Privacy and Compliance Design Options in Offline Central Bank Digital Currencies

Panagiotis Michalopoulos*, Odunayo Olowookere†, Nadia Pocher‡,
Johannes Sedlmeir‡, Andreas Veneris*§, Poonam Puri†
* Department of Electrical and Computer Engineering, University of Toronto
p.michalopoulos@mail.utoronto.ca, veneris@eecg.toronto.edu
§ Department of Computer Science, University of Toronto
† Osgoode Hall Law School, York University
odunayoolowookere@osgoode.yorku.ca, ppuri@osgoode.yorku.ca
‡ 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 many discussions revolving around these systems' design is the ability to perform transactions even without network connectivity. While this approach is generally believed to provide additional degrees of freedom for user privacy, the lack of direct involvement of third parties in these offline transfers also interferes with key regulatory requirements that need to be accommodated in the financial space. This paper presents 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, CBDC, compliance by design, offline payments, secure computation, secure hardware**

I. Introduction

Over the past years, more than 90 % of central banks have started active investigations into digital versions of fiat money that are accessible to end users [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, including digital sovereignty aspects; and (4) foster 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 network (e.g., Internet and/or cellular) connectivity [7]–[11]. *Offline CBDC transactions*, colloquially known as *proximity payments* [12], 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 [5], [13], [14]. On the other hand, such designs should not allow to circumvent anti-money laundering and counter-terrorism financing (AML/CFT) regulations, evade international financial sanctions regimes, or facilitate tax evasion [15]–[19]. Hence, solutions must address the *tension* between end users' privacy expectations and transparency and accountability measures required to deter illicit activities [13]. One effective approach is to move beyond merely identifying the regulatory impact of technology (or vice versa) and instead adopt *inherently* compliant solutions [20].

Leveraging the approach known as compliance-by-design [20], 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]. Additional contributions include:

- 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) processes and transaction monitoring, as well as of how said design choices align with the AML/CFT *risk-based approach*.

This paper extends our previous work [21] by expanding on the technical building blocks and by performing a more

comprehensive regulatory analysis. Our findings confirm that, leveraging existing hardware and software technology solutions, the provision of offline CBDC functionalities introduces additional degrees of flexibility to privacy-related designs. As a corollary, prospect retail CBDC systems offer a wide range of implementations for offline payments, including one emulating the strong privacy features of physical cash today.

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, privacy and data protection regulations, 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 cater to financial institutions and interbank transactions, while the latter deliver 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. 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 [4], [16]. 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 [4], [15]. Many CBDC explorations and pilots focus on the second option.

Another common classification for CBDCs that applies to both online and offline designs distinguishes between *token-based* and *account-based* structures [10], [22]. 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 [23]. However, this classification is not unique (e.g., account updates can be represented as spending a token and receiving a new one [18]) and reportedly also falls short in covering the features of many potential CBDC designs [24].

B. Motivations for the Offline Functionality

There is broad consensus on the significance of the offline functionality in CBDC systems [25], with central banks ranking it as both the most important and most challenging feature of CBDCs [26]. Representing a self-contained digital ecosystem, CBDCs are meant to stand as a modern counterpart to physical cash [27]. Evidently, central banks are actively exploring [28] or piloting [8] various designs. Offline CBDCs align with a myriad of system goals, heralding a paradigm shift in the realm of central banking objectives [7], [29]. These goals include:

- *System resilience and accessibility:* Facilitating payments during connectivity and system disruptions, or in regions with communication infrastructure deficiencies. Indeed, for 43 % of the central banks in developed markets, system resilience is the primary reason for pursuing offline CBDCs, whereas for 33 % of the central banks in emerging markets, accessibility in remote areas is one of the main drivers [26].
- *Financial inclusion and accessibility:* Promoting access to financial services in underserved communities (e.g., the unbanked and individuals with no access to networking resources) is the most important concern for around 35 % of the central banks in emerging markets [26].
- *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 payment means [7], [13]. 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.

	Capabilities	Limitations
Secure Elements (SEs)	• Highest integrity and confidentiality guarantees • Tamper-proof offline data storage • Secure device provisioning	• Low computational capabilities • Low upgradeability • Risk of side-channel attacks • Dependency on manufacturer
Trusted Execution Environments (TEEs)	• Similar to SEs, with increased computational capabilities and flexibility • Verifiable confidential computations	• Wider range of vulnerabilities compared to SEs • Risk of side-channel attacks • Dependency on manufacturer
Blind signatures	• Confidentiality during signing • Signature unlinkability • Security based on established cryptographic primitives	• No tamper-proof offline storage • Low degree of flexibility • Offer only one-sided privacy
Zero-Knowledge Proofs (ZKPs)	• Computational integrity • Confidentiality w.r.t. verifier • Security based on established cryptographic primitives	• No confidentiality w.r.t. prover • No tamper-proof offline storage • Mathematical and implementation complexity • Large computational overhead • No shared secrets
Multi-Party Computation (MPC)	• Confidential computations among multiple parties (more general than ZKPs) • Security based on established cryptographic primitives	• No tamper-proof offline storage • Mathematical and implementation complexity • Large computational and communication overhead

Fig. 1: Key capabilities and limitations of building blocks for offline CBDCs

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 explore yet cannot cover exhaustively in this paper due to space restrictions. Fig. 1 features a summary of their functionalities and limitations.

1) Secure Elements (SEs): SEs are tamper-resistant integrated circuits commonly found in mobile phone subscriber identification module (SIM) cards and smart cards (e.g., chip-and-PIN or signature bank cards, biometric passports) [30]. SEs comprise a secure microprocessor resistant to both remote and physical attacks, accompanied by small amounts (typically on the order of hundreds of KBs) of random-access memory (RAM) and persistent memory in the form of electrically erasable programmable read-only memory (EEPROM) 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 Java Card and MULTOS [32].

SEs can provide the highest levels of integrity and confidentiality and they are frequently certified against the common criteria (CC) evaluation assurance level (EAL) and federal information processing standard (FIPS) 140-2 [33] specifications for use in environments with particularly high security requirements. Further, they can be provisioned in a way that ensures that applications and data are installed on the SE during manufacturing time in a secure way, resisting tampering attempts [34]. However, due to the general need to reduce the attack surface (i.e., a system's components that can be used by an attacker to compromise it [35]), SEs usually remain low on computational capabilities [31] and often offer only highly restricted functionalities (e.g., only selected common cryptographic operations).

Attacks on SEs can be *invasive/active* or *non-invasive/ passive* [36]. The first category requires specialized equipment to actively manipulate the secure microprocessor (e.g., via probing or ion beaming). As such, they tend to be expensive and time-consuming. The second category includes side-channel attacks, where the attacker can extract confidential information from the system by observing its behavior without any active form of manipulation. This can include timing and power analysis attacks that take advantage of variations in the execution time of instructions or in the device's power consumption. As showcased by a recent issue with a large number of SEs that allowed the extraction of a private ECDSA key through a timing-based attack, such attacks often exploit vulnerabilities in the software libraries used by the SE [37].

