Atlantic Council
GEOECONOMICS CENTER

FRANKFURT FORUM on US-EUROPEAN GEOECONOMICS

ATLANTIK-BRÜCKE

Privacy in Cross-border Digital Currency

A Transatlantic Approach

By Giulia Fanti & Nadia Pocher

Frankfurt Forum

This paper is one of four publications launched at the inaugural Frankfurt Forum on US-European GeoEconomics held in Germany from September 27 – 29, 2022. Co-hosted by the Atlantic Council GeoEconomics Center and Atlantik-Brücke, the Frankfurt Forum anchors critical work on transatlantic economic cooperation. The war in Ukraine, and the G7 response, reminded the world of the impact of transatlantic coordination. As part of the Frankfurt Forum, this new research aims to advance transatlantic dialogue from crisis response to addressing the key economic issues that will underpin the US-EU partnership over the next decade. The goal of the Frankfurt Forum is to deliver a blueprint for cooperation in four key areas: digital currencies, monetary policy, international trade, and economic statecraft.

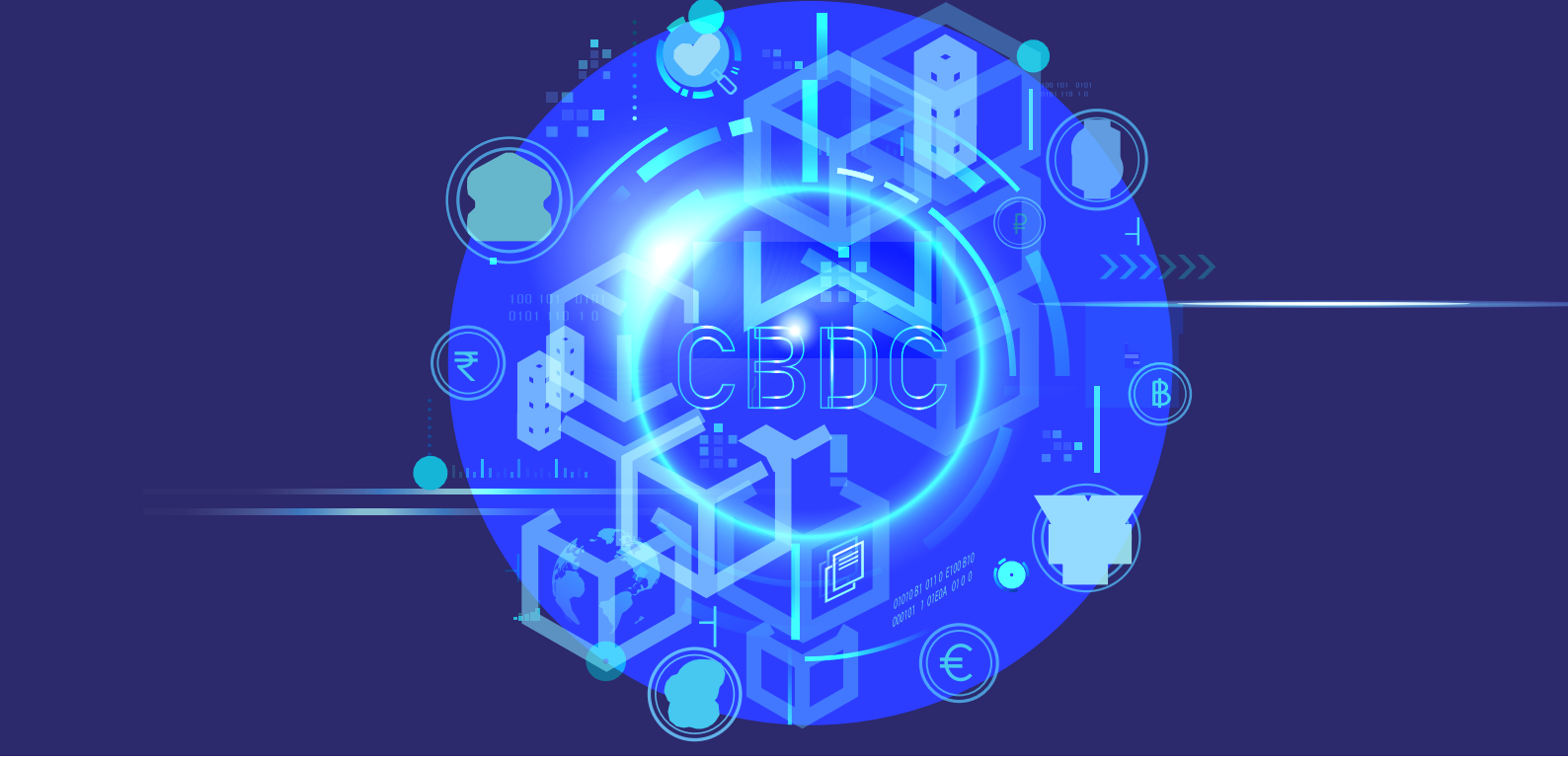
Atlantic Council's GeoEconomics Center

Launched in 2020, the Atlantic Council's GeoEconomics Center has become the go-to place at the intersection of economics, finance, and foreign policy. The Center bridges the divide between these oft-siloed sectors and helps shape a better global economic future for the US and its allies. The Center is organized around three pillars: 1) The Future of Capitalism; 2) The Future of Money; and 3) The Economic Statecraft Initiative.

Atlantik-Brücke

Founded in 1952, Atlantik-Brücke is a non-profit and non-partisan association committed to deepening cooperation between Germany, Europe and America. Transatlantic cooperation remains pivotal for global order and stability, now more than ever. With nationalist tendencies gaining popularity worldwide, Atlantik-Brücke has doubled down on its mission to solidifying relations across the Atlantic among policymakers, industry leaders, journalists, academics, and civil society by offering a platform for different perspectives and lively debate. Atlantik-Brücke also fosters ties between young professionals and representatives of civil society through annual conferences and exchanges. The approximately 500 members of Atlantik-Brücke are decision-makers from business, politics, science and the media on both sides of the Atlantic.

TABLE OF CONTENTS



EXECUTIVE SUMMARY

Central bank digital currencies (CBDCs), virtual money backed by central banks, are continuing to gain momentum. According to Atlantic Council research, 105 countries, accounting for more than 95 percent of global gross domestic product, are currently considering issuing a CBDC. While more and more countries are exploring CBDCs for the domestic context, multi-country cross-border CBDCs pilots are also proliferating. According to the Atlantic Council, there are more than 7 cross-border projects currently underway with more likely coming throughout 2023. The motivation for cross-border usage is clear: CBDCs could significantly improve cross-border financial transactions by simplifying the current process, making it faster, and reducing costs for users. However, for any cross-border CBDC to unlock these benefits and be widely adopted it must address key concerns, chief among them privacy risks. Cross-border CBDCs could potentially increase the scale, scope, and speed of breaches threatening users' privacy.[1] To develop safe cross-border CBDCs, participating countries will therefore need to align their technological frameworks and regulatory standards at the outset of development.

