IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 18 June 2024, accepted 19 August 2024, date of publication 11 September 2024, date of current version 2 October 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3458451

RESEARCH ARTICLE

HybCBDC: A Design for Central Bank Digital Currency Systems Enabling Digital Cash

RICKY LAMBERTY[1,2], DANIEL KIRSTE[1,3], NICLAS KANNENGIEßER[3,4], AND ALI SUNYAEV[3,4], (Member, IEEE)

[1]Robert Bosch GmbH, 70442 Stuttgart, Germany
[2]Research Center Digital Science, German University of Digital Science, 14482 Potsdam, Germany
[3]Karlsruhe Institute of Technology, 76131 Karlsruhe, Germany
[4]KASTEL Security Research Labs, 76131 Karlsruhe, Germany

Corresponding author: Ricky Lamberty (ricky.lamberty@bosch.com)

This work was supported by the KASTEL Security Research Labs.

ABSTRACT Central Bank Digital Currencies (CBDCs) have the potential to increase the financial reliability of digital payment systems by offering direct interactions between payment system participants, including institutional and private ones. To unfold the potential of CBDCs, CBDC systems need to offer confidential payments to protect participants from surveillance. However, confidential payments lay at odds with requirements for transparency of payments in CBDC systems to enforce regulations, such as anti-money laundering (AML) and countering the financing of terrorism (CFT) regulations. This work presents HybCBDC, a CBDC system design that tackles the tension between confidential payments and the enforceability of regulations. We iteratively refined HybCBDC in three rounds of focus group interviews with finance and industry experts. HybCBDC offers cash-like confidential payments and means to enforce regulations. HybCBDC builds on a hybrid access model for using monetary items of a CBDC and combines an account-based and an unspent transaction output (UTXO)-based subsystem to record payments. The main purpose of this work is to support the design of CBDC systems that can tackle the tension between offering payments with cash-like confidentiality while allowing for enforcement of regulations related to AML and CFT.

INDEX TERMS Central bank digital currency (CBDC), confidential payments, digital cash, distributed ledger technology (DLT), privacy enhancing technologies (PETs).

I. INTRODUCTION

While offering valuable services to individuals (e.g., offering mortgage loans for purchasing services), commercial banks bear financial risks to the reliability of commercial bank money. For example, commercial banks can go bankrupt, as Lehman Brothers did in the financial crisis 2009 [1]. To decrease such financial risks, the idea of digital payment systems offering participants the option to make direct claims to central banks arose [2]. Various efforts were made in research and practice to better understand how central banks can issue and manage Central Bank Digital Currencies (CBDCs) in digital payment systems called CBDC systems [3]. CBDC systems have the potential to augment existing central bank systems by supporting more streamlined payment processes and micro-payments [4], [5].

Notwithstanding the potentials of CBDC [6], [7], CBDC systems come with challenges. A prominent challenge originates from the fact that CBDC systems can empower central banks to gain access to histories of digital payments of institutional and private payment system participants [8]. Through such access, central banks can be enabled to surveil payments of even private participants [9]. This can form a foundation for excluding payment system participants, such as dissident individuals, and erode confidentiality in CBDC systems. To mitigate surveillance-related risks, confidential payments inherently anchored in CBDC systems are paramount [10].

The associate editor coordinating the review of this manuscript and approving it for publication was Barbara Guidi.

In CBDC systems, confidential payments refer to payments where transaction details (e.g., identities of senders and receivers, transaction dates, and transferred amounts) are only visible to senders and receivers [11]. To enable confidential payments, a digital equivalent to physical cash (i.e., digital cash) seems reasonable [12]. Physical cash can be used for confidential payments because payments are executed offline and peer-to-peer. Amounts are only known to payers and payees. Moreover, parties do not need to disclose their identities in payments using cash [13]. No third party should be able to surveil digital payments that offer cash-like confidentiality.

Although promising to mitigate surveillance, cash-like confidential payments can complicate enforcement of regulatory mandates, such as the 5th EU Anti-Money Laundering Directive (AMLD5), US Anti-Money Laundering Act (AMLA), and Countering the Financing of Terrorism (CFT). Stringent controls over digital payments may not be possible in CBDC systems that offer cash-like confidentiality because transaction information required for such controls cannot be extracted [14].

Under careful consideration of requirements for confidential payments and regulatory compliance, various CBDC system designs were proposed (e.g., [15], [16], [17]). However, while focusing on confidential payments, extant CBDC systems (e.g., [18], [19], [20]) often fall short in simultaneously meeting requirements for regulatory compliance. For example, with a focus on confidential payments, CBDC system designs were presented that build on privacy-enhancing technologies (PETs), such as zero-knowledge proofs (ZKPs) and blind signatures (e.g., [15], [21]). Those CBDC system designs offer valuable approaches to support confidential payments. Still, they are unsuited for enforcing regulations, such as those related to anti-money laundering (AML) and countering the financing of terrorism (CFT). To support development of CBDC systems that offer both confidential payments and allow for enforcement of AML and CFT, we approach the following research question: *What is a CBDC system design that offers confidential payments on par with physical cash while allowing for enforcement of regulations related to AML and CFT?*

We developed HybCBDC, a hybrid CBDC system design that combines an account-based and an unspent transaction output (UTXO)-based subsystems to offer cash-like confidential payments and allow for enforcement of regulations related to AML and CFT. We developed and iteratively refined HybCBDC in three steps. First, we developed a requirements catalog for CBDC systems with a focus on confidential payments (e.g., amount obfuscation, sender-receiver unlinkability) and regulatory compliance (i.e., AML and CFT). Second, based on the requirements catalog, we developed an initial version of HybCBDC. Third, we refined HybCBDC in three iterations with nine experts in distributed ledger technology (DLT) and finance from the industry.

The main purpose of this work is to support development of CBDC systems that offer confidential payments while allowing for the enforcement of regulations related to AML and CFT. In particular, this work has three main contributions. First, by presenting a set of confidentiality characteristics of cash, we support a granular understanding of the requirements for cash-like confidential payments in CBDC systems. This is useful to guide design of CBDC systems that support confidential payments. Second, by showing how the combination of an account-based subsystem (e.g., transaction transparency [22]) and a UTXO-based subsystem (e.g., unlinkability of transactions for third parties [23]) can be leveraged in CBDC systems, we support development of CBDC systems that enable digital payments with cash-like confidentiality. Third, we support design of CBDC systems by presenting HybCBDC. HybCDBC showcases a CBDC system design offering digital payments with cash-like confidentiality while allowing for compliance checks and audits as required by law.

The remainder of this work is structured into five sections. First, we explain the foundations of CBDC systems and cash characteristics that are relevant to the development of HybCBDC. Moreover, we offer an overview of related works on CBDC system designs. Second, we describe how we proceeded in the development of HybCBDC. Third, we present HybCBDC with a focus on its architecture and main functionalities. Moreover, we argue about the extent to which HybCBDC can meet those requirements. Fourth, we discuss our principal findings, describe the contributions and limitations of this work, and outline future research directions. We conclude with a short summary of this work in section VI.

II. BACKGROUND AND RELATED WORK

The following describes foundations of CBDCs, cash and DLT for understanding the key concepts and related research relevant to our study. Important aspects of CBDCs, such as access models and account models, are described and mapped to design options. Additionally, cash characteristics are described to point out important aspects of monetary items important in development of CBDC systems, such as HybCBDC (see section IV). Last, we outline the use of DLT and privacy-enhancing technologies (PETs) in CBDC system designs and how those technological building blocks can enhance confidentiality in digital payment systems.

A. CENTRAL BANK DIGITAL CURRENCIES

CBDCs are envisioned to complement, not substitute, existing monetary items [24]. CBDCs comprise digital monetary items issued by central banks in CBDC systems. CBDC systems are digital payment systems mainly administrated by central banks [2]. In CBDC systems, participants (e.g., individuals and organizations) can transfer digital representations of monetary items (i.e., tokens) of CBDCs.

Compared to conventional central bank reserves (e.g., government securities and reserve deposits) that are only accessible by commercial banks, monetary items of CBDCs can be accessed and used by various payment system participants, including commercial banks, financial authorities, and individuals. By offering access to monetary items of CBDCs to a wide variety of payment system participants, participants can facilitate transaction settlement and decrease transaction costs of financial services [25].

Extant CBDC systems, such as those in which the *Chinese Digital Currency Electronic Payment* [26] and *Swedish e-krona* [27] are operated, differ in their main purposes, access models, and account models. Those differences are described in the following.

a: CBDC MAIN PURPOSES

The main purposes of CBDC systems are to support retail and wholesale [9]. CBDC systems for retail offer digital payments that can be used by the general public, for example, for transactions between private buyers and sellers [6]. The central bank is responsible for handling retail transactions and recording retail balances [3].

CBDC systems for wholesale enable transactions between financial institutions (e.g., commercial banks) are in focus. Central banks account for issuing monetary items of CBDCs, recording wholesale balances, and verifying transactions between financial institutions [16]. Confidential payments are less critical for wholesale because financial institutions are subject to stringent regulatory scrutiny.

b: ACCESS MODELS

CBDC systems can offer *direct*, *indirect*, and *hybrid access* to monetary items of a CBDC [17]. Such access models define how monetary items of a CBDC are issued and how participants can use monetary items represented in the form of digital tokens in a CBDC system (e.g., for payments). In *direct access* models, monetary items of a CBDC represent a direct claim on a central bank, and the central bank processes payments and records retail holdings. Participants can directly transfer monetary items of CBDCs.

In CBDC systems with *indirect access* models, monetary items of a CBDC represent a claim against intermediaries (e.g., commercial banks). Claims against commercial banks represent commercial bank money and are liabilities of private financial institutions, not issued by central banks. Thus, commercial bank money is private debt and bears counter-party risks [28].

CBDC systems with *hybrid access* models offer direct claims on central banks to participants while intermediaries (e.g., commercial banks or payment service providers) handle payments. A central bank retains a copy of all retail CBDC holdings, allowing transfers of holdings from one payment service provider to another in the event of technical failure [17].

c: ACCOUNT MODELS

There are two principal account models to record balances of payment system participants [29], [30]: Account-balance and UTXO models.

Account-balance models record participants' balances directly in individual accounts, similar to conventional online banking systems and the Ethereum system.

Unspent transaction output (UTXO)–based models do not use a single account per participant to record balances. Instead, UTXO-based account models rely on a kind of 'safe' (i.e., UTXOs) that store monetary items represented as tokens. Existing UTXOs need to be unlocked to spend monetary items. Upon unlocking, transferred monetary items are locked in new UTXOs that can only be unlocked by receivers of transferred monetary items, which enables a change in ownership of monetary items [31]. Monetary items locked in a UTXO can only be spent if the correct secret (e.g., a private key) is proved. Participants generate and store a new secret for each UTXO that locks monetary items they own.