Recently, SEs have been integrated as stand-alone chips in some high-end mobile phones [38]. Notably, Google Pixel phones and select Samsung models have an embedded SE to which limited developer access is provided through APIs [39], [40]. Similarly, Apple plans to give developers access to the APIs for its own SE that is part of its near-field communication (NFC) chip to facilitate a multitude of use cases, such as payments, corporate badge access, and virtual keys for smart locks [41]. As such, both secure cryptographic key management and the execution of sandboxed applets will be feasible. Finally, the advent of eSIMs has led to the increased availability of roaming profiles, i.e., SIM applets that can be securely downloaded to the eSIM chip after undergoing certification with the Global System for Mobile Communications Association (GSMA). As such, eSIMs constitute effectively a type of embedded SE with rich functionality, when compared to the aforementioned currently limited-access offerings.

2) Trusted Execution Environments (TEEs): TEEs are secure areas of a general-purpose microprocessor that offer increased integrity and confidentiality of the code executed and the data stored or processed in them [42]. 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 [43], [44]. As TEEs are part of a larger general-purpose processor, they usually have a wider range of computational capabilities than SEs. In particular, they not only protect the data stored in them from extraction, but they also flexibly execute arbitrary programs, called trusted applications (TAs), with low performance overhead [44]. Their ability for remote attestation, through which they can demonstrate *computational integrity*, i.e., that the code being executed was untampered [45], makes them compelling solutions for applications with increased security requirements and high risks of an attack, such as mobile payments. The combination of secure key storage and computational integrity also allows TEEs to be used for *verifiable confidential computations* among multiple parties, where sensitive information only leaves the TEE in encrypted form and can be decrypted and used for meaningful computations only within the TEE. Further, certain TEEs offer some valuable features that SEs do not support, for instance, integrated network connectivity and time-keeping capabilities [46]. Lastly, TEEs can have dedicated access to peripherals (e.g., sensors), ensuring the integrity of the exchanged information [47].

On the other hand, TEEs suffer from a wide range of vulnerabilities [48]. These can be software-based, architectural, and hardware-based, with the latter encompassing 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. Finally, due to the high privilege level in which TEEs execute, compromising the TEE can allow attackers to also compromise the unsecured OS, regardless of a lack of vulnerabilities of its own [48]. 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) Blind signatures: Blind signatures are a special type of digital signature in which the content of the message to be signed is hidden from the signer [49]. The resulting signature can be verified similarly to regular digital signatures by using the original unblinded message. Yet, even if the signer is called to verify their signature, they will not be able to link the blind signature to the unblinded message, effectively decoupling the two. Many popular digital signature constructions (e.g., RSA and ECDSA) can be adjusted to facilitate blind signing [50]. In many cases, creating a blind signature should still give the signer some confidence that the signed content is genuine. A very simple but inefficient probabilistic construction could, for instance, involve the signer blindly signing N messages and require the recipient to open all but one of them to check their content, and holding the recipient accountable for detected

misuse [51].

Blind signature schemes are frequently used when preservation of user privacy and particularly unlinkability are desired, such as in electronic voting or electronic cash. For example, a user could provide a blinded banknote to a bank for signing, unblind it, and then spend it. The payee must verify the signature and redeem the note with the bank. The bank checks the signature — but cannot relate it to the payer who requested it. The bank then credits the payee's account if the note has not been spent yet. Several such payment systems, including CBDCs, have been devised [17]. Importantly, common constructions of payment systems using blind signatures achieve only one-sided privacy for the payer, as the bank learns the payment amount and identity of the payee during the redemption process. This feature can be useful in payments involving merchants, where a reduction in the payee's privacy can be easily tolerated or is even desirable [18].

4) Zero-Knowledge Proofs (ZKPs): ZKPs are defined as those proofs that reveal nothing beyond the correctness of the proposition in question [52]. More precisely, ZKPs are required to satisfy the properties of *completeness*, *soundness*, and *zero-knowledge*. As per the first, an honest prover must be able to convince an honest verifier about a true statement (e.g., that they executed an algorithm) with high probability. Conversely, soundness requires that a malicious prover can produce a proof for a false statement with only a small (and, by means of repetition, arbitrarily small) probability. Finally, the zero-knowledge property ensures that the verifier learns nothing but the truthfulness of the statement. Note that if the sharing of additional information underlying the statement — such as inputs and intermediary results of a computation or predicates derived thereof — is desirable, this can always be done by a modification of the statement.

As such, 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) and obtained a public output (result) [42]. With slight modifications of the algorithm under consideration, any input can be made public if desirable, and any output can be hidden with additional checks being executed on them. Thus, ZKPs provide, similarly to TEEs' remote attestation but by only software-based means, computational integrity for arbitrary programs and confidentiality of the private input with respect to the verifier [42], [52]. However, in the offline setting (unlike SEs and TEEs), ZKPs do not ensure data integrity in the sense of preventing the user from manipulating locally stored data (unless the data can be verified against an external trust anchor), and they also cannot provide confidentiality toward the prover, i.e., the prover can access all the data underlying the corresponding computation.

An example application of ZKPs is the hiding of linkable cryptographic identifiers and personal information appearing on a digital certificate while proving their integrity, authenticity, and validity — including that it is properly signed [53]. They also offer selective disclosure and predicate proofs that can convince a verifier that a computation on the data included in the certificate, such as checking for a minimum age, yields a given result, without exposing the input data. This specific application area of ZKPs is called anonymous credentials. On the other hand, general-purpose ZKPs allow for the creation of proofs for the correctness of arbitrary computations without requiring the participants to execute an interactive protocol. A prominent example of general-purpose ZKPs is zk-SNARKs [54], which have the additional property of short ("succinct") proofs and verification times.

ZKPs can be considered a generalization of blind signatures, as they allow the prover to give compelling evidence that if the verifier were to conduct the signature verification algorithm on some obfuscated data, it would return true. Indeed, blind signatures have been constructed from ZKPs to achieve the highest level of unlinkability [55]. Blind signature generation can also benefit from ZKPs, as the recipient of the blind signature can prove that what is being blindly signed conforms to certain expectations (e.g., that a digital banknote has a given denomination) without disclosing any more information to the signer about it, e.g., the note's serial number.

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. Furthermore, ZKPs are flexible to meet both repudiability and non-repudiability requirements: While interactive ZKPs by design have the *designated verifier* property, i.e., they convince only the verifier that is directly involved in the interaction (usually by deciding on some random values) and lose their verifiability upon forwarding, non-interactive ZKPs, such as zk-SNARKs, are by construction verifiable by any third party. However, by including a specific modification of the statement, non-interactive proofs can still be made relevant only to the designated verifier [53].

On the other hand, ZKPs suffer from a high degree of mathematical and implementation complexity. For instance, common bug patterns [56] and side-channel attacks have been reported on ZKPs [57]. Further, as opposed to TEEs, general-purpose ZKPs involve a significant prover overhead, although continuous improvements are being made on this front. Some of these ZKP implementations also require a one-time 'trusted setup' that relies on at least one honest party to ensure that the soundness property holds; yet, there are also many variants that do not [42], [58].