The EU has been experimenting with cross-border CBDCs since 2019. It has also been responsive to private sector developments, particularly stablecoins, as evident with the provisional agreement on the Markets in Crypto Assets (MiCA) regulation. Moreover, the EU has several privacy protections for consumer data, and the General Data Protection Regulation (GDPR) sets out strict rules for personal data storage, processing, and transfer to third parties for all EU residents. In the US, privacy is understood differently. Data protection laws are defined sectorally, and consumer data law is protected by states or created by case law. As both the EU and the US develop a wholesale CBDC, these differentiated privacy regulations between the EU and the US need to be harmonized. The looming alternative is a web of different technology choices and standards that could result in inadequate interoperability between different CBDCs, threaten financial stability as well as citizens' data, and undermine CBDCs' promise of improved cross-border transactions.

In view of these risks, we argue that the US and EU should work together alongside other partners to create the technological and regulatory environment to enable privacy-preserving cross-border CBDCs. The US and EU should seize the emergence of CBDCs as an opportunity to finally establish a transatlantic privacy framework. Further, they should streamline its interplay with the prevention of money laundering and financing of terrorism (AML/CFT/CPF). More broadly, both should harness the clout of their combined financial systems to develop digital asset regulation and standards with a global reach and democratic values. In keeping with the techno-regulatory approach of this paper, the following regulatory recommendations are based on the technical findings highlighted in section 3:

1. Recommendation 1: Policy makers must seize the opportunity presented by the global interest in CBDCs to establish the necessary regulatory background for successful multi-CBDC models
2. Recommendation 2: Multi-CBDC frameworks, at the most basic level, impact messaging formats, data frameworks, and AML/CFT/CPF requirements. These need to be standardized across jurisdictions.
3. Recommendation 3: The initial phase of multi-CBDC should also include an assessment of different data-sharing mechanisms, and the risks arising in different scenarios.
4. Recommendation 4: All jurisdictions must agree upon the adequate privacy-transparency trade-off and on the right enforcement and implementation mechanisms.
5. Recommendation 5: Greater regulatory alignment, which includes a transatlantic privacy and data protection framework, is needed to enable any successful deployment of multi-CBDC involving the EU and the US.

INTRODUCTION

In a global interconnected economy, cross-border payments—i.e., transactions in which the sender's and recipient's accounts are located in different jurisdictions—are growing at a rapid pace. The total cross-border flow is estimated to reach $156 trillion in 2022,[2] and more than $250 trillion by 2027.[3] Cross-border payments influence economic relationships and uphold the mobility of people, goods, services, capital, and emerging business lines and models.[4] Making these transactions faster, cheaper, and inclusive, without threatening safety and security, is a top priority for the Group of Twenty that requires public-private cooperation, enhancing current systems, and exploring new technical and financial solutions.[5] While these transfers traditionally rely on banks, new players now provide alternatives that meet the needs of consumers and emerging markets.[6] Hence, central banks and monetary authorities must assess their future role in this field.

The same institutions are increasingly experimenting with Central Bank Digital Currencies (CBDCs). Although most efforts have focused on domestic CBDCs,[7] the acknowledgement of the current critical role of international payments in both wholesale and retail systems drove several pilot programs to explore the design and capabilities of cross-border CBDCs, also known as multi-CBDCs. Early on in these projects, the interplay between technology and regulation emerged.[8] CBDC models are influenced by, and have an impact on, a wide array of requirements—e.g., privacy and data protection, financial

transparency, prevention of money laundering and financing of terrorism and proliferation (AML/CFT/CPF), and monetary law.

These requirements are delicately intertwined with the technological design. At one extreme, certain designs enable full transparency for regulators via sweeping data collection, spurring fears of government surveillance. At the other extreme, centralized transaction data collection can be minimized, challenging regulatory compliance. Although domestic CBDCs are not immune to privacy/transparency concerns, the multi-CBDC setting enhances them. Due in part to differing regulatory and geopolitical frameworks, the projects may embed different technical choices, which impact the resulting properties of the system. How to overcome discrepancies in a cross-border CBDC is a complex question without a single, clear answer.

In this paper, we explore the interplay between multi-CBDC models and the regulatory domains of privacy and data protection and AML/CFT/CPF.[9] Our goals are to show the main privacy/transparency impacts of various technical design decisions—both from a wholesale as well as a retail payment perspective—and to provide regulatory recommendations for an efficient approach to their management in a US-EU collaboration scenario.

1. THE ROAD TO MULTI-CBDCS

Cross-border transactions can be performed between financial institutions for settlement purposes—i.e., wholesale transfers—or they can consist of transfers where the payer and payee are consumers and businesses—i.e., retail transfers. Besides having different objectives, the two types of transfers differ in size: retail transactions make up the vast majority of payments by number, but only a small fraction of total value, while wholesale transactions comprise almost the entire value of payments, but their number is (relatively) small.[10]

Today, the most common model (but not the only one) for cross-border payments is the correspondent banking system, which passes transactions through a network of intermediary financial institutions. The correspondent banking network is slow, expensive, and difficult to automate. These difficulties arise because of several practicalities, which include:

1. Different domestic banking systems have different engineering specifications, including character encodings and field demarcations.
2. A transaction may be checked many times for compliance with local regulations regarding financial crime. Each check may involve a different intermediary, with differing standards; there are different supervision and oversight models.[11]
3. Banks only update their balance sheets during normal business hours. This causes delays as transactions pass between banks in different time zones, while also forcing banks to keep on hand enough cash to cover the foreign exchange rate.
4. Quick settlement requires banks to pre-allocate funds, often in other jurisdictions. This capital cost increases overhead and risk for banks, which manifests as high fees.

Cross-Border CBDCs

A cross-border CBDC, or multi-CBDC, is a term that describes one or more systems that automatically handle cross-border payments between domestic CBDCs. Although the majority of ongoing CBDC projects are domestic in nature,[12] the importance of cross-border payments led both central banks and independent researchers to explore requirements and implementation of cross-border CBDCs.[13]

Multi-CBDCs offer at least two key advantages over existing systems. First, by building a consistent, interoperable digital platform, many compliance and validity checks that currently slow down correspondent banking could be automated and integrated. Second, a multi-CBDC could reduce or eliminate the need for intermediaries by allowing banks to directly hold foreign CBDCs. For example, a European bank could directly hold digital dollars (and transact in them) without requiring the cooperation of a correspondent bank in the United States. This reduces the overall friction of transacting, which in turn reduces latency and fees for end users.

No multi-CBDCs have been deployed to this day, but groups of countries have launched pilot studies to evaluate the options (see Table 1).[14] How to best design a multi-CBDC is an open question that raises technical, organizational, and governance challenges. Most projects have so far focused on wholesale scenarios between two-tier domestic models. In two-tier or hierarchical multi-CBDCs, a core tier of nodes (e.g., central banks, select commercial banks, select non-banks) run the validation core, whereas other participants (e.g., other banks, users in a retail system) participate by establishing relationships with a core node.