In the UTXO model, a participant's total balance is calculated by summing up the UTXOs for which the participant owns the secret. Because UTXOs do not necessarily reference receiver addresses, it is difficult to reconstruct payment senders and receivers. Thus, UTXO models commonly offer more confidentiality than account-balance ones [21]. To reach UTXO-like unlinkability in account-balance models, participants need to create new accounts for transactions.

To link digital payments to participants in CBDC systems using account-balance and UTXO models, metadata, such as participants' IP addresses, need to be gathered and analyzed. Various valuable countermeasures, such as mixing protocols [32], [33], are available to enhance unlinkability of digital payments. However, approaches to map digital payments to payment system participants based on cyber-observables and corresponding countermeasures are not in the scope of this work.

B. CASH CHARACTERISTICS

Monetary items can differ in their characteristics, such as risk-neutrality and permanence, and can be grouped in *value* and *access*. The group of *value* covers characteristics that refer to universal acceptance and fungibility. The monetary item must be *risk-neutral* to be universally accepted for payments. Moreover, it must be *uniform* to ensure the fungibility of the monetary items [12].

The group of *access* refers to characteristics that impact the secure use of monetary items. Payments are when no payment information is disclosed to unauthorized third parties [34]. To protect private payment system participants from surveillance, monetary items must be *confidentiality-preserving* [12]. Moreover, monetary items must be *inclusive* for cheap, easy use without specific knowledge. Monetary items shall be utilized *efficiently* for handling retail payments. Monetary items must preserve *integrity* that they cannot be changed by unauthorized third parties. Monetary items must offer a *persistent* store of value.

Monetary items can be intangible, for example, in the form of digital tokens used in the Bitcoin and Ethereum systems, in the cases of commercial bank money, and in CBDCs [35]. Monetary items can be tangible [12], such as

TABLE 1. Characteristics of monetary items and digital payment systems (adapted from [12]).

Category	Characteristic
Value	**Risk-neutrality:** The level to which a monetary item is free from counter-party risks.
	Uniformity: The extent to which a monetary item is fungible.
Access	**Confidentiality:** Information related to transactions that involve a monetary item is protected from unauthorized access.
	Efficiency: Transaction processing is scalable, instant, and at low (or even none) transaction costs.
	Inclusiveness: Every payment system participant can equally use a monetary item.
	Integrity: The value of a monetary item cannot be changed through unauthorized parties.
	Permanence: The extent to which a monetary item is a persistent store of value.
	Tangibility: A monetary item can be perceived by touch.

cash (i.e., banknotes and coins), that represent direct claims to central banks in many jurisdictions [36].

Cash has benefits over intangible monetary items, such as being universally used as legal tender in many jurisdictions worldwide [36]. Cash is issued by central banks and, thus, risk-neutral for respective jurisdictions. Holders do not face counter-party risks, in contrast to holding commercial bank money, which represents private debt obligations of financial institutions [28]. Integrity is given since cash notes cannot be changed by third parties. Banknotes and coins are standardized and have uniform values to ensure the fungibility of cash.

Cash can be considered efficient for offline payments because it can be physically handed over from the payer to the payee in real time without incurring transaction fees, particularly when both parties are in the same geographical location. Inclusiveness of cash is given because cash is a physical item that everybody can carry.

Cash keeps its value and thus is persistent due to its stability provided by government backing. In addition, the tangibility of cash ensures independence from critical infrastructures, allowing them to compensate for faults and preserving their usability and worth in various circumstances (e.g., power cut) [37].

Most importantly, in this work, cash is confidentiality-preserving because payments are performed offline without leaving traces. Thus, transaction amounts, sender, and receivers are only known to payers and payees, while both parties do not have to reveal their identities, enabling confidential transactions [13].

Illicit transactions can be performed using tangible and intangible monetary items [38]. Enforcing regulations seems inherently more challenging with cash transactions than with intangible ones. This difficulty arises because tangible items, such as cash, can be transferred without leaving a digital trace, making it harder for authorities to monitor and control these transactions. Accordingly, cash seems less suitable to facilitate regulatory compliance by design [39] but has the potential to increase confidentiality of payments.

The presented cash characteristics form a foundation to devise requirements for CBDC system designs that offer confidential payments. Enabling confidential transactions with cash-like characteristics in CBDC systems is paramount. At the same time, other cash characteristics, such as accessibility and convenience, need to be ensured in development of effective and inclusive CBDC systems [10].

C. CBDC MAIN PURPOSES

Many CBDC system designs (e.g., [15], [40], [41]) rely on DLT, including blockchain technology [42]. DLT helps ensure integrity and permanence of monetary items represented as tokens and can enhance inclusion by easy-to-use mobile applications and hardware to store monetary items of a CBDC [43], [44]. At the same time, many DLT systems often fall short in terms of confidential payments [45]. This section describes the potential benefits and drawbacks of using DLT in CBDC systems. Moreover, principal approaches to tackling the drawbacks of using DLT in CBDC systems regarding payment confidentiality are described.

1) DISTRIBUTED LEDGER TECHNOLOGY

DLT enables the operation of distributed ledgers, a type of distributed database, such as those used in the Bitcoin system and blockchain systems based on Hyperledger Fabric [42]. Many DLT-based digital payment systems (e.g., Circle's USDC and Tether's USDT) were designed to enable payments based on intangible monetary items of real-world currencies [46].

DLT is used in CBDC systems for three main purposes. First, DLT can help standardize processes related to digital payments by offering a shared and unified infrastructure that ensures consistency in transaction processing and reconciliation across different payment service providers [8].

Second, DLT systems can record tamper-resistant payment histories for audits to prove regulatory compliance. This can help meet the mandate for anti-money laundering and combating financing terrorism [47], [48].

Third, DLT supports different account models (e.g., for account-balance models and UTXO models) that can be used in CBDC systems to account for substantially different requirements for confidential payments [41]. For example, if accounts are always bound to real-world identities like in traditional banking systems, confidentiality is a constraint.

While increasingly used in digital payment systems, including proposed CBDC systems, DLT introduces challenges. Each node maintains a replica of the ledger in DLT systems based on the replicated state machine concept [42], [49]. Thus, each party with access to such a node can read transaction data, which can compromise payment confidentiality [42]. Insufficient confidentiality of payments can facilitate surveillance and financial exclusion of participants [15], [50]. To benefit from using DLT in CBDC systems while tackling challenges for confidential payments, privacy-enhancing technologies (PETs) can be used to expand DLT protocols in terms of confidential payments [51].

2) ENHANCING PAYMENT CONFIDENTIALITY IN DISTRIBUTED LEDGER TECHNOLOGY SYSTEMS

PETs commonly used in CBDC and payment system designs are blind signatures, mixing protocols, and ZKPs. Such PETs and their uses in CBDC system designs are briefly described below. Moreover, we showcase common benefits and drawbacks of using PETs in digital payment systems and, in particular, CBDC systems.

a: BLIND SIGNATURES

Blind signatures build on the concept of digital signatures based on public/secret key pairs but conceal (i.e., *obscure*) the contents of transactions (e.g., amounts of financial transactions) before signing. The blinded transaction content is sent to a trusted third party (e.g., a financial institution) that signs the transaction without revealing transaction details. The third party verifies the sender's digital signature. This process ensures that the signer (e.g., a financial institution) cannot see the content of the transaction (e.g., a financial transaction) of the sender while verifying its authenticity [52]. After the trusted third party signed the transaction, the sender can unblind the transaction and send the unblinded transaction to the receiver.

Although largely enabling confidential payments, third parties still learn about transactions processed in payment systems using blind signatures [21]. Such (partial) visibility of transactions does not necessarily compromise confidentiality but still does not fully meet requirements for confidential payments. For example, a trusted third party learns the identities of senders initiating transactions.

In short, blind signatures can help to enhance payment confidentiality in digital payment systems [52], particularly by disguising receivers and amounts of payments. However, they still allow third parties to learn about transactions issued by participants that are identifiable for a trusted third party.

b: MIXING PROTOCOLS

Mixing protocols help disguise transaction histories by (randomly) merging and splitting payments in payment systems using the UTXO model to obfuscate senders and receivers of payments [53]. Obfuscating senders, receivers, and amounts helps increase payment confidentiality and makes tracing transaction histories difficult. This can help to achieve a level of confidentiality akin to that of cash while offering benefits of digital payment systems [54], such as convenient, fast, and reliable payments over long distances. However, mixing protocols usually increase complexity in transaction processing and, foremost, introduce challenges related to regulatory compliance with AML and CFT. This is because mixing protocols can be used for illicit activities [32].

In short, mixing protocols can support confidential payments in digital payment systems, including CBDC systems, by obfuscating transaction details. Nevertheless, implementation of mixing protocols requires careful consideration to balance confidentiality needs with regulatory compliance.

c: RING CONFIDENTIAL TRANSACTIONS

Ring confidential transactions implement principles of ring signatures to hide senders and receivers of transactions [55]. Ring confidential transactions disguise the producer (original signatory) of a signature. A set of n possible signatories is used, where only one signatory must sign the transaction. This helps obfuscate the actual signatory of a transaction. The signature can be generated without the approval of other signatories [56]. In ring confidential transactions, the sender uses a commitment to obfuscate the transacted amount. The commitment allows third parties to verify that the sum of inputs and outputs are equivalent while hiding the transferred amount [55].

Ring confidential transactions are a valuable feature for retail CBDC systems to obfuscate transaction histories (e.g., [57]) and enable confidential payments. However, their use can pose a hurdle to achieving regulatory compliance [56], [58].

d: ZERO-KNOWLEDGE PROOFS

ZKPs refer to cryptographic techniques that enable one party to prove to another that a statement is true without revealing information beyond the validity of the statement itself. ZKPs allow validation of the syntactic alignment of transactions without disclosing transaction details to third parties. Information about senders, receivers, and amounts does not need to be disclosed [59]. This makes ZKPs suitable for offering confidential payments [60].

In the Zerocoin system [61], for example, transaction amounts are concealed and verified using Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zkSNARK) without disclosing transaction data to unauthorized parties [23]. While effective in enabling confidential payments, use of (non-interactive) ZKPs can present challenges regarding standardization and detecting software vulnerabilities [42], [62], [63]. Moreover, proposed CBDC system designs built on ZKPs tend to be subject to challenges related to enforcing turnover limits [64] and compliance with regulations related to AML and CFT [65].

Blind signatures in combination with zkSNARK can help obfuscate sender information [21]. While sender anonymity can be enhanced, transparency of transactions allows for inferring a receiver's identity through transaction patterns and linkage analysis [66]. Thus, surveillance-related concerns cannot be fully resolved for all parties involved in transactions [67].

Another CBDC system design [15] envisioned to enable confidential payments uses ZKPs. Payment system participants have their own CBDC accounts and can prove correct accounting based on zkSNARK to institutional payment system participants [15]. That CBDC system design helps achieve regulatory compliance and offers an approach for confidential payments. However, zkSNARKs are not yet feasible at scale for CBDC systems due to insufficient operational readiness and missing standards [62], [63].