5) Multi-Party Computation (MPC): MPC enables general-purpose confidential computations — i.e., multiple parties can jointly run an algorithm on their data without revealing each party's data to the others. Formally, the problem of MPC can be defined as follows [59]: Let f be a function that has n inputs and m outputs: $(y_1, \ldots, y_m) = f(x_1, \ldots, x_n)$ and $P = \{P_1, \ldots, P_N\}$ be a set of N parties. The goal of MPC is for participants to run a cryptographic protocol that will allow them to compute f, where each input x_i is provided by the party P_i, x_i is not shared with any party $P_{j \neq i}$, and each y_i is obtained by one or more of the parties. It is possible that a party does not submit any inputs (setting, e.g., $x_i \equiv 0$) or obtain any outputs.

Usually, MPC protocols are expected to satisfy the properties of *privacy*, *soundness*, and *input independence* [59]. The first property, as a generalization of the zero-knowledge

property, requires that a party cannot infer any information regarding the inputs of other parties apart from what can be already deduced from its own input and the part of the output of f it obtains. As such, a privacy assessment of any MPC-based protocol critically depends on the outputs and may need to be supplemented by other means, such as differential privacy, to achieve the desired privacy guarantees [42]. The second ensures that even in the presence of a certain threshold of malicious parties, if the MPC protocol does not abort, it will ensure that the result is correct. However, as each party involved in the MPC protocol controls their input, they can contribute fake data unless there is a check that the data is authentic within the MPC, e.g., by means of verifying a digital signature. In general, achieving maliciously secure MPC commonly is substantially more compute and bandwidth-intensive, and some MPC protocols integrate ZKPs to ensure that each party follows the agreed-on steps [60]. Finally, the third property requires that it is infeasible for a party to select their input based on the input of another party with the intention to manipulate the result or infer information about other inputs.

A special case of MPC is the set of techniques that fall under the umbrella of Fully Homomorphic Encryption (FHE), whose most common application is computation outsourcing. In the simplest form of FHE, a cryptographic protocol is run between two participants. The *provider* encrypts and sends the inputs of f to the (typically computationally more powerful) *processor* that evaluates f on the inputs without decrypting them and provides the encrypted outputs back to the provider. It is obvious that MPC offers greater versatility as it allows either party to provide private inputs. On the other hand, FHE reduces the communication overhead between parties required by MPC protocols as it does not require interaction between the parties during output computation. Finally, MPC can be achieved by the combination of FHE with distributed key generation, where the parties use the former for computing the outputs and the latter for encrypting the inputs (using the public key) and jointly decrypting the final public output (engaging in an MPC with the distributed private keys). Such solutions have found many applications on blockchains [61].

As such, MPC can provide a software-based alternative to TEEs (except for offline integrity and confidentiality towards the user) without the need for trusting the device manufacturer, but instead only leveraging cryptographic primitives. ZKPs can also be seen as a special case of a two-party MPC, where the verifier has an empty input and an accept/reject output. Nevertheless, this work dedicates a separate section to them due to the different applicability of ZKPs and MPC in the context of AML/CFT tasks and the higher degree of maturity of ZKPs, as they have been used at large scale in recent years in many privacy-oriented blockchain projects, such as mixers [62], as well as CBDC constructions [10], [18], [63]. While in the case of ZKPs, all sensitive information is held by one party (i.e., the prover), in MPC, the sensitive information can be distributed among multiple parties. This increases the applicability of MPC to cases with shared confidential state where ZKPs cannot be used, such as confidential transaction graph analysis. In this use case, metrics are derived from the entire graph while each involved party only knows a subset of the transaction graph [64], e.g., their own in the case of an individual or their own customers' in the case of a bank.

D. Balancing Compliance Requirements

If CBDCs are intended to mirror the user experience of coins and banknotes, the corresponding systems should include accessibility options that differ from the management of a traditional bank account [15]. The privacy characteristics of payment systems are consistently ranked as a top priority for citizens in public surveys [13], [14]. At the same time, several regulatory frameworks around the world mandate the protection of privacy and personal data also in the context of payments [65]. A prominent example is that of the General Data Protection Regulation (GDPR) in the European Union (EU) [66], [67].

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 [68], [69]. However, the inherent anonymity of cash and other bearer instruments (e.g., anonymous e-money) notoriously impacts crime prevention and the safeguarding of financial integrity [70]. In particular, anonymity hinders the identifiability of payer and payee and the traceability of the associated flows, e.g., by means of transaction graph analyses [71]. This challenge led to compliance standards and restrictions for transactions involving cash [72]. These restrictions can consist of limits on the purchase of specific types of goods or services, cross-border transfers, and the denomination of banknotes. For example, the EU introduced a EUR 10,000 limit on cash payments for goods or services — unless it is a private operation between individuals that are not acting in a professional function — in 2024 [73].

However, the effectiveness of these restrictions may diminish if CBDCs eliminate some physical limitations of cash. One immediate aspect relates to the potential to automate transactions in the digital realm. Moreover, although recent CBDC proposals have suggested that proximity payments have a similar risk profile to physical cash [12], malicious actors may abuse the fact that reliable digital proofs of proximity are difficult to implement [74], [75]. Therefore, they may disguise a remote payment as a proximity payment to benefit from potentially more lenient compliance rules for offline transactions. Consequently, offline CBDCs striving to replicate the anonymity of cash while surmounting their physical limitations raise concerns similar to an online setting, a fact that may necessitate certain restrictions. Furthermore, an exploit of secure hardware (SEs, TEEs) or cryptographic functionality that is aimed at ensuring certain compliance safeguards or even the foundational security requirements expected from a payment system (see (3) below) may give an attacker the opportunity to create and spend unlimited amounts of money that cannot be distinguished from legitimate money [18]. 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.

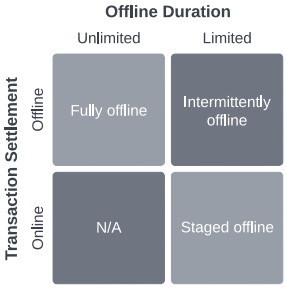

Fig. 2: Different types of offline CBDC transactions

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) [72]. 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 [17], [28];
4) It neither addresses the issues of scalability [76] nor interoperability [77] of offline CBDC systems;
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) are also sometimes 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. 2 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 one or multiple additional ledgers to keep track of the users' offline balances or transaction logs. In the following, we will assume that the online system comprises an "offline payments ledger" that directly receives updates from wallets about previous offline transactions and an "online payments ledger" that is connected to users' online accounts and the offline payments ledger.
- *Staged offline:* Here, the payer and payee do not need to connect to an online ledger system for value exchange between purses to occur, but the payee cannot spend the transferred value until they connect to an online ledger (similarly to 'intermittently offline') for 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 a more versatile and self-reliant approach [27]. 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 [27].