Table 1. Existing Multi-CBDC Pilot Studies

Year	Project	Participants	Scope
2018–19	Jasper-Ubin phase IV	Bank of Canada and Monetary Authority of Singapore	Builds on phase III of Projects Jasper and Ubin to explore a cross-border, -currency, and -platform payments system, testing interoperability between Corda and Quorum
2019	Stella phase III	European Central Bank and Bank of Japan	Experiments with synchronized cross-border payments between (i) distributed ledgers, (ii) centralized ledgers, and (iii) distributed and centralized ledgers
2019–20	Aber[15]	Saudi Arabian Monetary Authority and Central Bank of the U.A.E.	Explores the feasibility of a single dual-issued digital currency as an instrument of domestic and cross-border settlement

2019	Inthanon-LionRock[16]	Hong Kong Monetary Authority and Bank of Thailand	Explores the deployment of Distributed Ledger Technologies (DLTs) to increase efficiency in cross-border transfers by having a cross-border corridor network work as a bridge between two DLT-based local networks
2021	Inthanon-LionRock phase II[17]	BISIH Hong Kong Center, Hong Kong Monetary Authority, and Bank of Thailand	Explores the use of DLTs to aid real-time cross-border transfers using an atomic payment versus payment mechanism for transactions between two different jurisdictions
2021	Multiple mCBDC bridge[18]	BISIH Hong Kong Center, Hong Kong Monetary Authority, Central Bank of the U.A.E., Bank of Thailand, and People's Bank of China	Builds on Project Inthanon-LionRock II to develop a DLT platform through which multiple central banks issue their CBDC to participants that can perform P2P payments and redeem the CBDC for reserves at the issuing central bank
2021	Jura[19]	BISIH Swiss Center, Bank of France, and Swiss National Bank	Explores the direct transfer of euros and Swiss francs between commercial banks on a DLT platform operated by a third party
2021–22	Dunbar[20]	BISIH Singapore Center, Reserve Bank of Australia, Central Bank of Malaysia, Monetary Authority of Singapore, and South African Reserve Bank	Involves two DLT-based prototypes for a platform for settlements through digital currencies issued by multiple central banks to facilitate direct cross-border transactions between financial institutions in different currencies

Source: Table created by Nadia Pocher

European Commissioner for Values and Transparency Vera Jourova and European Commissioner for Justice Didier Reynders (R) give a news conference on EU rules on data protection (GDPR) and the new EU Strategy on victims' rights, in Brussels, Belgium, June 24, 2020. Olivier Hoslet/Pool via REUTERS

2. PRIVACY AND TRANSPARENCY REQUIREMENTS

We begin this section by outlining a framework for thinking about the privacy implications of a cross-border CBDC. We first define the main stakeholders in a cross-border CBDC, followed by the main privacy and transparency requirements for a typical transaction.

Stakeholders

We identify seven main types of stakeholders in a typical payment over a cross-border CBDC:

1. **Sender and receiver:** In a retail setting, a payment sender (respectively, receiver) is associated with a sending (respectively, receiving) bank, which has accounts carrying the CBDC in which the transaction is denominated. In a wholesale setting, the sender (respectively, receiver) is itself a sending bank.

2. **Intermediary financial institutions:** These institutions are expected to enable cross-border transactions by providing services such as foreign exchange, customer onboarding, or compliance checks, to name a few.

3. **Central banks:** Cross-border transfers will be settled by updating CBDC ledgers. Issuing central banks for the sender and receiver's CBDCs may see transaction details, depending on the domestic CBDC architecture. In addition, other central banks could possibly have visibility into the global ledger.

4. **Validators:** Multi-CBDC designs typically rely on the existence of validators whose job it is to check the validity of each transaction. These validators could be run by banks (commercial or central), as well as non financial institutions.

5. **Third-party service providers:** Multi-CBDC pilots currently rely on public-private partnerships, with third parties providing key code, infrastructure, and services (e.g., cloud service providers, network operators).

6. **Oversight bodies:** Regulatory or oversight bodies are likely to need access to (parts of) the cross-border CBDC ledger. In particular, there are different regulators in different jurisdictions, and each may have different, and changing, requirements.

7. **Third-party observers:** A multi-CBDC may involve the participation of third parties that are not directly involved in a given transaction, including other users and advertisers, or third parties that attempt to purchase or otherwise access user data.

Privacy, Data Protection, and Transparency Requirements

In addressing privacy and transparency in CBDCs, we want to clearly distinguish between privacy—which controls how much data is ingested and shared within the system, and how it is used or disseminated—and data protection, which aims to prevent unauthorized access to data after it has been collected.[21] From a legal perspective, privacy and data protection are closely connected, but refer to two separate rights. While privacy is recognized as a universal human right (e.g., the Universal Declaration of Human Rights), data protection is not.[22]

The approach to privacy and data protection in the United States is different from that in the European Union (EU). In the United States, privacy is safeguarded by sector, primarily from governmental intrusion. Typically, consumer data is treated as property and relevant civil rights are set by case law. In the EU, the rights to privacy and data protection are enshrined in the European Convention on Human Rights, the EU treaties, and the Charter of Fundamental Rights of the European Union. The protection of personal data is addressed extensively by the General Data Protection Regulation 2016/ 679 (GDPR),[23] with rules directly applicable at the member state level, and by Law Enforcement Directive 2016/680.

The GDPR has extensive cross-border impacts: EU and non-EU-based entities handling, accessing, or processing personal data of EU residents must comply,[24] and the transfer of personal data to third countries is subject to strict conditions.[25] The different legal and policy approaches challenge—and may, at times, disrupt—transatlantic data flows and bilateral trade. Sector-specific agreements did not erase concerns about the impact of US intelligence and surveillance laws on personal data of EU citizens, as testified by the Court of Justice of the European Union's Schrems II decision.[26] Now, discussions on a Trans-Atlantic Data Privacy Framework are ongoing.[27]

In addition to privacy and data protection, financial institutions must comply with AML rules.[28] At times, the two domains include incompatible requirements, and fragmentation cripples international transactions.[29] Several patterns can be noted regarding the data types a multi- CBDC might need to process for AML purposes, due to the risk-based approach laid out by the Financial Action Task Force (FATF).[30] The framework largely thrusts on regulated entities the decision on the extent of data to collect, which increases their responsibility for balancing transparency and privacy.[31]

Data Types

In principle, the types of data protected by privacy and data protection regulations are broader than those covered by AML regulations. However, the data types collected for AML purposes, chiefly related to identifying individuals and monitoring their financial transactions, are generally the ones that pose the most obvious privacy and data protection risks in a CBDC scheme. Usually, an AML-compliant regulated entity collects and retains for five years (after the end of the business relationship/occasional transaction) the following:[32]

Customer and beneficial owner information. This includes data on customer identification and contact information (e.g., phone number, e-mail, address). For individuals, data ordinarily includes name, surname, ID/passport number, nationality, date of birth; for legal entities (e.g., companies, trusts, other legal arrangements), it includes the country of incorporation and the nature of the entity's business, information on the entity's directors, and beneficial owners.

Account information. This includes account details such as the intended purpose of the account and the expected location of transactions. Such data can be valuable for transaction monitoring and to increase confidence in abnormal activity alerts.

Transaction information. This includes transaction records and patterns, including sender, receiver, amount, and modality (e.g., credit). It can also include associated metadata such as timestamps, IP addresses, whether the transaction succeeded or failed, and any accompanying analysis used to detect suspicious transactions.