In short, ZKPs can enhance confidentiality and security. However, they are often complex to develop and can entail high computational costs [62].

Overall, the requirement for confidential payments is at odds with regulatory compliance requirements. Extant CBDC system designs hardly enable confidential payments and regulatory compliance at the same time. To meet requirements for confidential payments and regulatory compliance, CBDC systems should be compliant-by-design. Confidential payments should only be possible in contexts that do not allow for activities violating regulations. This hints at the need for offering enforcement of regulatory compliance through the design of technical systems [65], [68]. Offering the possibility for such enforcement and confidential payments is the principal design goal in the development of HybCBDC.

III. METHODS

The goal of this work is to develop a CBDC system design, HybCBDC, that reconciles with the prevalent financial system and offers confidential payments to participants. We developed HybCBDC in three steps. In the first step, we developed a requirements catalog by reviewing extant literature on CBDC and cash characteristics. In particular, we devised key requirements for monetary items with a focus on confidential payments and prominent legal regulations (i.e., AML and CFT) in financial systems. In the second step, based on the requirements catalog, we developed an initial version of HybCBDC. In the third step, we conducted semi-structured focus group interviews with experts in the fields of finance and industry with utmost expertise in CBDC to obtain feedback on HybCBDC. After the interview, we refined HybCBDC according to the feedback we gathered. We repeated step three until the interviewees did not mention further improvements to HybCBDC. In the following, we describe each step in more detail.

A. DEVELOPMENT OF THE REQUIREMENTS CATALOG

We extracted characteristics of monetary items from extant literature to gather requirements for confidential payments for our system design [12]. Next, we contextualized the identified characteristics of monetary items in CBDC systems. To develop key requirements for confidential payments in CBDC systems, we mapped that basic set of transaction information to formal specifications of confidentiality [69]. The confidentiality requirements we devised formed a foundation for the design of HybCBDC.

We consolidated the requirements for confidential payments and for the enforceability of regulations related to AML and CFT in a requirements catalog. The requirements catalog forms the foundation for the subsequent steps of the development of HybCBDC.

B. DEVELOPMENT OF AN INITIAL VERSION OF HYBCBDC

Based on the requirements catalog developed in the previous step, we started the development of HybCBDC by analyzing the structure and mechanisms of established financial systems (e.g., SEPA and TARGET2) by analyzing extant publications in this field. We translated the structure (e.g., relationships between commercial banks and central banks) and mechanisms (e.g., commercial bank money creation) as a blueprint for HybCBDC. Then, we designed a digital payment system that allows for cash-like confidentiality. This digital payment system meets requirements for confidential transactions and forms one of two subsystems of HybCBDC. Subsequently, focusing on supporting the enforceability of regulations related to AML and CFT, we designed a second digital payment system for transparent digital payments, which forms the second subsystem of HybCBDC. Next, we compared different approaches to enable interoperability between the two subsystems, such as centralized and decentralized notaries [70].

Throughout the development process, we documented each version of HybCBDC in detailed architecture, sequence, and activity diagrams. The diagrams were essential in the iterative refinement of HybCBDC in the subsequent step.

C. ITERATIVE REFINEMENT OF HYBCBDC

We conducted three semi-structured focus group interviews to obtain feedback on HybCBDC [71]. To acquire interviewees, we approached potential participants for the focus group interviews through an extensive network of experts with thorough knowledge of the diverse aspects of CBDC systems related to economic, technical, and regulatory domains. The participants in the focus group interviews represent a blend of senior professionals from various industries, including banking, consulting, and industry, enabling a multifaceted analysis with valuable feedback on HybCBDC. Table 2 illustrates the composition of each focus group conducted in this study.

In preparation for the semi-structured focus group interviews, we developed an interview guide [72]. The interview guide was structured into five parts. In the first part, we introduced the interviewees to the research project and obtained their consent to record the interview. In part two, we described the research project and highlighted its relevance for the design of CBDC. In the third part, we clarified the technological background. Then, we presented HybCBDC and details on the confidential transactions in the fourth part. Fifth, we guided a discussion on HybCBDC to collect feedback on the system design. To help the interviewees prepare for the focus group interview, we sent them an overview of the interview guide prior to the focus group interviews.

After each focus group interview, we systematized the gathered feedback to prepare the refinement of HybCBDC [73]. After refining HybCBDC, we updated the interview guide in preparation for the subsequent focus group interview. In total, we conducted three focus group interviews that helped us improve HybCBDC. Each focus group interview took about two hours on average.

The first focus group interview revealed several potentials for refinement of HybCBDC. For example, two interviewees demanded compliance with regulations related to AML. Accordingly, we refined the UTXO-based subsystem to comply with the regulations of the AMLD5 using ring confidential transactions with unique commitments.

In the second focus group interview, the feedback led to refinements of HybCBDC in terms of (1) the AMLD5 regulation using commitments in ring confidential transactions was rated positive and (2) the barriers for large companies to enter the retail layer should be lowered.

In the third focus group interview, the interviewees approved the refined version of HybCBDC. Additionally, the interviewees had two principal ideas for potential future improvements. First, the participants assumed that state channels could improve the scalability of HybCBDC for the account-based subsystem. Second, all interviewees acknowledged the mechanisms used to enable confidential payments in the UTXO-based subsystem. We reached the end condition as the interviewees did not mention additional criticisms and improvements related to HybCBDC.

TABLE 2. Overview of focus group interviewees.

Group	No.	Expertise	Role	Sector
1	1	CBDC, Regulation	Head of Digital Assets	Banking
	2	Economics	Chief Financial Officer	Automotive
	3	Strategy, Economics	Board Member, Strategist	IT Provider
2	4	DLT, AI	Technology Consultant	Consulting
	5	CBDC, Regulation	Co-founder, COO	Consulting
	6	Digitalization, DLT	Digitalization Lead	Automotive
3	7	DLT, Economics	DLT Product Lead	Automotive
	8	DLT, Payment	Senior Manager	Consulting
	9	Economics, DLT	Managing Director	Consulting

IV. HYBCBDC

We developed a CBDC system design, which we call HybCBDC, with a focus on enabling confidential payments and enforceability of regulations related to AML and CFT. This section first introduces the principal requirements for confidential payments and regulatory compliance to be met by HybCBDC. Then, the structure and functioning of HybCBDC are described. Subsequently, we argue to what extent the requirements are met in section IV-A.

A. REQUIREMENTS CATALOG

CBDC systems need to meet four core requirements to offer cash-like confidential payments [69]: *Amount obfuscation*, *balance obfuscation*, *sender and receiver obfuscation*, *sender-receiver third-party unlinkability* and *regulatory compliance*. We describe the requirements in the following.

a: AMOUNT OBFUSCATION

The amount sent in transactions of participants must be obfuscated and unknown to third parties. Only senders and receivers must be able to learn spent amounts. Disclosure of transacted amounts can facilitate profiling (larger) transactions and tracing payments of identities [66].

b: BALANCE OBFUSCATION

Balances of participants must be obfuscated. Unauthorized third parties must not obtain information on the balance of private payment system participants. Disclosure of balances of private payment system participants can facilitate targeted attacks on high-net-worth private payment system participants, discrimination, and loss of financial autonomy [74].

c: SENDER AND RECEIVER OBFUSCATION

Third parties must not be able to learn the real-world identities of senders and receivers involved in confidential transactions. By obfuscating sender and receiver identities through pseudonymization, the ability to trace transactions back to individuals can be effectively eliminated to anticipate surveillance of payments [21].

d: SENDER-RECEIVER THIRD-PARTY UNLINKABILITY

Third parties must not be able to associate senders with recipients of payments. Even if the pseudonyms of senders and recipients are known, the link between them must remain obscure to prevent third parties from learning transactions between payment system participants [69]. Linkability of static identifiers (e.g., pseudonyms) can allow third parties to reveal transaction information. This can increase the risk of exposing relationships, personal preferences, and confidential communication patterns, violating requirements for confidential payments [75].

e: REGULATORY COMPLIANCE

Compliance with regulations related to AML and CFT must be guaranteed. This ensures that while confidential payments are offered, illicit activities must be detectable and preventable in CBDC systems [28]. Meeting this requirement calls for a balance between confidentiality to protect payment system participants from surveillance and transparency to enforce regulations related to AML and CFT in digital payment systems [12].

B. OVERVIEW AND PRINCIPAL FUNCTIONING

HybCBDC is a two-tiered CBDC system design that can be used for retail and wholesale transactions. To fulfill that purpose, HybCBDC comprises two interconnected subsystems: An account-based subsystem that builds on an account-balance account model and a UTXO-based subsystem that uses a UTXO-based account model. Trusted third parties, such as banks, mediate interactions between private payment system participants in the account-based subsystem. Thus, HybCBDC uses an indirect access model that only allows private payment system participants to interact with central banks via institutional payment system providers. HybCBDC uses a direct access model that allows private payment system participants to spend monetary items of CBDC. Due to the use of an indirect and a direct access model, HybCBDC relies on a hybrid access model. The following presents an overview of HybCBDC and its principal functioning. Then, we argue to what extent HybCBDC meets the requirements presented in section IV-A).

1) OVERVIEW

HybCBDC comprises two interconnected subsystems (see Figure 1): An account-based and a UTXO-based subsystem. In the account-based subsystem, various application-specific DLT systems can be operated. The UTXO-based subsystem is operated as one separate, application-specific DLT system.

HybCBDC is designed to enable confidential digital payments without requiring modification of power structures and roles of established financial systems. Therefore, HybCBDC maintains the operational structure of the existing financial system. For instance, the administration of real-time gross settlement systems, which are typically managed by central banks to facilitate the settlement of large-value inter-bank transactions, remains unchanged [76]. This ensures that established mechanisms for financial stability and transaction security still apply.

The operation of nodes for the subsystems of HybCDBC should be in line with the existing operational framework of the orchestrating central bank. The nodes can be operated by the central bank or distributed among various entities (e.g., authorized financial institutions and national central banks). HybCBDC offers a balance between accommodating centrally orchestrated and operated systems and federated and more decentralized ones. This flexibility allows for a variety of operational models to offer confidential payments while dynamics in central bank operations remain intact.

Payment system participants can transfer monetary items of a CBDC within and between those subsystems. The subsystems are interconnected using the Inter-Blockchain Communication (IBC) protocol [77], [78]. An alternative to the IBC protocol represents atomic swaps [70], [79]. Atomic swaps can offer direct asset exchanges between DLT systems without the need for intermediaries [80]. However, after careful consideration, we selected the IBC protocol [77] because it offers high flexibility by effectively separating the transport layer from the application layer. This separation allows for high flexibility in cross-chain communication. Furthermore, the IBC protocol supports easy-to-use monitoring tools for cross-chain interactions, supporting transparency and facilitating auditing processes [81].