We now examine the various phases of the offline CBDC payment process and gain an initial understanding of their operation (see Fig. 3). Before CBDC transactions can be conducted, users go through step ⓪, 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 [18]. 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

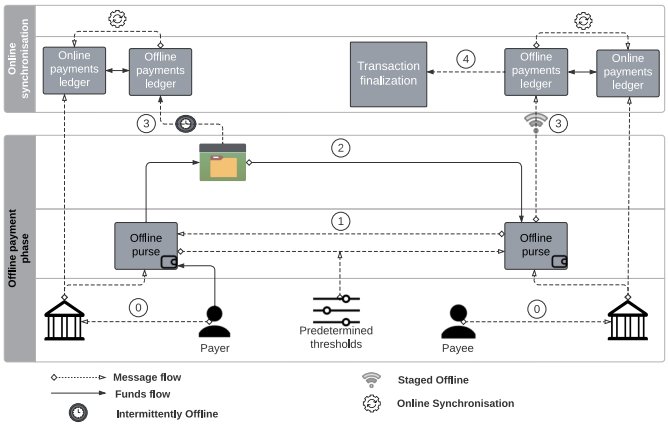

Fig. 3: Offline CBDC payment cycle

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 security (in particular, 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 means of 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. Further, a participation certificate signed by the central bank or 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. The public key for proving ownership of certificates can also function as a pseudonymous identifier for the device. In settings that maximize privacy, and where the verification of device authenticity or participation is not executed confidentially (e.g., in a TEE), many devices may obtain the same keypair from the manufacturer [78]. However, since sharing a common key can raise security concerns, anonymous credentials may constitute a better way to avoid the disclosure of unique identifiers when proving a device's authenticity.

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 (in an account-based system) may be updated, or the payer's wallet may send unique serial numbers corresponding to coins to the payee and delete them subsequently (in a token-based system) [79]. 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, including selected information about the transacting partners. In parallel, they can enforce basic AML/CFT rules based on pre-loaded risk parameters.

D. The Online Synchronization Phase

1) Offline-online data synchronization: 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 payments ledger. This procedure may involve some proof of ownership of the corresponding (KYCed) online payments 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 for spending, either online or offline. Additionally, data may be exchanged between the online and offline payments ledgers in accordance with the transaction's specific needs. These may be subject to additional verification processes to increase trust in offline transactions, such as the redemption of a coin on an unspent online list, similar to some payer-anonymous e-cash transactions based on blind signatures [17].

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 AML/CFT 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 [72], and the EU has recently strengthened the regime through a major reform [73]. 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, as well as checks of personal and business information according to given criteria), ongoing monitoring (e.g., transaction monitoring and screening), and record retention [80]. 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 [72]. The final objective is to inform the authorities of any suspicion of illicit deeds by filing a suspicious transaction report.

It is worth briefly expanding on the relationship between AML/CFT measures and compliance with regimes that impose financial sanctions [19]. Both pursue financial integrity and global economic security, and the AML/CFT framework is increasingly used to enforce restrictive financial measures [81]. However, while AML/CFT typically follows a risk-based approach that allows for varying levels of intervention based on assessed risks [72], sanctions regimes rely on lists of individuals, nations, or entities, compiled by governments or international bodies. Examples are the United Nations Security Council, the Office of Foreign Assets Control (OFAC) in the US, and the Council of the EU. These publicly available lists are based on certain criteria — such as involvement in

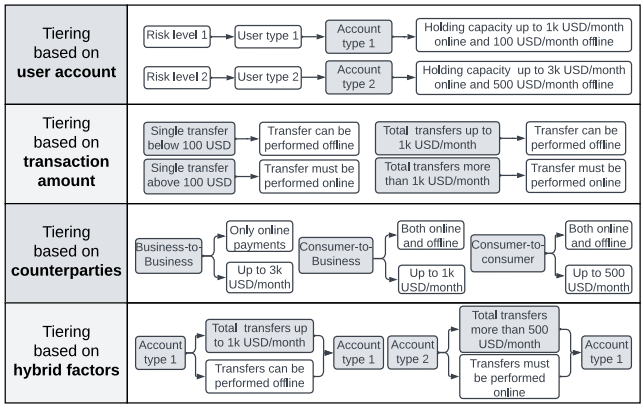

Fig. 4: Types of accounts and transaction tiering and examples

terrorism and human rights abuses. Inclusion in such lists carries predetermined consequences [82], such as exclusion from SWIFT, the international inter-banking system [19]. Compliance with some of the financial sanctions regimes is part of the AML/CFT framework, such as targeted financial sanctions in the area of counter-terrorism [72].

The AML/CFT dimension is at the core of CBDC experiments. Indeed, monitoring and limiting the use of physical cash are widespread means to combat money laundering and terrorism financing, as well as tax evasion and the enforcement of sanctions [20]. 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 [83] because it relates to giving access to data not only to regulatory and supervisory bodies but also to private actors (as with commercial bank money and e-money today). The corresponding privacy risk for individuals is amplified by the foreseen potential of CBDCs to intrude into the private lives of individuals [84] — e.g., payment history datasets generated by commercial payments platforms [20].

B. Privacy and Data Protection Regulations

While the protection of privacy has emerged as a key design objective, CBDC research often merges the concept of safeguarding 'privacy' with that of ensuring 'data protection'. The work of [23] distinguishes between 'privacy' — which refers to the end-user's control of how much data enters the CBDC system and how it is managed — and 'data protection' — the definition of who has access to specific data and the prevention of unauthorized access to it after collection. Indeed, already in [85], privacy was defined as the right of individuals to control access, collection, storage, and disclosure of personal information and maintain confidentiality and anonymity in their private lives. Data protection, on the other hand, involves the measures that safeguard personal data on identified and identifiable persons from misuse, ensuring its secure processing and handling [85]. However tied, privacy and data protection are two separate rights: the former is recognized by the Universal Declaration of Human Rights and enshrined by the European Convention of Human Rights, while both are recognized by the Charter of Fundamental Rights of the EU [86]. In the EU, both are protected by the GDPR and Regulation (EU) 2018/1725 for the processing of personal data by EU institutions (e.g., the European Central Bank).

Compliance with privacy and data protection regulations often seems at odds with AML/CFT, which brings challenges when designing a CBDC system. Indeed, the core tension lies in the fact that compliance with AML/CFT rules and the corresponding supervision is based on somewhat extensive data collection [20], while data protection laws, such as EU's GDPR, emphasize purpose limitation and data minimization and impose strict restrictions on data collection and processing [66]. Also in a CBDC context, when it comes to identifying the lawful basis for processing personal data (e.g., consent of the data subject, performance of a contract, compliance with legal obligations, or legitimate interest), such assessments are tied to the principles of necessity and proportionality, which align with the AML/CFT risk-based approach. Balancing the two, however, requires careful identification of the purpose and scope, as well as of the actors involved in the system [87].

From a cross-border perspective, regimes such as the GDPR impose restrictions on international transfers of personal (payment) data. Chiefly, such transfers are permitted if the receiving country ensures an adequate data protection level, which is assessed in several ways [66]. This landscape underscores the importance of discussions on designing CBDC systems by integrating technologies that prioritize data minimization while also ensuring both end-user privacy and transaction transparency for compliance purposes.

C. 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 [88]. While certain checks are increasingly automated to reduce costs and improve accuracy [71], compliance itself is a granular concept that is not fully translatable into binary requirements [88]. Specific aspects can, however, be streamlined into the technology design process. This proactive approach first emerged with privacy-by-design [89] and evolved into compliance-by-design, where compliance is embeddable into technology [90]. When technology design is leveraged for compliance purposes, it requires preliminary engineering and standard setting [20]. 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 [19]. In contrast, AML/CFT compliance operates within a risk-based system, navigating nuanced scenarios affecting collections of transactions, defining risk parameters, and balancing diverse regulatory requirements (e.g., privacy-transparency trade-offs) [15].