Sharing Mechanisms

In principle, Know Your Customer (KYC) data is not by default available to the authorities, nor to other public or private third parties. However, sharing takes place in different circumstances, listed below.[33]

Pre-suspicion information sharing (private-to-private).
This refers to data sharing that occurs prior to flagging a transaction, as a blanket precaution. Such data is shared (often in real time) with service providers like analytics companies and other RegTech (Regulatory Technology) firms that increasingly support automated KYC checks and monitoring.[34] In the same context, data can be shared with other financial firms. Data is also shared on a regular basis for operational reasons, such as correspondent banking or to process wire transfers.[35]

Post-suspicion information sharing (mostly private-to-public, but also public-to-private and public-to-public).
Some data is shared after identifying suspicious activity, when filing Suspicious Transactions Reports (STRs), known in some countries as Suspicious Activity Reports (SARs). The typical information flow sees the regulated entity filing the report to the national Financial Intelligence Unit (FIU) (private-to-public data sharing), and the FIU sending financial intelligence to other competent authorities. The data types shared in post-suspicion data sharing are extensive, including information on transferred amounts, identities of the parties involved, and historic transaction patterns.[36]

Aggregate information sharing (private-to-public).
Financial institutions have several obligations, not only AML-related, to submit aggregated data to the authorities for supervision and/or statistical purposes—e.g., cash transactions, regulatory returns for banking supervision. No personal data is usually involved. The sharing is monthly, quarterly, or yearly, with FIUs and supervisory authorities. Data can be financial (e.g., balance sheet) or operational (e.g., number of a specific type of transactions).

Supervisory access (private-to-public, public-to-public).
In other circumstances, supervisory authorities, sometimes the FIU itself, perform routine checks without a previous submission of an STR/SAR or the opening of an investigation. In other cases, Law Enforcement Agencies (LEAs) and supervisory authorities may share information. Further, national FIUs are routinely sharing information with each other, and domestic LEAs do the same.

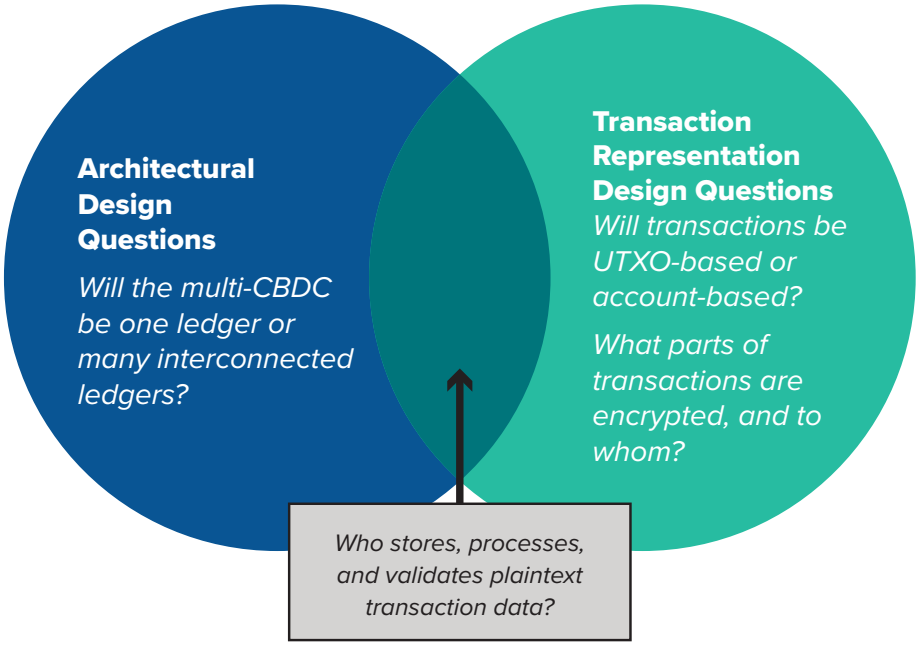
Other information-sharing mechanisms (private-to-public, public-to-public).
Regulatory frameworks other than AML may provide for the use of data collected and retained for AML for other reasons, such as for tax purposes. In these cases, other authorities can have access to the information, to different extents. Usually, these authorities access data previously shared by the regulated entity with other authorities. The stakeholders involved in this type of data sharing could be classified as oversight bodies or third-party observers.

U.S. Federal Reserve Chair Jerome Powell testifies before a House Financial Services Committee hearing in Washington, U.S., June 23, 2022. REUTERS/Mary F. Calvert

3. HOW MULTI-CBDC DESIGNS AFFECT PRIVACY AND TRANSPARENCY

The privacy and transparency properties of a multi-CBDC depend heavily on the underlying technical design. Existing pilots have largely relied on enterprise blockchain solutions (e.g., Corda, Quorum, Hyperledger Fabric, Hyperledger Besu, Elements), and they make different choices about how to disseminate and represent transactions in order to provide privacy with respect to various stakeholders. In doing so, various designs necessarily make trade-offs in terms of efficiency, security, and transparency. In this section we outline different design choices and show how they can impact a multi-CBDC's privacy and transparency. These design choices can be broadly categorized into architectural choices—i.e., choices that impact the roles and relationships between processes and software systems—and transaction representation choices—i.e., choices that control the way in which transactions are encoded (e.g., encryption), and how this impacts the flow of information to various stakeholders. Figure 1 summarizes the design choices discussed in this article, and whether each is architectural and/or representational.

Figure 1. Design questions for a multi-CBDC that impact privacy and data transparency.



Source: Figure created by Giulia Fanti

Design Choice: Single Ledger or Multiple Interconnected Ledgers?

The first design choice we consider is purely architectural. Namely, will the multi-CBDC maintain a single ledger, or will it interconnect separate ledgers? Most existing multi-CBDC pilot studies have focused on interconnecting separate ledgers. Single-ledger systems are beneficial from an interoperability and ease of implementation standpoint. On the other hand, in architectures that interconnect existing ledgers, cross-border transactions must be recorded on both parties' ledgers (e.g., using cross-chain atomic swaps).

In cases where the parties use different ledger models, one party's privacy preferences may be at odds with the counterparty's ledger implementation. In the Project Jasper-Ubin multi-CBDC pilot, for example, Canada was running Corda, whereas Singapore was running Quorum. As we show in Table 2, these two tools make different implementation choices with regard to storage of private data. Hence, in interconnected ledgers, the final privacy properties of any given transaction will depend on the ledger designs of the sender, receiver, and any intermediaries.

Design Choice: Which Nodes Receive, Store, and Process Transactions?

The next design choice combines architectural considerations with data representation ones. Most enterprise blockchain solutions allow senders to specify that a transaction is private. This typically means only a subset of ledger participants can receive, store, and/or decrypt the transaction. In Table 2, we categorize different Distributed Ledger Technology (DLT) solutions in terms of two questions:

1. Which nodes receive and/or store private transactions? Here, we do not distinguish between encrypted or unencrypted data.

2. Which nodes have plaintext (unencrypted) access to full details of private transactions? This could either mean that a party is able to decrypt an encrypted private transaction, or it could mean that the transaction was not encrypted in the first place.

The gray boxes in Table 2 indicate impossible options. In each category, we list existing DLT solutions, as well as multi-CBDC pilot projects that have used them.[37] We also include DLT solutions from the cryptocurrency world, such as Zcash and Bitcoin, as points of comparison.