The account-based subsystem in HybCBDC operates a wholesale layer and a retail layer and allows institutional payment system participants, such as commercial banks, to issue their own digital currencies backed by an account-balance wholesale CBDC. The issuance process in the account-based subsystem is analogous to common commercial bank money creation. Banks create new money through deposits or scriptural money, primarily through lending.

In the account-based subsystems, balances to manage monetary items of participants are recorded in accounts linked to identities of participants [24]. To create an account in the account-based subsystems, payment system participants need to verify their identities, like in most prevalent financial systems. The account-based subsystem processes transactions on the wholesale layer similar to established inter-banking systems, such as the TARGET2 system in the EU [82]. In addition, the account-based subsystem can process transactions between private payment system participants.

The account-based subsystem can interact with the UTXO-based subsystem, which offers confidential payments to private payment system participants. In the UTXO-based subsystem, private payment system participants use wallets to store public/secret key pairs corresponding to individual UTXOs in the UTXO-based subsystem.

To transfer monetary items stored in the UTXO-based subsystem, private payment system participants must first authenticate toward a UTXO using a secret key [31]. The monetary items can be exchanged at a one-to-one ratio while the total supply of monetary items remains constant in the UTXO-based subsystem. The value of monetary items in the UTXO-based subsystem and monetary items in the account-based subsystem are treated equally, which enables uniformity of those items.

In HybCBDC, authorized financial institutions (e.g., commercial banks) take the role *gatekeeper*. As gatekeepers, such institutions monitor the conversion (i.e., minting and burning) of monetary items from the account-balance to the UTXO-based subsystem and vice versa. The conversion can be (semi-)automated through a central bank in line with predefined rules (e.g., manifested in smart contracts) or manually controlled by gatekeepers. Additionally, authorized regulatory bodies (e.g., the European Banking Authority in Europe or the Financial Crimes Enforcement Network in the US) represented through notary nodes can be used to adhere to regulatory compliance regarding AML and CFT.

2) ACCOUNT-BASED SUBSYSTEM

The account-based subsystem in HybCBDC uses the account-balance model (see section II-A0c) and is interoperable with application-specific DLT systems from authorized financial institutions issuing commercial bank money tokens (CBMT).

HybCBDC builds on established mechanisms and responsibilities of conventional financial systems. For example, conventional money creation procedures [83] remain unchanged. Payment system participants cannot create accounts on their own but must request creation of accounts from

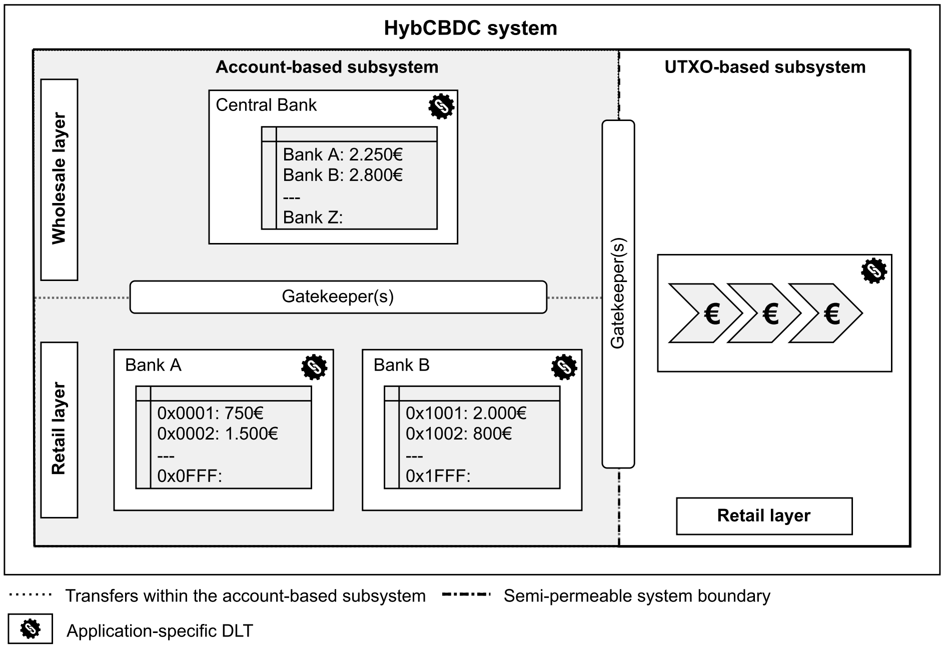

FIGURE 1. Simplified overview of HybCBDC, its account-balance and UTXO-based subsystems, and the retail and wholesale layers.

authorized financial institutions. Account creation requires identity verification, like in traditional financial systems. This controlled setup ensures that accounts are mapped to verified identities and are not freely generated in the account-based subsystem. Confidential transactions in the account-based subsystem are hardly possible, but enforcement of regulations is facilitated.

The account-based subsystem covers three transaction mechanisms: Mint, transfer, and burn. The central bank has the privilege to create (i.e., mint) and destroy (i.e., burn) monetary items of a CBDC as part of the capabilities of programmable money. The account-based subsystem offers an alternative to the existing real-time gross settlement system, such as TARGET2 in the EU [82].

The account-based subsystem incorporates a wholesale and retail layer that allow financial institutions to issue CBMTs backed by CBDC reserves in the account-based subsystem. Interaction between the wholesale and retail layers is standardized through the IBC protocol [77].

a: WHOLESALE LAYER

The wholesale layer is only accessible to institutional payment system participants and must be integrated with a central bank's ledger. Such institutions interact directly with a central bank's ledger. Every financial institution must prove its identity to be authorized to mint monetary items, process transactions, and manage accounts.

b: RETAIL LAYER

Each authorized institutional payment system participant can operate its own application-specific ledger in the retail layer to issue its own CBMT. In such a scenario, account-based wholesale CBDCs could serve as the reserve assets or collateral for CBMTs issued by commercial banks. The application-specific ledgers are operated in ledger systems, which can be distributed like in DLT systems or monolithic [70]. For example, application-specific DLT systems could be operated by a consortium of commercial banks.

As financial institutions can operate their own ledger systems, established procedures for creating commercial bank money in the traditional financial system can be executed (e.g., fractional reserve banking) [84]. In HybCBDC, ledger systems of financial institutions are directly connected to the account-based subsystem via a standardized interface to execute wholesale transactions. CBMTs are interchangeable, eliminating the risks related to the lack of one-to-one conversion. Furthermore, CBMTs have standards similar to the ones of ERC-20 tokens in the Ethereum system. The application-specific ledger system handles transactions within the same financial institute. Transactions across multiple financial institutes are settled via the wholesale layer. Application-specific ledgers of financial institutions offer private payment system participants indirect access to the account-based subsystem of HybCBDC.

3) UTXO-BASED SUBSYSTEM

The UTXO-based subsystem is exclusively designed to handle payments of private payment system participants and exclusively operates the retail layer. In the UTXO-based subsystem, HybCBDC uses a UTXO-based account model in combination with unique commitments inspired by ring confidential transactions [52], [55] to achieve unlinkability between payments and identities of senders and receivers.

The UTXO-based subsystem allows for cash-like characteristics of monetary items in HybCBDC (see section II-B). Cash notes are represented by UTXOs with a unique ID, a puzzle, and a fixed value. In HybCBDC, a puzzle is a public key used to prove ownership of the UTXO. Holding references to digital monetary items in the UTXO-based subsystem in a wallet is comparable to holding cash notes in a purse. Transitions, such as spending monetary items locked in a UTXO, must be signed with the secret key associated with the UTXO to prove ownership of those UTXOs. Payment system participants hold one secret key and a corresponding public key for each UTXO in their wallets. Neither secret keys nor public keys can be linked to known identities. No verification of identities is required to get access to the monetary items in the UTXO-based subsystem.

Figure 2 illustrates a simple payment in the UTXO-based subsystem. In the initial state, the UTXO stores information about (1) the value locked in the UTXO, (2) the issuance date of the UTXO, (3) the public key to verify ownership, and (4) the state of the UTXO. The UTXO update transaction includes the new public key to lock the UTXO, which should be updated and signed using the secret key used to generate the public key. After the successful transition, the UTXO can be unlocked by whoever knows the secret key of the new public key, which usually is the recipient of transferred monetary items. Payments from A to B can be performed by B sending a new public key to A, who creates an update transaction changing the UTXO's public key to B's new unused public key. After the transaction is finalized, only B can unlock the UTXO because only B knows the new secret key.

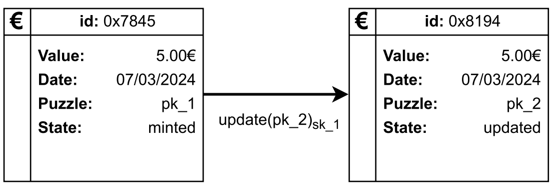

FIGURE 2. Exemplary transfer of cash-like monetary items in the UTXO-based subsystem.

We assume that wallets used by payment system participants ensure that public/secret key pairs are only used once in favor of forward secrecy. This can be achieved by implementing hierarchical deterministic wallets [85]. Because public keys cannot be mapped to identities in the UTXO-based subsystem, therefore, for third parties, every transaction could represent a possible change of ownership. Additionally, we assume that the wallet supports mixing functionality that executes random UTXO updates to shuffle the public/secret key pairs [53]. Mixing enhances payment confidentiality in the UTXO-based subsystem (see section II-C2b). A third party can neither determine whether the ownership of monetary items locked in a UTXO was transferred to another payment system participant nor whether the original owner has merely updated their secret. Consequently, it becomes difficult for third parties to trace transaction histories of private payment system participants.

4) MINT AND BURN MECHANISMS

To enable minting and burning monetary items in order to convert monetary items in the UTXO-based subsystem into monetary items in the account-based subsystem, HybCBDC uses an atomic burn mechanism and an atomic mint mechanism based on the IBC protocol [77]. Burning monetary items in the account-based subsystem leads to minting monetary items in the UTXO-based subsystem. This is comparable to depositing and withdrawing cash at an ATM. For example, Alice withdraws monetary items from her bank account (i.e., the account-based subsystem burns monetary items) and receives the withdrawn amount in cash (i.e., the UTXO-based subsystem mints monetary items). Conversely, Alice deposits cash in her bank account (i.e., the UTXO-based subsystem burns Alice's monetary items) and receives the deposited amount in her bank account (i.e., the account-based subsystem mints monetary items and sends them to Alice's account).

Cash transactions are often regulated, for example, by the AMLD5 and the cash control regulation (2018/1672) in the EU [28]. This means that for cash withdrawals and deposits exceeding 10,000 €, the origin and use of the money must be stated [86]. To achieve compliance with such regulations, financial institutions in the role of *gatekeepers* supervise conversions between digital cash in the UTXO-based subsystem and traceable digital money in the account-based subsystem. Moreover, gatekeepers issue corresponding burn and mint transactions to their DLT systems.