CBDC investigations must balance diverse regulatory requirements. Concerning privacy and transparency, CBDCs can

be designed to accommodate multiple options [18], [83]. Most CBDC projects aim to offer both some degree of privacy for end-users and some transparency to authorities by means of a composite system [20]. 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 [91]. 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) [91]. 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, e.g., on the amounts or frequency of offline transfers. These limits, in turn, may depend on further parameters, such as transaction type. 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. 4, we depict possible examples of transaction tiering in the context of offline capabilities. Meanwhile, the provision of offline functionalities with no AML/CFT tracing for low-value transfers has emerged as particularly conducive to meeting GDPR's principle of proportionality. That is, the same principles applicable to cash, cryptocurrencies, and prepaid cards may be applicable to (offline) CBDC payments [18], [92].

D. AML/CFT Design Choices for an Offline CBDC System

Three overarching CBDC design angles highlighted in [83] 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 privacy spectrum that spans from a high level of privacy where all transactions are hidden from every stakeholder, to selective visibility, where certain data from specific transactions are accessible to designated stakeholders, and finally to a high degree of transparency, where all transactions are visible to all stakeholders [83]. 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 [91].

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 and elaborate on the possibility and/or requirement to perform certain corresponding checks real-time (e.g., before the transaction is settled, such as in the case of checks behind sanctions), near real-time (e.g., in batches at the end of the day) or ex-post, when allowed by the AML/CFT regime (Fig. 5). 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 an end-user's 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 as well as other more complex operations, including transaction graph and behavioral analysis – i.e., the ability to screen and analyze transactions in real-time before approval and to block them when identified as risky or illicit. As a result of the inability to conduct real-time screening, transactions may need to be screened in batches or ex-post following online synchronization (Fig. 5);
- It is possible to blocklist payers and/or payees, and financial sanctions lists (with amendments) can be integrated in the form of a watchlist into the offline system;
- 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's identity [18].

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 [23]. 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. 6 features a summary of our findings.

Real-time		Near real-time (e.g., in batches)		Ex-post	
Operation	*Data source*	*Operation*	*Data source*	*Operation*	*Data source*
Identity verification	• Locally stored credentials (e.g., eID, KYC certificate)	**Balance tracking**	• Locally stored offline transaction history • Online transaction metadata	**Historical transaction graph analysis**	• Online transaction metadata • Data from multiple users
Basic transaction limits	• Predetermined thresholds • Locally stored offline transaction history	**Transaction screening**	• Online and offline transaction metadata • Locally stored credentials	**End-user risk profiling**	• Online and offline transaction metadata • Users' KYC information
Sanctions screening	• Locally stored credentials • Sanctions lists	**Graph analysis for transaction tracking**			

Fig. 5: AML/CFT functionalities in CBDC systems that include offline capabilities

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 [78] or SEs in combination with anonymous credentials [18]), 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. 6). 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. For instance, it would be impossible to conduct real-time transaction screening due to a lack of real-time data and network connectivity. Thus, the AML/CFT compliance mechanism for this scenario will be limited to the data available on the local storage of the end-user's device. Consequently, regulations 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 [93]. 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 anonymous prepaid/gift cards: they must not be reloadable and are subject to balance (and, therefore, also transaction) limits of EUR 150 [73]. In the context of offline CBDCs, such types of restrictions can be enforced by common forms of SEs and TEEs.

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 [18]. In contrast to the previous hypothetical model, this design is of more practical relevance. 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 [94] for critical risk parameters. Therefore, TEEs seem to not confer a significant advantage at this level. If the online ledger is transparent and employs no privacy-enhancing technologies, then this model 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 [18], [63], 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, and can be stored on the local storage of the device. Just as with the earlier scenario, real-time transactions screening will not be possible. Thus, the AML/CFT compliance mechanism will be limited to the basic transaction limits and identity verification from locally stored thresholds, credentials, and KYC certificates (see Fig. 5). In this context, *all-or-nothing non-transferability* plays an essential role [18], 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, arguably this alone may not deter active sharing. This is especially true when considering the numerous

		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	×	×	×	×	✓
	Sanctions screening	×	✓	✓	✓	✓
Technologies	SE	✓	✓	✓	×	×
	TEE	×	✓	✓	✓	✓
	ZKP	×	✓	✓	⁄	⁄
	MPC	×	×	×	✓	✓
	Blind singatures	×	×	×	×	✓

Fig. 6: Offline design models for privacy and AML/CFT compliance

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 [95]. This form of identification and authentication heightens both the drawbacks of passing the device and the accountability risks for actions associated with this identity [18]. Therefore, to mitigate device sharing risks, the verification of access to a corresponding digital identity in offline payments (via SEs or TEEs) is beneficial, potentially coupled with occasional revocation checks. If integration with sanctions lists is desirable, ZKPs could be used to produce proofs of non-membership in publicly available lists while preserving users' privacy by not revealing their identifier in the list [62].

C. Hybrid: Intermittently Offline and High Privacy

As outlined in Sec. III, this model ('Intermittently Offline I' in Fig. 6) for offline CBDC transactions necessitates the 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 enabled by the *periodic* access to real-time data from both offline and online sources. This 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 SEs, 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 enforcing time-based mandatory synchronization with TEEs.

Financial sanctions lists can be implemented in the same fashion as above using ZKPs, but with the addition of non-publicly available (e.g., institution-specific) watchlists that are periodically obtained and securely stored by a TEE, which in turn will produce an attestable cryptographic proof that the user of the device is not included in the list. Lastly, the periodic synchronization with an online ledger can mitigate the risks from known attack vectors against secure hardware in what can be considered a "two-factor approach". This approach transmits additional data to the receiver that ensures that a double-spending user can be identified after both conflicting recipients have synchronized the next time. By using ZKPs, it is possible to provide evidence that this additional information is authentic without compromising the sender's privacy guarantees [10].

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* made possible by access to real-time data from both online and offline sources when online. 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 sufficient. Regarding the technology stack that can be leveraged in this scenario, we note that transaction monitoring also 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, the latter may emerge as a more apt solution.

A commonly discussed solution for privacy-preserving transaction graph analysis is the deployment of MPC/FHE [59], [60], [64], [96]. Bank accounts can be represented as nodes in a graph and transactions between them as directed edges. Banks can then use this graph to execute certain algorithms for detecting illicit activities. Commonly, each bank only has a local partial view of the graph, and due to commercial and/or privacy reasons [59], [64], sharing its part of the graph with other banks is not desirable, thus necessitating the use of MPC. Such solutions usually involve a limited number of institutions, that have access to high-performance hardware, as the participants of the protocol. On the contrary, in the context of offline CBDCs, numerous participants hold devices with limited computational capabilities that are in general not online at the same time. Hence, such solutions may not be feasible as the complexity of MPC protocols grows quickly with the number of participating parties. Also, since MPC requires eventual participation from all the parties, even if FHE-based MPC protocols are used to minimize the degree of interactiveness, the protocol can only be executed after all the parties have synchronized with the bank. This seems to severely limit the potential applications of MPC for suspicious transaction detection in the context of CBDCs.