Table 2. Architectural Designs of Existing Multi-CBDC Pilot Studies

	Only sender and receiver	Validators	All nodes
Only sender and receiver	**Corda + non-validating notaries** **Hyperledger Besu** • Inthanon-LionRock		**Quorum** • Project-Jura • Jasper-Ubin **Zcash**
Validators		**Corda + validating notaries** • Project Dunbar • Project Jura • Inthanon-LionRock • Jasper Union • Project Stella **Hyperledger Fabric** • Project Aber • Project Stella	
All nodes			**Bitcoin, Ethereum**

For example, Quorum—which has been evaluated in Project Jura—broadcasts encrypted private transactions to all nodes, but only the intended counterparties are able to decrypt the transaction. In existing implementations, the implication has been that even validators cannot fully execute (and hence, validate) private transactions; instead, Quorum nodes maintain a private ledger that is not globally synchronized.[38] On the other hand, Corda—which has been used in Projects Dunbar, Inthanon-LionRock, and others—sends private transactions in a point-to-point manner only to the intended recipient and designated validators (known as validating notaries). This exposes full transaction details to the validating notaries.

TAKEAWAY:

Most existing multi-CBDC designs only send transactions (whether encrypted or not) to nodes that are also intended to process them in plaintext.

DLT nodes are responsible for two main functionalities: transaction validation and ledger storage. When it comes to private transactions, many common DLT designs take an all-or-nothing approach to assigning roles to nodes: either nodes store *and* process private transactions, or they do neither of the two (Table 2). This rule of thumb is not strictly necessary, nor is it universal.

At face value, the all-or-nothing approach to assigning roles for private transaction processing is reasonable from a privacy and efficiency standpoint. However, this strategy can have important security implications. It forces the system to make stronger trust assumptions on the validation process. For example, in a system like Corda, only the designated validators (known as validating notaries) are given access to private transactions, and they are fully responsible for validation; there is no Byzantine fault-tolerant agreement protocol in place to withstand corruptions from a subset of validating nodes. As such, if validators are compromised, the ledger can violate basic safety constraints, enabling attacks like double-spending of funds. Although this implies that validators must be fully trusted, these types of trust assumptions are not typically made explicit in writings on multi-CBDC.

TAKEAWAY:

Multi-CBDC pilots should explicitly document assumptions they are making in their threat model, particularly when navigating tensions between privacy and security. These assumptions should drive technology choices.

Many (multi-)CBDC studies do not explicitly state their threat model, including assumptions about which parties are trusted, and in what regard. Instead, they appear (understandably) to have chosen a technical solution based on existing enterprise DLT offerings, each of which comes with its own, often implicit, threat model. We recommend that multi-CBDC projects explicitly state their assumptions about which parties are trusted, and in what circumstances. These assumptions should then be used to justify technical choices.

Design Choice: Are Transactions UTXO or Account-Based?

There are two common ways of representing transactions in ledgers. The first is account-based; this means transactions (or smart contracts) must be associated with a specific account with a specific balance; the account can be controlled by a user or even another smart contract. The second model is the Unspent Transaction Output (UTXO) model. Transactions are represented by unique identifiers; new transactions must specify which coins (old transactions) they draw from. UTXO models have been more popular in systems that do not require complex smart contract functionality and/or when efficient validation is of paramount importance.

Table 3 lists the benefits and drawbacks of these two models, both in terms of privacy and transparency, and in general.

Table 3. Advantages and Disadvantages of the UTXO and Account Models, Particularly with Regard to Privacy and Transparency

Model	Properties	Pros	Cons
UTXO	Privacy	Transactions are not directly linked to a sending account Compatible with many cryptographic privacy enhancements[39]	Each token's trajectory can be traced across the entire ledger
	Transparency		Less transparency into the overall transaction volume, balance of a user
	General	More efficient transaction validation (can be processed in parallel)	More complex conceptual model More difficult to implement complex smart contract functionality Less efficient transaction creation
Account	Privacy		Makes it easier to link together transactions from the same user Privacy add-ons require multiple accounts to be locked[40]
	Transparency	Easier to reason about a user's total balance, aggregate transaction volumes, or transaction rates over time	
	General	Conceptually simpler	Harder to parallelize transaction validation

Source: Table created by Giulia Fanti

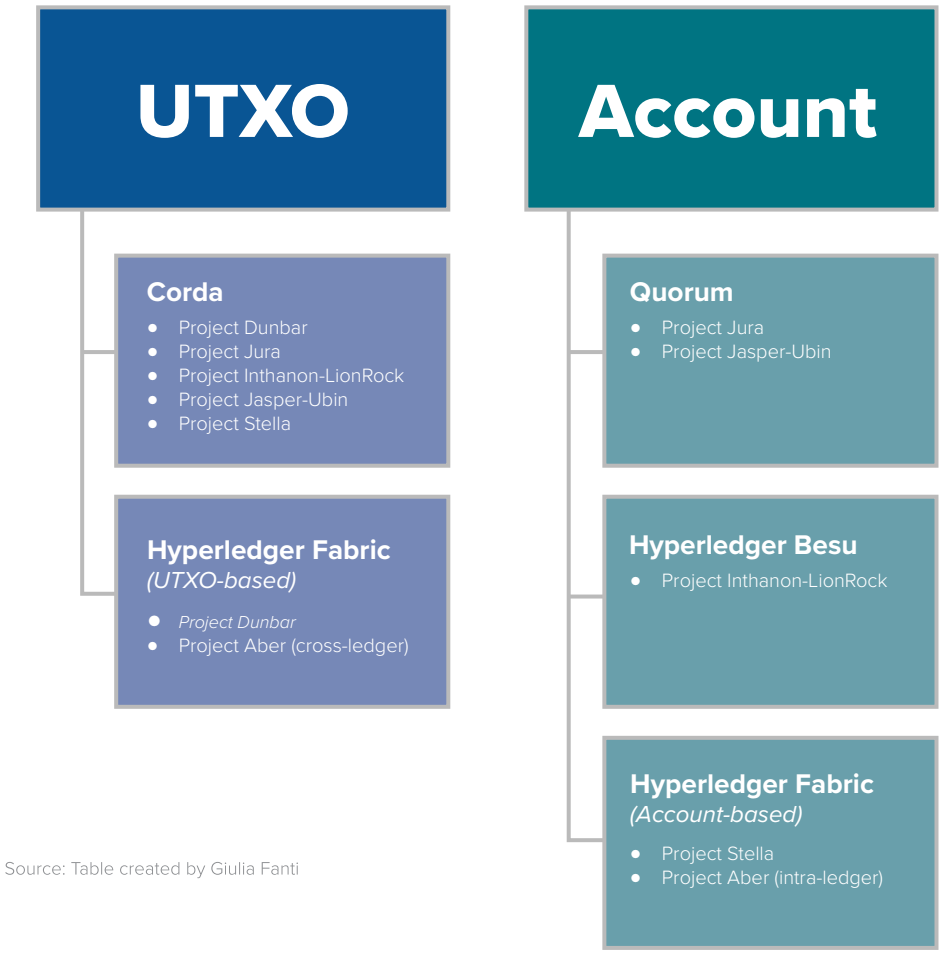
TAKEAWAY:

The UTXO model is often (but not always) slightly more compatible with privacy mechanisms and efficient (parallel) transaction processing, whereas the account-based model is often (but not always) more compatible with flexible smart contract functionality and transparency.