Gatekeepers can implement an automated monitoring process for embedded supervision [14]. This reduces the need for financial institutions to actively collect, verify, and deliver data to authorities. This kind of monitoring process enables HybCBDC to guarantee that the identification of payment system participants is only possible when minting or burning monetary items in the UTXO-based subsystem. Gatekeepers can enforce regulatory compliance, for example, to comply with cash regulations. In this case, the depositor has to provide the origin of the money if a certain amount (threshold) is exceeded. For example, in the EU, the AMLD5 states 10,000 € [86]. Nonetheless, payments within the UTXO-based subsystem are kept confidential.

Institutional payment system participants with access to the account-based subsystem must trigger the minting and burning transactions. When a financial institution mints monetary items in the UTXO-based subsystem, the financial institution must sign the newly created UTXO with its own secret key. Burning requires the financial institution to sign the burn transaction signed by the UTXO owner. The financial institution acts as a gatekeeper responsible for executing the conversion.

5) GATEKEEPERS AND REGULATORY COMPLIANCE

CBDC systems are regulated in most jurisdictions by governments to protect economies against malicious activities, such

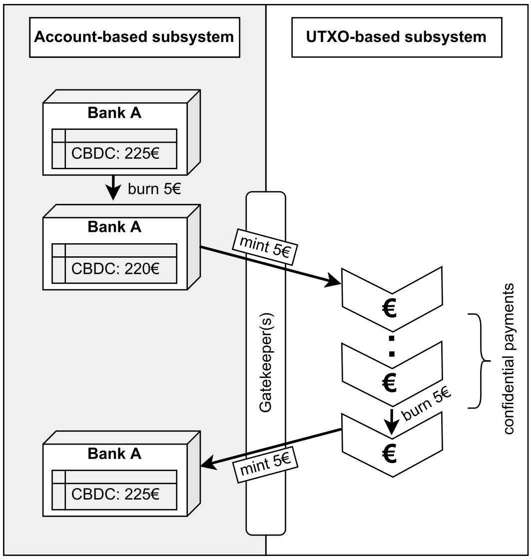

FIGURE 3. Schematic overview of burn and mint processes in HybCBDC to transfer monetary items from the account-based subsystem to the UTXO-based subsystem and vice versa.

as money laundering [36]. In HybCBDC, gatekeepers are expected to enforce cash regulations related to AML and CFT, for example, by stating the origin of the money to deposit or withdraw monetary items.

Regulation for digital monetary items, called electronic money in regulations, often include monthly turnover limits to address regulatory constraints related to AML and CFT. For example, in the EU, Article 12(7) (a) of the AMLD5 applies a monthly limit of 150 € per capita for anonymous digital [86]. However, this objective contrasts with the E-Money Directive (2009/110/EC), which, according to Article 1(1) (d), excludes CBDCs from the regulation of the AMLD5 [87]. We assume that CBDC systems shall meet the objectives of AMLD5 for regulating anonymous digital payments in the future. Building on that line of thought, balance, transfer, and conversion limits will likely be imposed to comply with regulations related to AML and CFT. Such limits can be enforced in HybCBDC by gatekeepers based on monthly unique commitments without the need to disclose transaction details. Unique commitments are renewed monthly. AML limits are enforced by design.

The UTXO-based subsystem uses unique commitments in combination with ring confidential transactions [55]. An anonymous onboarding process to HybCBDC hands out these commitments to every citizen. Every transaction in the UTXO-based subsystem is signed by senders using a ring signature of valid commitments. Such ring confidential transactions ensure that third parties cannot learn which commitments were spent. Commitments are automatically recharged within a certain period according to the turnover limit with existing regulations.

6) ILLUSTRATION OF THE TRANSACTION PROCESS IN HYBCBDC

This section describes how payments are processed in HybCBDC based on the example of Alice sending 5 € to Bob. The process is depicted in Figure 4.

Alice has an account at Bank A. Bob has one at Bank Z. For confidential payments to Bob, Alice must request monetary items in the UTXO-based subsystem at Bank A by submitting a burn request. When Bank A receives the request, the balance of 5 € is subtracted from Alice's account, and a burn transaction for the account-based subsystem is created with the public key pk_A submitted by Alice. The account-based subsystem deducts 5 € of the CBDC balance of Bank A. This allows Bank A to mint a 5 € UTXO on the UTXO-based subsystem. After checking if the corresponding burn mechanism exists on the account-based subsystem, the UTXO-based subsystem mints a new monetary item with pk_A and a value of 5 €. Alice holds the corresponding secret key sk_A to the pk_A. Therefore, she is the only one who can unlock the UTXO to spend the monetary item. Alice can trigger update, split, or merge transactions, as indicated by *any transitions* in the sequence diagram (see Figure 4).

Before Bob withdraws the 5 € from the UTXO-based subsystem back to the account-based subsystem, the monetary item could have switched hands multiple times. As UTXOs are spent, they are updated in the UTXO-based subsystem. This process complicates the tracing of transaction histories because it becomes difficult for third parties to determine whether a monetary item has changed hands or the owner just updated but still holds the UTXO, thus making tracking of monetary items in HybCBDC difficult [88].

If Alice wants to pay Bob, Bob needs to send a new pk_B to Alice. After receiving pk_B, Alice triggers an update to the UTXO-based subsystem. Alice unlocks monetary items locked in a UTXO using sk_A to prove ownership. Then, Alice locks the unlocked monetary items in a new UTXO with pk_B. Because only Bob knows the secret sk_B that can be used to compute pk_B, Alice cannot access the monetary item locked in the new UTXO. Bob is the legitimate monetary item owner. To withdraw monetary items in the UTXO-based subsystem to Bob's bank account, Bob must trigger the burn mechanism in the UTXO-based subsystem to burn the monetary item representing 5 € and trigger a mint mechanism at Bank Z. Bank Z issues a mint transaction signed with sk_B to the account-based subsystem, verifying if the corresponding monetary item with pk_B is burnt. If this check validates true, the minted 5 € are added to the balance of Bank Z. Finally, Bank Z increases Bob's balance by 5 €.

C. MAPPING OF HYBCBDC TO THE CONFIDENTIALITY REQUIREMENTS

In this section, we argue to what extent HybCBDC meets the requirements for confidential payments and enforceability of regulations related to AML and CFT (see section IV-A).

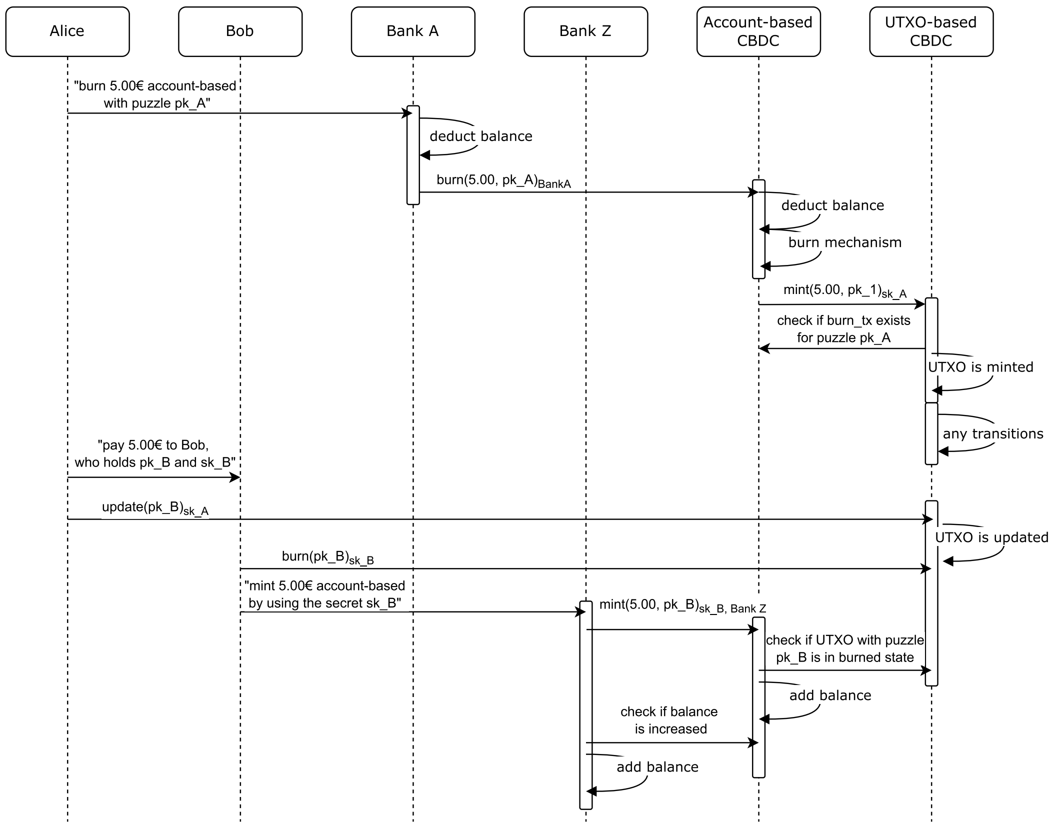

FIGURE 4. Sequence diagram for an example transaction.

a: AMOUNT OBFUSCATION

In the UTXO-based subsystem of HybCBDC, transactions are split into arbitrary small transactions. However, actual amounts paid to recipients are difficult to reconstruct because the individual transactions cannot be linked to each other due to using unique public/secret key pairs for each spent/received UTXO. Ring signatures allow the sender to obfuscate commitments used in transactions [55]. Therefore, unauthorized parties cannot learn actual payment amounts. HybCBDC meets the requirement *amount obfuscation*.

b: BALANCE OBFUSCATION

Each UTXO can only be unlocked with a unique, randomly generated secret. In combination with strategic random shuffling of public/secret key pairs, mapping public keys and UTXOs to payment system participants is difficult for unauthorized parties. Because such mapping is hardly possible in ideal settings (e.g., absence of cyber-observables), it is hard for unauthorized parties to compute balances of private payment system participants in a timely manner. Therefore, HybCBDC meets the requirement for *balance obfuscation*.

c: SENDER AND RECEIVER OBFUSCATION

For each UTXO, participants use new random public/secret key pairs (e.g., generated by wallets) to obfuscate identities. Therefore, unauthorized parties cannot map public keys to the identities of payment system participants. Because payment system participants always use new pseudonyms that are hard to link, it is difficult for unauthorized participants to learn the actual identities of senders and recipients in the real world. Therefore, HybCBDC meets the confidentiality requirement *sender and recipient obfuscation*.

d: SENDER-RECEIVER THIRD-PARTY UNLINKABILITY

The identities of payment system participants involved in transactions are not linkable in the UTXO-based subsystem due to the usage of unique public/secret key pairs that are only used once and cannot be mapped to identities. In combination with ring confidential transactions, this setup ensures that transaction details of payment system participants remain protected. Therefore, HybCBDC meets the confidentiality requirement *sender-receiver third party unlinkability*.

e: ENFORCEABILITY OF REGULATIONS

To support regulatory compliance with AML and CFT, enforcement of limits on confidential payments through gatekeepers is enabled. Commitments are automatically periodically recharged according to turnover limits defined in regulations. Gatekeepers notify authorities about behaviors that could violate regulations related to AML and CFT, for example, suspicious conversions of monetary items between the subsystems. By integrating those measures (e.g., gatekeepers that monitor conversions) into HybCBDC, compliance with regulations is supported.