However, MPC could be used by the banks distributing the CBDC to update their internal risk databases that they may keep about their customers. More specifically, banks may categorize clients into different AML/CFT risk levels based on a variety of data points, such as transaction data, possibly requiring stricter due diligence procedures or lower offline functionalities for riskier levels. To update this score, the bank would need to access and process users' private transaction information (e.g., participants, location, etc.) that would be subsequently combined with other data the bank may hold. To ensure that customers' data remains private, an MPC protocol could be employed between the two transacting parties and the bank to be executed after both devices have been synchronized with the online system. However, also for such a system to be able to reach its full potential, frequent synchronizations (or even automatic ones as soon as network connectivity is restored) would be necessary.

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 behavior is observed by the system. The transaction would be logged in the online system and flagged for further inspection. In case a regulatory offense 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 during the next synchronization process. 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.

However, in cases where one-sided anonymity is acceptable, blind signatures could be considered as an alternative, cryptography-based solution to TEEs in implementing a staged offline model since they cannot be immediately respent by the receiving party without online settlement. In this way, the requirement for trust in a manufacturer and devices that integrate a TEE and expose corresponding functionalities to a CBDC application would no longer be necessary. In this approach, double spending detection is performed during the deposit of the funds by the payee. Payment systems based on blind signatures can be designed in a way that if a note is double-spent, the payer can be de-anonymized [51]. As it is assumed that participants undergo KYC, accountability is guaranteed and may act as an additional deterrent to fraudulent behaviors. However, this approach would rely on a centralized settlement layer, or at least some mechanism to discover double-spent notes when multiple operators are responsible for maintaining the settlement infrastructure.

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 practical implementation and evaluation of the proposed design options remain intriguing open issues for future work that will allow for a more thorough examination (e.g., latency measurements) of the performance trade-offs involved in a real-world implementation of an offline CBDC system.

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 the 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 maintaining high privacy standards. Alternatively, one could focus on the cross-border dimension and additional challenges posed by regulatory divergences [16].

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 *beyond the AML/CFT dimension*. By focusing on the interrelation between privacy and AML/CFT considerations, we left out a thorough exploration of broader repercussions, such as implications to monetary policy and central bank law [15]. In addition, specific frameworks tied to financial sanctions, such as those outlined by OFAC and the different financial restrictive measures imposed by the EU, introduce an added layer of complexity. While our paper provides insights into AML/CFT and financial sanctions implications, a more expansive analysis is needed to exhaustively address the diverse 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, regarding the adaptability and resiliency of the proposed framework to new attack vectors, several solutions could be leveraged. First, as described above, thresholds function as a first line of defense that can considerably limit the scope for a new attack that could hypothetically allow an attacker to spend counterfeit money, since the legitimate peers would refuse to accept more than a pre-set amount. Enforcing the expiration or revocation of the user's secure device (and it's replacement with a new one), similar to credit cards, could help ensure that only the latest hardware — offering the highest security possible — is in circulation in the field. In exceptional cases where the discovered vulnerability can be easily replicated, threatening the stability of the system, batch revocations of secure devices targeting a specific manufacturer could be issued. Finally, the security of the framework cannot only be challenged by new attack vectors, but also by emerging technologies, such as quantum computers that could jeopardize the security of the system by directly challenging the cryptography on which it is based. This is aggravated by the fact that updating hardware such as SEs and TEEs in the field to address such issues can be challenging and needs to be explicitly foreseen in the design process.

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 and compliance. Specifically, we provide a classification of privacy design options and corresponding technical building blocks for offline CBDCs. By leveraging secure hardware technologies, such as SEs and TEEs, and cryptographic protocols, such as ZKPs and MPC, smarter versions of cash are achievable. They cater to end-user privacy and also enable a wide array of regulatory controls to combat illicit activities traditionally associated with cash. Further, the increased availability of regulatory control mechanisms allows for higher and more flexible limits.

Our findings reveal that supporting offline transactions introduces additional degrees of freedom to the privacy design options of CBDCs. In line with findings for online CBDC solutions [18], a fully offline CBDC appears to maximize privacy but compromises transaction monitoring and other essential risk management approaches. 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 transparency, including the detailed reporting of offline payments to the online ledger during 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 severely 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, and pointing to potential pitfalls and corresponding mitigations. 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) and Yaya Fanusie (Center for a New American Security and former CIA counterterrorism analyst). The contributions of Nadia Pocher and Johannes Sedlmeir were funded by 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. We are also grateful for the support by Banque et Caisse d'Épargne de l'État, Luxembourg (Spuerkeess). 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] S. Allen, S. Čapkun, 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," 2020. [Online]. Available: https://www.nber.org/papers/w27634

[5] 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/

[6] B. J. Tan, "Central bank digital currency and financial inclusion," *Journal of Macroeconomics*, vol. 81, p. 103620, Sep. 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0164070424000351

[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] K. Attarde, C. Jaiswal, R. Khatwani, G. Pinto, and V. Kumar, "A novel central bank digital currency framework design for offline and foreign transactions based on blockchain," *Digital Policy, Regulation and Governance*, vol. 27, no. 2, pp. 201–220, Jan. 2025.

[10] C. Beer, S. Zingg, K. Kostiainen, K. Wüst, V. Capkun, and S. Capkun, "Payoff: A regulated central bank digital currency with private offline payments," 2024. [Online]. Available: https://arxiv.org/abs/2408.06956

[11] M. Christodorescu, W. C. Gu, R. Kumaresan, M. Minaei, M. Ozdayi, B. Price, S. Raghuraman, M. Saad, C. Sheffield, M. Xu, and M. Zamani, "Towards a two-tier hierarchical infrastructure: An offline payment system for central bank digital currencies," 2020. [Online]. Available: https://arxiv.org/abs/2012.08003

[12] 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

[13] 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

[14] A. Cupak, P. Gertler, D. Hajdiak, J. Klacso, and Š. Rychtárik, "Survey of potential users of the digital euro: New evidence from Slovakia," 2024, National Bank of Slovakia Occasional paper 2/2024. [Online]. Available: https://nbs.sk/dokument/83315e7e-3523-49e6-a4dc-46b91dcbcdd0/stiahnut/

[15] N. Pocher and A. Veneris, *Central bank digital currencies*. Springer International Publishing, 2022, pp. 463–501. [Online]. Available: https://doi.org/10.1007/978-3-031-07535-3_15

[16] 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

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

[18] 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

[19] 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.

[20] 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.

[21] P. Michalopoulos, O. Olowookere, N. Pocher, J. Sedlmeir, A. Veneris, and P. Puri, "Compliance design options for offline CBDCs: Balancing privacy and AML/CFT," in *2024 IEEE International Conference on Blockchain and Cryptocurrency*. IEEE, May 2024, pp. 307–315.

[22] 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

[23] 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. [Online]. Available: https://doi.org/10.3390/fi13050130

[24] 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

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

[26] "CBDCs: it's time for action," Official Monetary and Financial Institutions Forum, Tech. Rep., Feb. 2025. [Online]. Available: https://www.gi-de.com/corporate/Currency_Technology/Central_Bank_Digital_Currencies/Retail_CBDC/GD-OMFIF-2025-CBDCs-Report.pdf

[27] 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/

[28] 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.