This statement is a generalization—there exist tools for providing privacy in account-based models, and options for providing transparency in UTXO-based systems. There even exist hybrid models, which combine the strengths of both.[41] A CBDC design should choose its transaction model carefully, taking into account a government's internal privacy, transparency, and performance requirements.

In practice, multi-CBDC pilots have used both UTXO models and account-based models. In fact, it is possible to create interoperable ledgers that run different transaction models; for example, in Project Jasper-Ubin, Singapore was running Quorum (an account-based DLT) and Canada was running Corda (which is UTXO-based).[42] As shown in Figure 1, there has been a fairly even split of UTXO versus account-based multi-CBDC pilot studies. We speculate the choice of transaction model appears to have been dictated by enterprise DLT offerings.

Figure 2. Transaction Models Used in Existing Multi-CBDC Pilots



Source: Table created by Giulia Fanti

Design Choice: How Are Transactions Encrypted or Encoded?

Data encoding refers to the way data is represented. For example, is a transaction (partially) encrypted prior to sending it over the network? If so, how is it encrypted, and with whose encryption keys? We note several common data encoding techniques that enhance privacy.

Subdivision of transactions. A common trend among enterprise DLT platforms is to decompose transactions into components that can be separately cryptographically encoded. The main benefit of this approach is that different parts of the transaction can be processed (e.g., validated) by different sets of nodes, thereby limiting what information each party needs to see. This approach is taken by Corda, which provides transaction tear-offs; these use a data structure called Merkle Trees to enable validators to see only specific parts of a transaction, while still being able to verify the transaction signature's validity. While this approach limits leakage of data, ultimately validators still need to see transaction data to validate it. To the extent validators may not be fully trusted, this presents a privacy concern.

Zero-knowledge proofs (ZKPs). ZKPs are a cryptographic construction that allow a party to prove they know some secret quantity without revealing it. For example, they could allow an account holder to prove they have sufficient funds in their account without revealing their balance to a validator. ZKPs are one of the most powerful technical tools for enabling both privacy and compliance. Nonetheless, for the most part, existing multi-CBDC pilots have not experimented extensively with ZKPs. One issue is that different reporting requirements for different ledgers would require different ZKPs, which requires more implementation overhead.

Interoperability of data encodings

In interlinkages of existing ledgers, the most common way to process cross-border transactions is through a technique called cross-chain atomic swaps. Suppose Alice wants to send $10 to Paulo in Brazil, but he wants to receive the money in Brazilian reals, cross-chain atomic swaps can use an intermediary (Charlie) to facilitate the exchange without needing to trust the intermediary. Instead, each party places a specially formed transaction on their local ledger. Upon verifying the other parties' transactions, Alice can initiate payment to the intermediary without worrying about the latter stealing her funds.

In cross-chain atomic swaps, counterparties need visibility into both ledgers over which the swap is happening; they must verify that each party's transaction was committed properly. This technical requirement may be challenging to combine with domestic privacy requirements. For example, if one of the ledgers (say the digital real) were hypothetically obfuscated using ZKPs to encode all transactions, then Alice (who is based in the United States) might not be able to verify that Charlie committed his ledger on the real ledger correctly.

TAKEAWAY:

In a multi-CBDC architecture (especially one that interlinks ledgers), cryptographic privacy protections must be deployed carefully to ensure interoperability, including different privacy or transparency requirements across jurisdictions and over time. These concerns are less severe, but still present, in the single-ledger model.

4. REGULATORY RECOMMENDATIONS

Wholesale and retail cross-border payments are an inherent component of a globalized economy, and they will continue to develop alongside technology. Multi-CBDCs are an appealing option to improve by-design cross-border and cross-currency payments,[43] and they are inextricably linked to regulation. Payment systems are often part of a broader policy agenda, and regulation drives standardization and enables cross-border cooperation.[44] Against this backdrop, our recommendations range from general to specific suggestions.

Multi-CBDCs and Regulation: A Two-Way Process

Although multi-CBDCs could make cross-border payments resemble the seamlessness of many domestic systems, they generate considerable challenges and possibly adverse effects—e.g., on local currency, capital control, macroprudential policies.[45] Many problems of cross-border transfers are influenced by regulation and diverging local requirements. Payment operations must comply with domestic rules, and despite international standards there can be significant implementation differences and controversial cross-border interplays.

These issues can be managed through design and multilateral coordination. In order to do so:

- The jurisdictions involved have to agree on techno-regulatory standards. CBDCs can be the opportunity to align regulatory and supervisory frameworks, review the interaction between data frameworks and cross-border payments, and harmonize KYC requirements.[46]
- Cross-border considerations must be addressed in the design phase of a CBDC project, which means devising from the start a plan to handle the international dimension of the model. Setting up the appropriate architecture and governance scheme is crucial, given the involvement of many central banks and possibly financial institutions and private partners.
- The model must be compliant by design with the crucial pieces of regulation that concern the payments domain—e.g., privacy and data protection and AML regime.

TAKEAWAY:

The existing challenges of incompatible regulatory regimes can further complicate the implementation and design of multi-CBDCs. Hence, we must seize the opportunity presented by the global interest in CBDCs to establish the necessary regulatory background for successful multi-CBDC models.

To devise a cross-border CBDC model that is compliant by design, regulatory issues should be addressed early on. The opportunity offered by the interest in CBDC plans should be seized upon to discuss regulatory provisions and their use as the solid basis for an effective and efficient multi-CBDC model that offers actual improvements vis-à-vis the current solutions. The current incompatibilities between (a) privacy and data protection, and AML, and (b) the US and the EU's approaches challenge cross-border data flows.

Standardization and Interoperability

A multi-CBDC can aim to enhance or transform international payments. Either way, it needs interoperability: domestic systems should offer cross-currency capabilities; in public-private models, users of various providers should be able to transact with each other; and a cross-border CBDC should be interoperable with domestic schemes.[47] Hence, it is necessary to develop technical, regulatory, and supervisory standards, mirroring "a common language and sets of expectations."[48] In CBDCs, the value of standards was stressed in many areas.[49] In particular:

- ISO 20022 has emerged as the default messaging standard for payments, and the adoption of a harmonized version is key to enhance cross-border transactions.[50] In multi-CBDCs, it is important also to ensure interoperability with domestic architectures;
- Consistent vision of the interplay of data frameworks with cross-border payments. Harmonization and technology-agnostic design of API protocols for data exchange to ensure interoperability as needed for cross-border information exchange;[51]
- Establishment of harmonized frameworks for AML requirements such as KYC, digital ID, red flag indicators, STR/SAR.[52] Although current incompatibilities can be mitigated by technology, consistent regulation would streamline its development considerably.