Based on the above argumentation, the UTXO-based subsystem in HybCBDC meets the requirements of the requirement catalog (see section IV-A) and, thus, offers confidential payments and allows for enforcement of regulations related to AML and CFT in ideal settings.

V. DISCUSSION

This work presents HybCBDC, a CBDC system design developed to tackle the tension between confidential payments and transparency required to enforce regulations related to AML and CFT. In the following, we discuss our principal findings and point out the main contributions and limitations of this work, and outline future research directions.

A. PRINCIPAL FINDINGS

This study presents five requirements for confidential payments in CBDC systems (i.e., amount obfuscation, balance obfuscation, sender and receiver obfuscation, sender-receiver unlinkability, and regulatory compliance). We recognized that CBDC systems could require even stronger confidentiality requirements than cash. Cash payments do not have transaction recording. Typically, cash payments are only recorded by senders and receivers. Thereby, cash payments have a kind of 'decentralized transaction record'. Using cash, no central party could analyze or censor payments. Therefore, cash enables confidential payments by design. In contrast to cash, CBDC systems are digital payment systems administered by central banks. If payment confidentiality is not ensured, central banks can analyze and censor payments in real-time, which can lead to the emergence of surveillance states [9]. To mitigate risks associated with surveillance, confidential payments in CBDC systems are paramount [9], [10].

HybCDBC is designed to support confidential digital transactions with cash-like characteristics. The majority of illicit transactions are digital transactions in traditional financial systems [89]. This is attributed to higher convenience and assumed pseudonymity of digital transactions compared to cash transactions [90], even if regulations for digital payments seem much stricter than for cash [86]. For example, digital payment systems have a monthly per capita limit of 150 € in the AMLD5 regulation [86]. To account for illicit digital transactions, HybCBDC can help enforcement of regulations through gatekeepers.

The interviewees pointed out that the use of ring confidential transactions to comply with regulations of confidential payments related to AML and CFT has two principal challenges. First, the automated mixing of UTXO to obfuscate ownership of monetary items locked in UTXOs drains the monthly balance of the ring confidential transaction's commitment. The monthly turnover limitation would be applied to the mixing and spending of monetary items of a CBDC issued through the UTXO-based subsystem. Second, correlation attacks could be performed based on recurring payments, involving the same commitment in each payment [66]. Daily confidential payments could be used to deduce a customer's commitment because the actual commitment would be part of the 'ring' in every transaction. After multiple payments from one customer, only one commitment would be consistent in the ring signature. Merchants can potentially track future customer payments since they learn customer commitments.

Interactions between the account-based subsystem and the UTXO-based subsystem are in line with the established 'trust framework' [91], [92]. That trust framework is a result of the functioning of the banking system, where regulations (e.g., E-Money Directive [93]) form the source of trust [94]. The trust framework helps ensure that all participants can trust the integrity, security, and proper functioning of the financial system. If this trust is compromised (e.g., by censoring transactions of dissidents), the entire financial system is at risk. To mitigate this risk, atomic swaps can decrease dependencies on the established trust framework to enhance resilience.

In future cashless societies, HybCBDC could be useful in tackling challenges related to money laundering. Every participant in HybCBDC must adhere to strict compliance rules (e.g., monthly limit for confidential payments). Such strict enforceability mitigates risks associated with cash-based money laundering and offers a solution to hinder financial crimes and enhance transparency. This emphasizes the need for adequate regulation of CBDC systems to enable enforcement of such regulations through gatekeepers in HybCBDC.

B. CONTRIBUTIONS

We present HybCBDC to support confidential payments in CBDC systems and enforceability of regulations at the same time. In particular, this work has three main contributions. First, we support a better understanding of the requirements for confidential payments by mapping privacy notions [69] to payment systems. This can support developers of CBDC systems in better understanding what aspects of the payment processes need to be carefully considered to enable confidential payments.

Second, by showing how cash-like confidentiality can be achieved for digital payments in the UTXO-based subsystem (e.g., unlinkability of transactions to senders and receivers of payments [23]), we support the development of CBDC systems that support confidential payments. Enabling confidential payments for CBDC, HybCBDC can increase the adoption of CBDCs in a cashless society.

Third, by showing how the CBDC system can be designed considering requirements for confidential payments and regulatory compliance, we offer a novel approach for resolving tensions between those requirements. HybCBDC offers an approach to offering confidential payments and achieving regulatory compliance. Furthermore, HybCBDC can be useful for developers of CBDC systems by offering a CBDC system design that can be seamlessly integrated into established financial systems. This is useful to guide decision-makers in development of CBDC systems in the future.

C. LIMITATIONS

Despite the rigorous development of HybCBDC in several iterations of refinement, this work has limitations. We conducted focus group interviews with experts in banking, consulting and industry to iteratively enhance HybCBDC. Notwithstanding the valuable feedback obtained in the focus group workshops, we did not quantitatively evaluate the performance of HybCBDC. Thus, we can hardly predict the system behavior of implementations of HybCBDC.

One significant challenge is the complexity introduced by using multiple interoperable DLT systems. Managing and ensuring seamless interaction between these distinct systems is inherently more complex than utilizing a single DLT system. This increased complexity can increase operational costs. Although the interviewees considered the use of two DLT systems to be beneficial, we cannot definitively state whether the implementation of HybCBDC is practical for banks. The dual-system approach, while theoretically sound, poses practical challenges in terms of integration, scalability, and maintenance that may impact its feasibility in real-world banking environments.

HybCBDC does not support confidential offline payments because the UTXO-based subsystem, in the presented form, requires receivers to check whether transactions are finalized in the DLT system. Thus, transactions are not necessarily securely completed in offline environments, which could constrain the usability of HybCBDC in scenarios of insufficient internet connectivity. Consequently, payment system participants might face challenges related to payments in areas with poor network coverage. An approach to tackle that challenge is to use identity-based signatures in offline scenarios [95]. Senders can send copies of UTXO updates to payment receivers. Senders and receivers can send the UTXO update to the DLT system when they are online again. If a receiver detects a double spend, they could enforce the payment themselves. Although this makes offline payments possible, it compromises the confidentiality that HybCBDC aims to ensure.

This work is focused on proposing a CBDC system design that resolves the tension between confidential payments and transparency for enforcement of regulations. We assumed ideal settings where metadata related to transactions (e.g., IP addresses) are not available to attackers. However, in real-world settings, such metadata can be available to attackers and could facilitate inferring identities of payment system participants. Consequently, HybCBDC cannot guarantee complete confidentiality in real-world settings without additional security measures. Therefore, HybCBDC should be extended by additional security techniques, such as mixing, to offer confidential payments in real-world settings.

D. FUTURE RESEARCH

HybCBDC builds on multiple DLT systems that interoperate based on the IBC protocol [77]. However, various alternative interoperability artifacts exist to enable interoperability between DLT systems, including centralized and decentralized notary schemes [70], [79]. Impacts of different cross-ledger interoperability artifacts on CBDC systems (e.g., in terms of performance and security) still remain largely unclear, which complicates the targeted design of CBDC systems. Future research should uncover best practices for interoperability (e.g., in the form of software design patterns) to support the targeted design of CBDC systems.

Using DLT systems can lead to scalability bottlenecks if consensus finding has high communication complexity [42]. To cope with scalability bottlenecks, financial institutions can use state channels [96], [97]. Future research should investigate how state channels can be used in HybCBDC while not violating the requirements for confidential transactions and enforceability of regulations.

From a social perspective, integration of CBDC systems with existing financial systems raises important questions beyond technical feasibility [94], [98]. Future research should delve into the implications of using CBDC on societies. This includes supporting a better understanding of the impact of CBDC systems on financial inclusion, privacy of private payment system participants, and changes in consumer behavior. Multidisciplinary research is needed to inform policymakers and guide the development of regulations that foster innovation while protecting the interests of societies [99].

VI. CONCLUSION

This work presents HybCBDC, a hybrid CBDC system design that offers confidential payments while allowing for enforcement of regulations related to AML and CFT. To appropriately address the tension between the need for confidential payments and the enforceability of legal regulations (e.g., AML and CFT), HybCBDC relies on a combination of an account-based and a UTXO-based subsystem. Each subsystem is operated based on different but interoperable DLT subsystems. HybCBDC was iteratively developed in three semi-structured focus group interviews with nine experts in finance and industry. In each iteration, HybCBDC was improved based on feedback obtained from focus group interviews.

By presenting HybCDBC, we support development of CBDC systems that provide a digital equivalent to cash for society to ensure that transactional freedom is preserved in the digital age. We hope that HybCBDC offers a useful foundation for paving the way for CBDC systems.

ACKNOWLEDGMENT

We thank all study participants who helped us design and improve HybCBDC. Moreover, we thank Benjamin Sturm, Mikael Beyene, and Gabriela Ciolacu for their valuable feedback on the manuscript. In honor of Philipp Sandner, whose support has significantly impacted this work. We remember him as an important figure in our research and a source of enduring inspiration.

REFERENCES

[1] R. Z. Wiggins, T. Piontek, and A. Metrick. (2019). *The Lehman Brothers Bankruptcy A: Overview*. [Online]. Available: https://elischolar.library.yale.edu/journal-of-financial-crises/vol1/iss1/2

[2] U. Bindseil, F. Panetta, and I. Terol. (2021). *Central Bank Digital Currency: Functional Scope, Pricing and Controls*. [Online]. Available: https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op286

[3] R. Auer, J. Frost, L. Gambacorta, C. Monnet, T. Rice, and H. S. Shin. (2021). *Central Bank Digital Currencies: Motives, Economic Implications and the Research Frontier*. [Online]. Available: https://ssrn.com/abstract=3922836

[4] European Central Bank. (2021). *ECB Publishes the Results of the Public Consultation on a Digital Euro*. [Online]. Available: https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414ca3013c852.en.html

[5] P. Sandner, J. Gross, and J.-C. Chung. *The Programmable Euro: Review and Outlook*. Accessed: May 2023. [Online]. Available: https://papers.ssrn.com/abstract=3971464

[6] European Central Bank and U. Bindseil. (2020). *Tiered CBDC and the Financial System*. Office. [Online]. Available: https://data.europa.eu/doi/10.2866/134524

[7] P. Wong and J. L. Maniff. (Aug. 13, 2020). *Comparing Means of Payment: What Role for a Central Bank Digital Currency?* FEDS Notes. [Online]. Available: https://www.federalreserve.gov/econres/notes/feds-notes/comparing-means-of-payment-20200813.htm

[8] R. Auer, G. Cornelli, and J. Frost. (2020). *Rise of the Central Bank Digital Currencies: Drivers, Approaches and Technologies*. [Online]. Available: https://ssrn.com/abstract=3724070

[9] U. Bindseil. (2022). *The Case for and Against CBDC—Five Years Later*. [Online]. Available: https://ssrn.com/abstract=4038828

[10] D. Ballaschk and J. Paulick, "The public, the private and the secret: Thoughts on privacy in central bank digital currencies," *J. Payments Strategy Syst.*, vol. 15, no. 3, pp. 277–286, 2021.

