data unless 'red flags' arise from parsing this data. It also just touches the surface of the important issue behind *data protection* from offline CBDC payment transactions. Admittedly, these topics constitute additional avenues for future techno-legal research in offline CBDCs.

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," Tech. Rep., 2020. [Online]. Available: https://www.bis.org/publ/othp33.htm

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

[5] Bank of Canada, "Contingency planning for a central bank digital currency," Tech. Rep., 2020. [Online]. Available: https://www.bankofcanada.ca/2020/02/contingency-planning-central-bank-digital-currency/

[6] U. Bindseil, "Tiered CBDC and the financial system," European Central Bank (ECB), Tech. Rep., 2020. [Online]. Available: https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf

[7] S. Allen, S. Capkun, I. Eyal, G. Fanti, B. Ford, J. Grimmelmann, A. Juels, K. Kostiainen, S. john, A. Miller, E. Prasad, K. Wüst, and F. Zhang, "Design choices for central bank digital currency: Policy and technical considerations," Tech. Rep. 13535, 2020. [Online]. Available: https://www.nber.org/papers/w27634

[8] 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/

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

[10] 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

[11] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro," 2023.

[12] 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

[13] B. of Canada, "A digital canadian dollar: What we heard 2020–23 and what comes next," Tech. Rep., 2023. [Online]. Available: https://www.bankofcanada.ca/digitaldollar/a-digital-canadian-dollar-what-we-heard-2020-23-and-what-comes-next/

[14] N. Pocher and A. Veneris, *Central Bank Digital Currencies*. Springer, 2022, pp. 463–501.

[15] G. Fanti and N. Pocher, "Privacy in cross-border digital currency: A transatlantic perspective," A. C. G. Center and A. Brücke, Eds., 2022. [Online]. Available: https://www.atlanticcouncil.org/wp-content/uploads/2022/09/Privacy_in_cross-border_digital_currency-_A_transatlantic_approach__-.pdf

[16] Bank for International Settlements, "Project Tourbillon – exploring privacy, security and scalability for CBDCs," 2023. [Online]. Available: https://www.bis.org/publ/othp80.htm

[17] 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

[18] 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.

[19] Committee on Payments and Market Infrastructures, "Central bank digital currencies," Bank for International Settlements, Tech. Rep., 2018. [Online]. Available: https://www.bis.org/cpmi/publ/d174.htm

[20] 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

[21] 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.

[22] R. J. Garratt, M. J. Lee, B. Malone, and A. Martin, "Token-or account-based? A digital currency can be both," Federal Reserve Bank of New York, Tech. Rep., 2020. [Online]. Available: https://ideas.repec.org/p/fip/fednls/88550.html

[23] J. Kiff, "Taking digital currencies offline." [Online]. Available: https://www.imf.org/en/Publications/fandd/issues/2022/09/kiff-taking-digital-currencies-offline

[24] 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/

[25] 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

[26] 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.

[27] 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

[28] A. Cao, "Beijing forum promotes SIM-based 'e-CNY hard wallet' for digital payments," 2023. [Online]. Available: https://www.scmp.com/tech/big-tech/article/3237735/china-digital-currency-beijing-forum-promotes-sim-based-e-cny-hard-wallet-alternative-mobile

[29] GlobalPlatform, "Introduction to secure elements," 2018. [Online]. Available: https://globalplatform.wpengine.com/resource-publication/introduction-to-secure-elements/

[30] 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.

[31] K. Mayes, "An introduction to smart cards," in *Smart Cards, Tokens, Security and Applications*. Springer, 2017.

[32] 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.

[33] S. Skorobogatov, "Teardown and feasibility study of IronKey – the most secure USB Flash drive," 2021. [Online]. Available: https://arxiv.org/abs/2110.14090

[34] GlobalPlatform, "Secure element protection profile," Tech. Rep., 2021. [Online]. Available: https://www.commoncriteriaportal.org/files/ppfiles/CCN-CC-PP-5-2021.pdf

[35] P. K. Manadhata and J. M. Wing, "An attack surface metric," *IEEE Transactions on Software Engineering*, vol. 37, no. 3, pp. 371–386, 2011.

[36] 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.

[37] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not." IEEE, 2015.

[38] GlobalPlatform, "Introduction to trusted execution environments," 2018. [Online]. Available: https://globalplatform.wpengine.com/resource-publication/introduction-to-trusted-execution-environments/?utm_source=iseepr&utm_medium=Blog&utm_campaign=TEE

[39] 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 International Publishing, 2022, pp. 95–113.

[40] G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. O'Hanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen, "Principles of remote attestation," *International Journal of Information Security*, vol. 10, no. 2, pp. 63–81, 2011.

[41] 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.

[42] 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.

[43] 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.

[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 Singapore, 2019.
[54] A. Poller, U. Waldmann, S. Vowé, and S. Türpe, "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
[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. A framework to align policy objectives and technology design choices," 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," Tech. Rep., 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, Commumcation & 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. [Online]. Available: https://www.aeaweb.org/articles?id=10.1257/jep.37.1.31
[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. [Online]. Available: https://brill.com/view/journals/eccl/28/2/article-p121_121.xml
[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," Tech. Rep., 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.