Information Sharing

Multi-CBDCs could facilitate data sharing with supervisors. A consistent technical foundation can enhance efficiency and quality, and level the compliance field for small and large firms. Data protection and privacy concerns can be addressed through cryptography and advanced data partitioning. If supervisors are among the maintaining nodes, they could take action in case a suspicion arises. This requires careful public-private allocation of responsibilities. Multi-CBDCs also enable regulated entities to share data among themselves, to increase compliance efficiency and effectiveness—e.g., avoid multiplication of efforts.[53]

Most surveillance concerns pertain to private-to-public sharing, but regulatory conundrums (e.g., legal basis) arise with private-to-private sharing. The design of the multi-CBDC must consider these differences. Besides falling under different restrictions (different data can be shared), they generate specific problems in terms of what data authorities can access, what information can be shared with them and other private entities, under which circumstances, and what data other private entities can see without a case-by-case assessment (e.g., analytics).

TAKEAWAY:

A multi-CBDC plan should assess allowed data-sharing mechanisms, clarifying the risks arising in private-to-private, private-to-public, and public-to-public scenarios.

The involved stakeholders are likely to have different perspectives on which sharing models are acceptable, and on the safeguards to be provided across the framework. Hence, this process should take place early in the multi-CBDC discussion. All involved jurisdictions should be encouraged to discuss specific design options that can meet their individual and/or common expectations.

Privacy/Transparency Trade-Offs

Cashless payments produce a huge amount of data about transactions, parties, timing, location, and products/services. This data is of great commercial value, and systems of credit scoring add information such as address, age, gender, and timeliness of payments.[54] Given the increasing capabilities to exploit data for various purposes, CBDCs must ensure privacy and confidentiality by design. Meanwhile, transaction monitoring and tracing opportunities offered by a DLT-based cross-border CBDC provide an unparalleled asset in the fight against financial crime. Fortunately, privacy and transparency requirements are not a zero-sum game, but mirror the trade-off between the need for financial confidentiality and auditability.[55]

To enable concurrent compliance with privacy and transparency requirements, the type and/or amount of anonymous transactions can be restricted.[56] Different models have been proposed and usually involve multiple wallet types according to the risk-based approach (higher risk, stronger restrictions) to reach a suitable privacy/transparency trade-off. In an international project, the trade-off has to be agreed upon by all jurisdictions involved. This is a key reason to heed the cross-border dimension early on. Regulatory reforms may be required before the implementation of the model, and likely involve multi-stakeholder negotiation.

TAKEAWAY:

All jurisdictions involved in a multi-CBDC project should define their preferred privacy/transparency trade-off, and be familiar with the options to implement it.

This is a necessary step to reach a compromise with all stakeholders involved in an efficient way, as well as to engage in a discussion on the ways to implement the chosen model from the perspectives of architecture and data representation.

U.S. Secretary of State Antony Blinken, U.S. Secretary of Commerce Gina Raimondo, European Commission Vice President and Commissioner for Competition Margrethe Vestager, European Commission Vice President and Commissioner for Trade Valdis Dombrovskis, and France's Foreign Minister Jean-Yves Le Drian. May 15, 2022. REUTERS/Kevin Lamarque/POOL

What Now?

To enable the efficient deployment of a US-EU cross-border CBDC scheme, we believe it is important to prepare the transatlantic regulatory environment in advance. As confirmed during the July 2022 US-EU Joint Financial Regulatory Forum, cooperation is key to meet the challenges arising in this sphere.[57] Cross-border dialogue on initiatives such as the EU MiCA regulation emerges as crucial.

From a broader perspective, we provide the following recommendations:

- Develop a transatlantic privacy and data protection framework with specific focus on financial and payment-related data;
- Agree on common implementation principles of the FATF Recommendations—e.g., joint risk assessments, joint red flag indicators to foster harmonized implementation;
- Narrow the gap between the two regulatory domains, address them together to establish suitable privacy/transparency trade-offs;
- Establish a body to translate the previous points into techno-regulatory standards, embed them by design in the multi-CBDC, and update/monitor them as needed.

TAKEAWAY:

Regardless of whether a decision is taken to implement a multi-CBDC scheme, regulatory coordination and technology pilots should be performed to lay the foundation for such a project.

CONCLUSION

The development of a shared vision of the future of cross-border payments is at the forefront of the current international agenda.. As explored in this paper, many key questions raised by multi-CBDC initiatives are hybrid in nature, situated at the intersection of technology and regulation. This is not surprising, but can generate uncertainties that stall development, especially in a multi-jurisdictional context. For this reason, we believe it is crucial to focus on the value and power of this interplay.

In our view, an essential goal of a multi-CBDC model is to balance the efforts to safeguard the privacy of CBDC users and the protection of their data, with the endeavor to guarantee transparency as a critical instrument to curb financial crime. This view grounded our analysis of privacy and transparency requirements, and of how they can be mirrored, but also affected, by architectural and data representation methods. Technical design options, however, do not exist in a vacuum. They cannot be made effectively and efficiently without a backbone comprising a consistent regulatory framework, standardization initiatives, and harmonization efforts. We believe the current worldwide interest in CBDCs offers an opportunity to address regulatory clarity as a preliminary objective, thus paving the road for a multi-CBDC model grounded in a strong consensus on its embedded privacy/transparency trade-off.

Acknowledgements

Nadia Pocher co-authored this report. Her research was funded by the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie International Training Network European Joint Doctorate G.A. No 814177

The authors would like to thank the leadership and staff of the Atlantic Council GeoEconomics Center and Atlantik-Brücke including Mrugank Bhusari, Sophia Busch, Kathy Butterfield, Katharina Draheim, Franka Ellman, Robin Fehrenbach, Julia Friedlander, Niels Graham, Cate Hansberry, Ananya Kumar, Charles Lichfield, Josh Lipsky, Ole Moehr, and Maia Nikoladze.

ENDNOTES

1 https://www.imf.org/en/Publications/fandd/issues/2022/09/Central-bankers-new-cybersecurity-challenge-Fanti-Lipsky-Moehr

2 Florian Seeh, "How New Entrants Are Redefining Cross-Border Payments," EY, February 23, 2021, https://www.ey.com/en_es/banking-capital-markets/how-new-entrants-are-redefining-cross-border-payments.

3 "Cross-Border Payments," Bank of England, last updated June 29, 2022, https://www.bankofengland.co.uk/payment-and-settlement/cross-border-payments.

4 Committee on Payments and Market Infrastructures, *Enhancing Cross-Border Payments: Building Blocks of a Global Roadmap*, Stage 2 report to the G20 — technical background report, July 2020, 2, https://www.bis.org/cpmi/publ/d194.pdf.

5 Financial Stability Board, *Enhancing Cross-Border Payments,* Stage 1 Report to the G20, April 9, 2020, 1, https://www.fsb.org/wp-content/uploads/P090420-1.pdf; Financial Stability Board, Enhancing Cross-Border Payments: Stage 3 Roadmap, October 13, 2020, https://www.fsb.org/2020/10/enhancing-cross-border-payments-stage-3-roadmap/; and Committee on Payments and Market Infrastructures, Enhancing Cross-Border Payments.

6 Seeh, "How New Entrants"; OMFIF (Official Monetary and Financial Institutions Forum), Digital Monetary Institute, *The Future of Cross-Border Payments: Evolution of Revolution?* 2021, https://www.omfif.org/wp-content/uploads/2021/12/Future_of_Payments_2021.pdf; and Elena Carletti et al., *The Bank Business Model in the Post-Covid-19 World: The Future of Banking 2*, 2020, https://media.iese.edu/research/pdfs/ST-0549-E.pdf.