[11] C.-A. Claussen, H. Armelius, and I. Hull. (2021). *On the Possibility of a Cash-Like CBDC*. [Online]. Available: https://www.riksbank.se/globalassets/media/rapporter/staff-memo/engelska/2021/on-the-possibility-of-a-cash-like-cbdc.pdf

[12] C. Zellweger-Gutknecht, B. Geva, and S. N. Grünewald, "Digital euro, monetary objects, and price stability: A legal analysis," *J. Financial Regulation*, vol. 7, no. 2, pp. 284–318, Sep. 2021.

[13] C. M. Kahn, J. McAndrews, and W. Roberds, "Money is privacy," *Int. Econ. Rev.*, vol. 46, no. 2, pp. 377–399, 2005.

[14] R. Auer, "Embedded supervision: How to build regulation into blockchain finance," *Federal Reserve Bank Dallas, Globalization Inst. Work. Papers*, vol. 2019, no. 371, pp. 1–9, Nov. 2019.

[15] J. Gross, J. Sedlmeir, M. Babel, and A. Bechtel. *Designing a Central Bank Digital Currency With Support for Cash-Like Privacy*. Accessed: May 2023. [Online]. Available: https://ssrn.com/abstract=3891121

[16] R. Auer, P. Haene, and H. Holden, "Multi-CBDC arrangements and the future of cross-border payments," Bank Int. Settlements, Basel, Switzerland, Tech. Rep. 115, 2020. [Online]. Available: https://ideas.repec.org/b/bis/bisbps/115.html

[17] M. Kumhof and C. Noone. (2018). *Central Bank Digital Currencies—Design Principles and Balance Sheet Implications*. [Online]. Available: https://ssrn.com/abstract=3180713

[18] W. Dai, X. Gu, and Y. Teng, "A supervised anonymous issuance scheme of central bank digital currency based on blockchain," in *Algorithms and Architectures for Parallel Processing*, M. Qiu, Ed., Cham, Switzerland: Springer, 2020, pp. 475–493.

[19] O. Atangana, L. Khoukhi, and W. Royer, "Securing privacy in offline payment for retail central bank digital currency: A comprehensive framework," in *Proc. 2nd Blockchain Cryptocurrency Conf.*, 2023, pp. 25–32.

[20] V. Dostov, P. Pimenov, P. Shoust, S. Krivoruchko, and V. Titov, "Comparison of the digital ruble concept with foreign central bank digital currencies," in *Proc. 4th Int. Conf. Blockchain Technol. Appl.*, New York, NY, USA, Dec. 2021, pp. 70–75, doi: 10.1145/3510487.3510498.

[21] D. Chaum, C. Grothoff, and T. Moser, "How to issue a central bank digital currency," *Swiss Nat. Bank Work. Papers*, vol. 2021, no. 3, p. 34, 2021. [Online]. Available: https://ar5iv.org/abs/2103.00254

[22] N. Pocher and A. Veneris, "Privacy and transparency in CBDCs: A regulation-by-design AML/CFT scheme," *IEEE Trans. Netw. Service Manage.*, vol. 19, no. 2, pp. 1776–1788, Jun. 2022.

[23] E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, "Zerocash: Decentralized anonymous payments from Bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 459–474.

[24] R. Auer and R. Böhme. *The Technology of Retail Central Bank Digital Currency*. Accessed: Sep. 2022. [Online]. Available: https://papers.ssrn.com/abstract=3561198

[25] P. Sandner, J. Gross, L. Grale, and P. Schulden. (2020). *The Digital Programmable Euro, Libra and CBDC: Implications for European Banks*. [Online]. Available: https://papers.ssrn.com/abstract=3663142

[26] C. Gengxuan, J. Qinmin, L. Hao, and L. Yuyang, "The digital currency of China's central bank: Digital currency electronic payment (DCEP)," *Contemporary Social Sciences*, vol. 2021, no. 4, pp. 1–16, 2021.

[27] H. Armelius, G. Guibourg, A. T. Levin, and G. Söderberg. *The Rationale for Issuing E-krona in the Digital Era*. Accessed: Sep. 2023. [Online]. Available: https://www.riksbank.se/globalassets/media/rapporter/pov/artiklar/engelska/2020/200618/2020_2-the-rationale-for-issuing-e-krona-in-the-digital-era.pdf

[28] R. Wandhöfer. (2017). *The Future of Digital Retail Payments in Europe: A Place for Digital Cash?* [Online]. Available: https://api.semanticscholar.org/CorpusID:85560335

[29] M. Xu, Y. Guo, C. Liu, Q. Hu, D. Yu, Z. Xiong, D. Niyato, and X. Cheng, "Exploring blockchain technology through a modular lens: A survey," *ACM Comput. Surv.*, vol. 56, no. 9, pp. 1–39, May 2024, doi: 10.1145/3657288.

[30] J. Zhang, R. Tian, Y. Cao, X. Yuan, Z. Yu, X. Yan, and X. Zhang, "A hybrid model for central bank digital currency based on blockchain," *IEEE Access*, vol. 9, pp. 53589–53601, 2021.

[31] S. Delgado-Segura, C. Pérez-Sola, G. Navarro-Arribas, and J. Herrera-Joancomartí, "Analysis of the Bitcoin UTXO set," in *Financial Cryptography and Data Security* (Lecture Notes in Computer Science). Berlin, Germany: Springer, 2019, pp. 78–91.

[32] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "CoinShuffle: Practical decentralized coin mixing for Bitcoin," in *Proc. 19th Eur. Symp. Res. Comput. Secur.*, Wroclaw, Poland. Berlin, Germany: Springer, Sep. 2014, pp. 345–364.

[33] F. Reid and M. Harrigan, "An analysis of anonymity in the Bitcoin system," in *Security and Privacy in Social Networks*. Berlin, Germany: Springer, 2013, pp. 197–223.

[34] A. Barth, A. Datta, J. C. Mitchell, and H. Nissenbaum, "Privacy and contextual integrity: Framework and applications," in *Proc. IEEE Symp. Secur. Privacy*, Oakland, CA, USA, May 2006, pp. 11–15.

[35] D. Kirste, N. Kannengießer, R. Lamberty, and A. Sunyaev, "How automated market makers approach the thin market problem in cryptoeconomic systems," 2023, *arXiv:2309.12818*.

[36] M. Hennies, "Cash as an elementary component of liberal social order," *Estonian Discuss. Econ. Policy*, vol. 24, no. 1, pp. 1–5, 2016, doi: 10.2139/ssrn.2840810.

[37] A. Zamora-Pérez, "The paradox of banknotes: Understanding the demand for cash beyond transactional use," Eur. Central Bank, Frankfurt, Germany, Econ. Bull. Articles, 2021, vol. 2. [Online]. Available: https://ideas.repec.org/a/ecb/ecbart/202100023.html

[38] G. Bichler, A. Malm, and T. Cooper, "Drug supply networks: A systematic review of the organizational structure of illicit drug trade," *Crime Sci.*, vol. 6, no. 1, p. 2, Dec. 2017, doi: 10.1186/s40163-017-0063-3.

[39] A. A. Dumitrache and G. Modiga, "New trends and perspectives in the money laundering process," *Challenges Knowl. Society. Law*, vol. 1, pp. 50–57, Jan. 2011.

[40] J. Lovejoy, C. Fields, M. Virza, T. Frederick, D. Urness, K. Karwaski, A. Brownworth, and N. Narula. (2022). *A High Performance Payment Processing System Designed for Central Bank Digital Currencies*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2022/163

[41] V. Sethaput and S. Innet, "Blockchain application for central bank digital currencies (CBDC)," *Cluster Comput.*, vol. 26, no. 4, pp. 2183–2197, Aug. 2023, doi: 10.1007/s10586-022-03962-z.

[42] N. Kannengießer, S. Lins, T. Dehling, and A. Sunyaev, "Trade-offs between distributed ledger technology characteristics," *ACM Comput. Surv.*, vol. 53, no. 2, pp. 1–37, Mar. 2021.

[43] T. Adrian and T. Mancini-Griffoli, *The Rise of Digital Money* (FinTech Notes). San Mateo, CA, USA: Annual Reviews, 2019.

[44] R. Morales-Resendiz, J. Ponce, P. Picardo, A. Velasco, B. Chen, L. Sanz, G. Guiborg, B. Segendorff, J. L. Vasquez, J. Arroyo, I. Aguirre, N. Haynes, N. Panton, M. Griffiths, C. Pieterz, and A. Hodge, "Implementing a retail CBDC: Lessons learned and key insights," *Latin Amer. J. Central Banking*, vol. 2, no. 1, Mar. 2021, Art. no. 100022.

[45] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[46] R. Lamberty, A. Poddey, D. Galindo, D. de Waard, T. Koelbel, and D. Kirste, "Efficiency in digital economies—A primer on tokenomics," 2020, *arXiv:2008.02538*.

[47] J. Groß, P. Sandner, and M. Klein, "The digital euro and the role of DLT for central bank digital currencies," Frankfurt School Blockchain Center, Working Paper, Frankfurt, Germany, 2020.

[48] A. Nugroho, S. H. Supangkat, and A. A. Arman, "Central bank digital currency (CBDC) information technology system design : A literature review," in *Proc. 10th Int. Conf. ICT Smart Soc. (ICISS)*, Sep. 2023, pp. 1–6.

[49] F. B. Schneider, "Implementing fault-tolerant services using the state machine approach: A tutorial," *ACM Comput. Surv.*, vol. 22, no. 4, pp. 299–319, Dec. 1990.

[50] E. Rennie and S. Steele, "Privacy and emergency payments in a pandemic: How to think about privacy and a central bank digital currency," *Law, Technol. Humans*, vol. 3, no. 1, pp. 6–17, May 2021.

[51] R. Auer, R. Böhme, J. Clark, and D. Demirag, "Mapping the privacy landscape for central bank digital currencies: Now is the time to shape what future payment flows will reveal about you," *Queue*, vol. 20, no. 4, pp. 16–38, Aug. 2022.

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

[53] T. Ruffing, P. Moreno-Sanchez, and A. Kate. (2016). *P2P Mixing and Unlinkable Bitcoin Transactions*. [Online]. Available: https://eprint.iacr.org/2016/824

[54] M. Nadler and F. Schàr. (2023). *Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers*. [Online]. Available: https://ssrn.com/abstract=4352337

[55] S. Noether, A. Mackenzie, and T. M. R. Lab, "Ring confidential transactions," *Ledger*, vol. 1, pp. 1–18, Dec. 2016.