[29] A. Tsareva and M. Komarov, "Retail central bank digital currency design choices: Guide for policymakers," *IEEE Access*, vol. 12, pp. 66 129–66 146, 2024.

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

[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," 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] M. Tunstall, "Smart card security," in *Smart Cards, Tokens, Security and Applications*. Springer US, 2008, pp. 195–228.

[37] T. Roche, "EUCLEAK," Cryptology ePrint Archive, Paper 2024/1380, 2024. [Online]. Available: https://eprint.iacr.org/2024/1380

[38] 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.

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

[40] Samsung eSE SDK. [Online]. Available: https://developer.samsung.com/ese/overview.html

[41] Developers can soon offer in-app NFC transactions using the secure element. [Online]. Available: https://nr.apple.com/dN9S3v5Wt1

[42] 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.

[43] 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.

[44] GlobalPlatform, "Introduction to trusted execution environments," 2018. [Online]. Available: https://globalplatform.wpengine.com/resource-publication/introduction-to-trusted-execution-environments/

[45] 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.

[46] 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

[47] M. Schneider, R. J. Masti, S. Shinde, S. Capkun, and R. Perez, "SoK: Hardware-supported trusted execution environments," May 2022.

[48] 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.

[49] D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Boston, MA: Springer US, 1983, pp. 199–203.

[50] ——, "Privacy protected payments: Unconditional payer and/or payee untraceability," in *Smart Card 2000: Second International Smart Card 2000 Conference*. New York, NY: Elsevier Science, 1989, pp. 69–93.

[51] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash," in *Advances in Cryptology — CRYPTO' 88*, S. Goldwasser, Ed. New York, NY: Springer New York, 1990, pp. 319–327.

[52] 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.

[53] M. Babel and J. Sedlmeir, "Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs," 2023. [Online]. Available: https://arxiv.org/abs/2301.00823

[54] N. Bitansky, R. Canetti, A. Chiesa, and E. Tromer, "From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again," in *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*. ACM, 2012, pp. 326–349.

[55] P. L. Barreto and G. H. Zanon, "Blind signatures from zero-knowledge arguments," Cryptology ePrint Archive, Paper 2023/067, 2023. [Online]. Available: https://eprint.iacr.org/2023/067

[56] 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

[57] F. Tramèr, D. Boneh, and K. Paterson, "Remote Side-Channel attacks on anonymous transactions," in *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, pp. 2739–2756. [Online]. Available: https://www.usenix.org/conference/usenixsecurity20/presentation/tramer

[58] 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.

[59] D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography*, Jan. 2023. [Online]. Available: https://toc.cryptobook.us/

[60] A. Ozdemir and D. Boneh, "Experimenting with collaborative zk-SNARKs: Zero-Knowledge proofs for distributed secrets," in *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Aug. 2022, pp. 4291–4308. [Online]. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/ozdemir

[61] N. P. Smart, "Practical and efficient FHE-based MPC," in *19th IMA International Conference on Cryptography and Coding*, Dec. 2023, pp. 263–283.

[62] T. Barbereau, E. Ermolaev, M. Brennecke, E. Hartwich, and J. Sedlmeir, "Beyond a fistful of tumblers: Toward a taxonomy of Ethereum-based mixers," in *Proceedings of the 44th International Conference on System Sciences*. AIS, 2023. [Online]. Available: https://aisel.aisnet.org/icis2023/cyber_security/cyber_security/13/

[63] K. Wüst, K. Kostiainen, N. Delius, and S. Capkun, "Platypus: A central bank digital currency with unlinkable transactions and privacy-preserving regulation," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*, 2022, pp. 2947–2960.

[64] M. B. van Egmond, V. Dunning, S. van den Berg, T. Rooijakkers, A. Sangers, T. Poppe, and J. Veldsink, "Privacy-preserving anti-money laundering using secure multi-party computation," Cryptology ePrint Archive, Paper 2024/065, May 2024. [Online]. Available: https://eprint.iacr.org/2024/065/20240530:123039

[65] T. Barbereau, L. Weigl, and N. Pocher, *Financial Regulation, Political Context, and Technology in the European Union*. Springer Nature Switzerland, 2024, pp. 19–46. [Online]. Available: https://doi.org/10.1007/978-3-031-66047-4_2

[66] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation)," https://eur-lex.europa.eu/eli/reg/2016/679/oj, Official Journal of the European Union, L 119, 4 May 2016, pp. 1-88.

[67] K. P. Murphy, T. Sun, Y. S. Zhou, N. Tsuda, N. Zhang, V. Budau, F. Solomon, K. Kao, M. Vucinic, and K. Miggiani, "Central bank digital currency data use and privacy protection," International Monetary Fund, Tech. Rep. 2024/004, Aug. 2024. [Online]. Available: https://www.imf.org/en/Publications/fintech-notes/Issues/2024/08/30/Central-Bank-Digital-Currency-Data-Use-and-Privacy-Protection-554103

[68] 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

[69] R. Lamberty, D. Kirste, N. Kannengießer, and A. Sunyaev, "HybCBDC: A design for central bank digital currency systems enabling digital cash," *IEEE Access*, vol. 12, pp. 137 712–137 728, 2024.

[70] M. Riccardi and M. Levi, "Cash, crime and anti-money laundering," in *The Handbook of Criminal and Terrorism Financing Law*. Palgrave Macmillan, 2018.

[71] 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.

[72] Financial Action Task Force (FATF), "International standards on combating money laundering and the financing of terrorism & proliferation: The FATF recommendations," 2012. [Online]. Available: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf

[73] "Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing," https://data.europa.eu/eli/reg/2024/1624/oj, Official Journal of the European Union, L series, 19 June 2024.

[74] 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.

[75] 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.

[76] B. Brodsky, A. Dubey, and D. Tercero Lucas, "Enabling offline payments in an online world. Scalability," 2023. [Online]. Available: https://www.lipisadvisors.com/whitepapers

[77] ——, "Enabling offline payments in an online world. Interoperability," 2023. [Online]. Available: https://www.lipisadvisors.com/whitepapers

[78] A. Poller, U. Waldmann, S. Vowé, and S. Türpe, "Electronic identity cards for user authentication – promise and practice," *IEEE Security & Privacy*, vol. 10, no. 1, pp. 46–54, 2012.

[79] Sveriges Riksbank, "E-krona pilot Phase 4," Mar. 2024. [Online]. Available: https://www.riksbank.se/globalassets/media/rapporter/e-krona/2024/e-krona-pilot-phase-4.pdf

[80] 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.

[81] S. Tosza, "Enforcement of international sanctions as the third pillar of the anti-money laundering framework. An unannounced effect of the AML reform and the Sanctions Directive," *New Journal of European Criminal Law*, vol. 15, no. 3, pp. 336–356, aug 2024.

[82] G. Powers, "Reconsidering economic sanctions," in *Soft War*, M. L. Gross and T. Meisels, Eds. Cambridge University Press, 2016, pp. 151–174. [Online]. Available: https://www.cambridge.org/core/books/soft-war/reconsidering-economic-sanctions

[83] 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

[84] 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.