[56] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology—ASIACRYPT*, vol. 2248, C. Boyd, Ed., Berlin, Germany: Springer, 2001, pp. 552–565.

[57] C. W. M. Tikvah. (2023). *A Privacy-preserving Central Bank Ledger for Central Bank Digital Currency*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2023/1496

[58] L. Malina, J. Hajny, P. Dzurenda, and S. Ricci, "Lightweight ring signatures for decentralized privacy-preserving transactions," in *Proc. 15th Int. Joint Conf. e-Business Telecommun.*, 2018, pp. 526–531.

[59] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox. (2022). *Zcash Protocol Specification, Version 2022.3.8 [NU5]*. [Online]. Available: https://zips.z.cash/protocol/protocol.pdf

[60] G. Kappos, H. Yousaf, M. Maller, and S. Meiklejohn, "An empirical analysis of anonymity in Zcash," in *Proc. 27th USENIX Conf. Security Symp.*, Baltimore, MD, USA, 2018, pp. 463–477. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/kappos

[61] I. Miers, C. Garman, M. Green, and A. D. Rubin, "Zerocoin: Anonymous distributed E-cash from Bitcoin," in *Proc. IEEE Symp. Secur. Privacy*, May 2013, pp. 397–411.

[62] C. V. Moya, J. R. Bermejo Higuera, J. Bermejo Higuera, and J. A. Sicilia Montalvo, "Implementation and security test of zero-knowledge protocols on SSI blockchain," *Appl. Sci.*, vol. 13, no. 9, p. 5552, Apr. 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/9/5552

[63] G. Almashaqbeh and R. Solomon, "SoK: Privacy-preserving computing in the blockchain era," in *Proc. IEEE 7th Eur. Symp. Secur. Privacy*, Genova, Italy, Jun. 2022, pp. 124–139.

[64] J. Camenisch, S. Hohenberger, and A. Lysyanskaya, "Balancing accountability and privacy using e-cash," in *Security and Cryptography for Networks*. Berlin, Germany: Springer, 2006, pp. 141–155.

[65] J. Herrera-Joancomartí and C. Pérez-Solà, "Privacy in Bitcoin transactions: New challenges from blockchain scalability solutions," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Berlin, Germany: Springer, 2016, pp. 26–44.

[66] M. N. S. Perera, T. Nakamura, M. Hashimoto, H. Yokoyama, C.-M. Cheng, and K. Sakurai, "A survey on group signatures and ring signatures: Traceability vs. anonymity," *Cryptography*, vol. 6, no. 1, p. 3, Jan. 2022.

[67] M. Petkus, "Why and how zk-SNARK works," 2019, *arXiv:1906.07221*.

[68] T. Bontekoe, M. Everts, and A. Peter, "Balancing privacy and accountability in digital payment methods using zk-SNARKs," in *Proc. 19th Annu. Int. Conf. Privacy, Secur. Trust (PST)*, Aug. 2022, pp. 1–10.

[69] C. Kuhn, M. Beck, S. Schiffner, E. Jorswieck, and T. Strufe. (2019). *On Privacy Notions in Anonymous Communication*. [Online]. Available: https://petsymposium.org/popets/2019/popets-2019-0022.php

[70] M. Pfister, N. Kannengießer, and A. Sunyaev, "Finding the right balance: Technical and political decentralization in the token economy," in *Blockchains and the Token Economy: Theory and Practice* (Technology, Work and Globalization), M. C. Lacity and H. Treiblmaier, Eds., Cham, Switzerland: Springer, 2022, pp. 53–86.

[71] R. A. Krueger and M. A. Casey, *Focus Groups: A Practical Guide for Applied Research*, 5th ed., Thousand Oaks, CA, USA: SAGE, 2014.

[72] M. D. Myers, *Qualitative Research in Business & Management*, 2nd ed., Thousand Oaks, CA, USA: SAGE, 2013.

[73] J. S. Ancker, N. C. Benda, M. Reddy, K. M. Unertl, and T. Veinot, "Guidance for publishing qualitative research in informatics," *J. Amer. Med. Inform. Assoc.*, vol. 28, no. 12, pp. 2743–2748, Nov. 2021.

[74] V. Verykios, A. Elmagarmid, E. Bertino, Y. Saygin, and E. Dasseni, "Association rule hiding," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 4, pp. 434–447, Apr. 2004.

[75] D. Chaum, "How to achieve unlinkable transaction histories," *J. Cryptograph. Eng.*, vol. 5, no. 3, pp. 123–136, 2021.

[76] European Central Bank. *TARGET2—The Eurosystem's Real-Time Gross Settlement (RTGS) System*. Accessed: Jun. 10, 2024. [Online]. Available: https://www.ecb.europa.eu/paym/target/target2/html/index.en.html

[77] C. Goes, "The interblockchain communication protocol: An overview," 2020, *arXiv:2006.15918*.

[78] Interchain Foundation. *Interchain Foundation: Building the Foundation of the Interchain*. Accessed: Nov. 2023. [Online]. Available: https://interchain.io/

[79] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Comput. Surv.*, vol. 54, no. 8, pp. 1–41, Nov. 2022.

[80] M. Herlihy, "Atomic cross-chain swaps," in *Proc. ACM Symp. Princ. Distrib. Comput.* New York, NY, USA: Association for Computing Machinery, Jul. 2018, pp. 245–254, doi: 10.1145/3212734.3212736.

[81] W.-T. Tsai, Z. Zhao, C. Zhang, L. Yu, and E. Deng, "A multi-chain model for CBDC," in *Proc. 5th Int. Conf. Dependable Syst. Appl. (DSA)*, Sep. 2018, pp. 25–34.

[82] K. Whelan. (2013). *TARGET2 and Central Bank Balance Sheets*. UCD Centre, Dublin, UCD Centre for Economic Research Working Paper Series WP12/29. [Online]. Available: http://hdl.handle.net/10419/72217

[83] M. McLeay, A. Radia, and R. Thomas, "Money creation in the modern economy," *Bank England Quart. Bull.*, vol. 54, no. 1, p. Q1, Mar. 2014. [Online]. Available: https://econpapers.repec.org/article/boeqbullt/0128.htm

[84] P. Bagus and D. Howden, "Fractional reserve free banking: Some quibbles," *Quart. J. Austrian Econ.*, vol. 13, no. 4, pp. 29–55, 2010.

[85] S. Banupriya, K. Kottursamy, and A. K. Bashir, "Privacy-preserving hierarchical deterministic key generation based on a lattice of rings in public blockchain," *Peer-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2813–2825, Sep. 2021.

[86] Council of the European Union. (2018). *Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU*. Accessed: Nov. 2023. [Online]. Available: http://data.europa.eu/eli/dir/2018/843/oj/eng

[87] Councils of the European Union. *Directive 2009/110/EC*. Accessed: Nov. 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX

[88] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of Bitcoins: Characterizing payments among men with no names," *Commun. ACM*, vol. 59, no. 4, pp. 86–93, 2013.

[89] J. Whisker and M. E. Lokanan, "Anti-money laundering and counter-terrorist financing threats posed by mobile money," *J. Money Laundering Control*, vol. 22, no. 1, pp. 158–172, Jan. 2019.

[90] E. A. Isolauri and I. Ameer, "Money laundering as a transnational business phenomenon: A systematic review and future agenda," *Crit. Perspect. Int. Bus.*, vol. 19, no. 3, pp. 426–468, Apr. 2023.

[91] B. Hayo and E. Neuenkirch. (2013). *The German Public and Its Trust in the ECB: The Role of Knowledge and Information Search*. [Online]. Available: https://ssrn.com/abstract=2389652

[92] N. Brouwer and J. de Haan, "Trust in the ECB: Drivers and consequences," *Eur. J. Political Economy*, vol. 74, Sep. 2022, Art. no. 102262, doi: 10.1016/j.ejpoleco.2022.102262.

[93] European Parliament and Council. (2009). *Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the Taking Up, Pursuit and Prudential Supervision of the Bus. of Electronic Money Institutions*. Accessed: Jun. 3, 2024. [Online]. Available: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF

[94] R. Lamberty and A. Poddey, "Regulation conform DLT-operable payment adapter based on trustless–justified trust combined generalized state channels," 2020, *arXiv:2007.01605*.

[95] A. Tobin, D. Reed, F. P. J. Windley, and S. Foundation. (2017). *The Inevitable Rise of Self-sovereign Identity*. [Online]. Available: https://sovrin.org/library/inevitable-rise-of-self-sovereign-identity/

[96] S. Dziembowski, S. Faust, and K. Hostáková, "General state channel networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2018, pp. 949–966.

[97] S. Dziembowski, L. Eckey, S. Faust, and D. Malinowski. (2017). *Perun: Virtual Payment Hubs Over Cryptocurrencies*. [Online]. Available: http://eprint.iacr.org/2017/635

[98] B. J. Tan, "Central bank digital currency and financial inclusion," Int. Monetary Fund, Washington, DC, USA, IMF Working Paper 23/69, 2023.

[99] A. Tsareva and M. Komarov, "Retail central bank digital currency design choices: Guide for policymakers," *IEEE Access*, vol. 12, pp. 66129–66146, 2024.

RICKY LAMBERTY is currently pursuing the Ph.D. degree with the German University of Digital Science, Germany. He is a Lead Expert of digital assets and digital economy with Robert Bosch GmbH, Germany. His research interests include decentralized finance, central bank digital currencies, automated market makers, and cryptoeconomic systems.

DANIEL KIRSTE is currently pursuing the Ph.D. degree in computer science with the Institute of Applied Informatics and Formal Description Methods, Karlsruhe Institute of Technology, Germany. His research is with the Corporate Research Department, Robert Bosch GmbH, Germany, with a focus on decentralized finance, automated market makers, and cryptoeconomic systems.

NICLAS KANNENGIEßER is currently a Research Associate with the KASTEL Security Research Labs and the Institute of Applied Informatics and Formal Description Methods, Karlsruhe Institute of Technology, Germany. He has authored or co-authored in journals, including IEEE ACCESS, *ACM Computing Surveys*, IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, and *Business and Information Systems Engineering*. His research interests include software engineering and analysis of system behaviors of distributed systems, such as distributed ledger technology systems and the dynamics of decentralized information systems.

ALI SUNYAEV (Member, IEEE) is currently a Professor of computer science with Karlsruhe Institute of Technology, Germany. His research work accounts for the multifaceted use contexts of digital technologies with research on human behavior affecting information systems and vice versa. He has authored or co-authored articles in journals, including ACM CSUR, IEEE TRANSACTIONS ON SOFTWARE ENGINEERING, ISR, JIT, JMIS, IEEE TRANSACTIONS ON CLOUD COMPUTING, and *Communications of the ACM*. His research interests include complex information systems, information infrastructures, cloud computing services, distributed ledger technology, information privacy, auditing or certification of IT, digital health, and trustworthy AI.