[85] J. Kokott and C. Sobotta, "The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR," *International Data Privacy Law*, vol. 3, no. 4, pp. 222–228, Nov. 2013. [Online]. Available: https://doi.org/10.1093/idpl/ipt017

[86] C. Nyst and T. Falchetta, "The right to privacy in the digital age," *Journal of Human Rights Practice*, vol. 9, pp. 104–118, 2017.

[87] European Data Protection Board and European Data Protection Supervisor, "EDPB-EDPS joint opinion 02/2023 on the proposal for a regulation on establishing the digital euro," Feb. 2023. [Online]. Available: https://www.edps.europa.eu/system/files/2023-10/edpb_edps_jointopinion_digitaleuro_en_0.pdf

[88] 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.

[89] A. Cavoukian, "Privacy by design," *Office of Information and Privacy Communication*, 2011.

[90] K. Yeung, "'Hypernudge': Big Data as a mode of regulation by design," *Information, Commumcation & Society*, vol. 20, no. 1, pp. 118–136, 2017.

[91] 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

[92] R. Anderson, J. Spring, R. Clayton, and A. Hutchings, "Taking the crime out of cybercrime: Theory and policy implications," *Journal of Cybersecurity*, vol. 7, no. 1, p. tyab004, 2021. [Online]. Available: https://academic.oup.com/cybersecurity/article/7/1/tyab004/6166133

[93] 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.

[94] GlobalPlatform, "Confidential card content management," 2019. [Online]. Available: https://globalplatform.org/specs-library/confidential-card-content-management-amendment-a-v1-2/

[95] 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.

[96] F. Effendi and A. Chattopadhyay, "Privacy-preserving graph-based machine learning with fully homomorphic encryption for collaborative anti-money laundering," in *Security, Privacy, and Applied Cryptography Engineering*. Springer, 2025, pp. 80–105.

Panagiotis Michalopoulos is a Ph.D. candidate at the Department of Electrical and Computer Engineering of the University of Toronto, Canada. He received an M.Sc. in Embedded Systems from the Eindhoven University of Technology, The Netherlands and a Diploma in Electrical and Computer Engineering from the University of Patras, Greece. His research focuses on privacy preserving and regulation compliant offline Central Bank Digital Currencies and on the secure hardware technologies to implement them. Other research interests include identity and trust systems and their applications on the Internet of Things.

Odunayo Olowookere is a doctoral candidate at Osgoode Hall Law School, York University. His research examines the legal foundations of money, particularly as they relate to monetary law, the administration of monetary policy, and the central banks' role in an evolving financial and monetary system. He focuses on how virtual currencies and digital assets challenge established legal concepts and institutional arrangements in finance. Odunayo's work critically engages with the legal and regulatory frameworks needed to support Central Bank Digital Currencies (CBDCs). More broadly, he explores how legal systems can adapt to financial innovation while maintaining essential public policy goals, including data governance, financial security, and systemic stability. His research aims to bridge legal theory with the practical demands of regulating digital finance in a rapidly changing global economy. In addition to his academic work, Odunayo has advised tech startups and financial service providers on a range of legal and regulatory issues.

Nadia Pocher is a postdoctoral researcher at the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, and affiliated researcher at the FutureFinTech National Centre of Excellence in Research & Innovation. She received her Ph.D. in Law, Science and Technology, excellent cum laude, from the University of Bologna, the Autonomous University of Barcelona and K.U. Leuven. In her research at the intersection of computer science and law, she focuses on the regulation and compliance of emerging technologies in the financial space, through the lens of the information systems discipline. Her interests include anti-money laundering and counter-terrorist financing in crypto-assets and decentralized finance, as well as blockchain analytics, central bank digital currencies and compliance by design. Her research has been published in international journals such as Electronic Markets and IEEE Transactions on Network and Service Management (TNSM), edited books such as Springer's Handbook on Blockchain, and conferences such as IEEE Conference on Blockchain and Cryptocurrency (ICBC) and the Atlantic Council's Forum on US-European GeoEconomics.

Johannes Sedlmeir is an acting professor of statistics, security & trust at the University of Münster's information systems department. He previously worked as a research associate (PostDoc) at the Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg and as a researcher at Fraunhofer FIT. He received his M.Sc. in Theoretical and Mathematical Physics from LMU and TU Munich and holds a Ph.D. in information systems engineering from the University of Bayreuth. In his research, Johannes focuses on the affordances of emerging digital technologies to enhance security and trust when processing data within and across organizations. He does so by designing innovative IT artifacts based on technical building blocks such as blockchains, digital identity attestations, and zero-knowledge proofs. Johannes has published his research in leading international journals such as Business & Information Systems Engineering (BISE), Electronic Markets (EM), Information & Management (I&M), Information Systems Journal (ISJ), Joule, and the Journal of the Association for Information Systems (JAIS).

Andreas Veneris is a Connaught Scholar and Professor at the Department of Electrical and Computer Engineering, cross-appointed with the Department of Computer Science at the University of Toronto. He obtained a Ph.D. from the University of Illinois, Urbana-Champaign. In the past, he held joint faculty positions with the Athens University of Economics and Business (2006-16) and with the University of Tokyo (2010-11). For 20 years he worked in CAD for VLSI synthesis, verification and debugging using formal methods. Today, he focuses on Central Bank Digital Currencies (CBDCs), mechanism/economic design of distributed systems, formal methods for smart contract verification, and techno-legal blockchain policy/regulatory questions. He has received a 10-year Best Paper Retrospective Award and five other best paper awards. He was a member of the team in the first webcast ever (37th Grammy Awards, 1995), an event acknowledged by the American Congress. In 2021 his work with the Bank of Canada became public, proposing Canada's Central Bank Digital Loonie with a comprehensive technological, regulatory/legal and economic model for a CBDC. In 2022 he was acknowledged for his contributions on the report titled "Digital Currencies: The US, China, And The World At A Crossroads" by the Hoover Institution and prefaced by former United States Secretary of State Condoleezza Rice. A week later President Joe Biden signed an Executive Order following many of its recommendations. His work has been featured in publications by the IMF and BIS, among other.

Poonam Puri is Full Professor of Law and the York Research Chair in Corporate Governance, Investor Protection and Financial Markets at Osgoode Hall Law School, York University in Toronto, Canada. She is internationally recognized for her expertise in corporate law, corporate governance, and the regulation of securities and financial markets. A silver medalist from the University of Toronto Faculty of Law and an LL.M. graduate of Harvard Law School, Professor Puri has led and participated in numerous interdisciplinary research initiatives, including research on Central Bank Digital Currencies in collaboration with researchers from the University of Toronto and the Bank of Canada. Professor Puri's contributions have been recognized with numerous honours, including the Order of Ontario, the Fellowship Award from the Institute of Corporate Directors, a Pierre Elliott Trudeau Foundation Fellowship, the Royal Society of Canada's Yvan Allaire Medal, the Law Society of Ontario's Law Society Medal, and the David Walter Mundell Medal for legal writing. She has twice been named one of Canada's Top 25 Most Influential Lawyers and is a recipient of Canada's Top 40 Under 40 Award.