7 "Central Bank Digital Currency Tracker," Atlantic Council, accessed August 10, 2022, https://www.atlanticcouncil.org/cbdctracker/.

8 Throughout this paper, the term "regulation" is purposefully used in a broad and jurisdiction-agnostic way. It includes laws, legislation, regulation, and standards.

9 In the remainder of this paper, the acronym "AML" reads "AML/CFT/CPF."

10 Financial Stability Board, *Targets for Addressing the Four Challenges of Cross-Border Payments: Final Report*, October 13, 2021, 6, http://www.g20.utoronto.ca/2021/FSB-Targets-for-cross-border-payments-roadmap.pdf; and Committee on Payments and Market Infrastructures, Cross-Border Retail Payments, February 2018, https://www.bis.org/cpmi/publ/d173.pdf.

11 BIS Innovation Hub, *Project Dunbar: International Settlements Using Multi-CBDCs*, March 2022, https://www.bis.org/publ/othp47.pdf.

12 "Central Bank Digital Currency Tracker."

13 Raphael Auer, Philipp Haene, and Henry Holden, "Multi-CBDC Arrangements and the Future of Cross-Border Payments," BIS Papers, No. 115, March 19, 2021, https://www.bis.org/publ/bppdf/bispap115.htm; Auer et al., "CBDCs Beyond Borders: Results from a Survey of Central Banks," BIS Papers, No. 116, June 11, 2021, https://www.bis.org/publ/bppdf/bispap116.htm; Hyunjun Jung and Dongwon Jeong, "Blockchain Implementation Method for Interoperability between CBDCs," *Future Internet* 13 (5) (133), https://doi.org/10.3390/fi13050133; Darrell Duffie, "Interoperable Payment Systems and the Role of Central Bank Digital Currencies" in *Finance and Insurance Reloaded*, Institut Louis Bachelier Annual Report, 2020, https://www.darrellduffie.com/uploads/policy/DuffiePaymentInteropMay2020.pdf; Dmitry Kochergin and Victor Dostov, "Central Banks Digital Currency: Issuing and Integration Scenarios in the Monetary and Payment System, Lecture Notes in Business Information Processing, 394: 111–119; Chusu He, Alistair Milne, and Markos Zachariadis, "Central Bank Digital Currencies and International Payments," SWIFT Institute Working Paper No. 2020-002, SWIFT Institute, May 2022, https://swiftinstitute.org/wp-content/uploads/2022/05/SWIFTInstitute_CBDCInternationalPayments_PublishedMay2022.pdf; Cheng-Yun Tsang and Ping-Kuei Chen, "Policy Responses to Cross-Border Central Bank Digital Currencies—Assessing the Transborder Effects of Digital Yuan," *Capital Markets Law Journal* 17 (2): 237–261, https://doi.org/10.1093/cmlj/kmac004; and INATBA (International Association for Trusted Blockchain Applications), "INATBA's Position on DLT-Based CBDC Development," July 20, 2022, https://inatba.org/news/inatbas-position-on-dlt-based-cbdc-development/.

14 As an example, see BIS Innovation Hub, *Project Dunbar,* 35.

15 Saudi Central Bank and Central Bank of the U.A.E., *Project Aber,* November 2020 https://www.sama.gov.sa/en-US/News/Documents/Project_Aber_report-EN.pdf.

16 Bank of Thailand and Hong Kong Monetary Authority, *Inthanon-LionRock: Leveraging Distributed Ledger Technology to Increase Efficiency in Cross-Border Payments,* January 2020 https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/Report_on_Project_Inthanon-LionRock.pdf.

17 Ibid.

18 BIS Innovation Hub, *Inthanon-LionRock to mBridge: Building a Multi CBDC Platform for International Payments*, September 2021, https://www.bis.org/publ/othp40.pdf.

19 Banque de France, Bank for International Settlements, and Swiss National Bank, P*roject Jura: Cross-Border Settlement Using Wholesale CBDC*, December 2021, https://www.bis.org/publ/othp44.pdf.

20 BIS Innovation Hub, *Project Dunbar*.

21 Geoffrey Goodell, Hazem Danny Al-Nakib, and Paolo Tasca, A Digital Currency Architecture for Privacy and Owner-Custodianship, Future Internet 13 (5) (130), doi:10.3390/fi13050130; and Giulia Fanti et al., *Missing Key: The Challenge of Cybersecurity and Central Bank Digital Currency, Atlantic Council GeoEconomics Center,* June 15, 11, https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/.

22 "Data Protection," European Data Protection Supervisor, accessed July 27, 2022, https://edps.europa.eu/data-protection/data-protection_en.

23 Under the GDPR, personal data processing must be backed by one of seven grounds, such as consent of the individual. Personal data is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR does not cover anonymized data but covers pseudonymized data.

24 This means data controllers, processors, and sub-processors fall within the scope of the regime.

25 Adequacy decisions, Standard Data Protection/Contractual Clauses, and Binding Corporate Rules.

26 Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Court of Justice of the European Union Schrems II Decision in Case C-311/18, July 16, 2020), https://curia.europa.eu/juris/liste.jsf?num=C-311/18.

27 Rachel F. Fefer and Kristin Archick, *U.S.-EU Trans-Atlantic Data Privacy Framework,* Congressional Research Service, updated June 2, 2022, https://crsreports.congress.gov/product/pdf/IF/IF11613 and European Commission, European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework, press release, March 25, 2022, https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087.

28 The term AML/CFT/CPF refers to a set of laws, regulations, and procedures that lays out preventive measures and sanctions to prevent criminals from enjoying illicit profits, financing terrorism, and proliferation of weapons of mass destruction. The framework centers on "regulated entities" (e.g., financial institutions, lawyers) providing "active cooperation" to the authorities by discovering and reporting suspicious activities.

29 Michelle Frasher, "Data Privacy and AML Rules on a Transatlantic Collision Course," American Banker, August 28, 2015, https://www.proquest.com/newspapers/data-privacy-aml-rules-on-transatlantic-collision/docview/1708155077/se-2; Iakovina Kindylidi, "The Data Protection Implications of the EU AML Framework: A Critical Overview & the Case of AI" in *Privacy Technologies and Policy*, eds. Agnieszka Gryszczyńska et al., 10th Annual Privacy Forum, APF 2022, Warsaw, Poland, June 23–24, 2022, Lecture Notes in Computer Science, 13279, https://doi.org/10.1007/978-3-031-07315-1_3; and He, Milne, and Zachariadis, "Central Bank," 3.

30 The Financial Action Task Force (FATF) is the intergovernmental, policy making, monitoring, and enforcement organization that sets standards and provides guidance on AML.

31 Marius Laurinaitis, Darius Štitilis, and Egidijus Verenius, "Implementation of the Personal Data Minimization Principle in Financial Institutions: Lithuania's Case," *Journal of Money Laundering Control* 24 (4): 664–680, 670, https://doi.org/10.1108/JMLC-11-2020-0128.

32 The list is elaborated on the basis of FATF Recommendations and FATF (Financial Action Task Force), *Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing*, July 2022, 62–63, https://www.fatf-gafi.org/media/fatf/documents/Partnering-int-the-fight-against-financial-crime.pdf.

33 Our account of sharing mechanisms includes a simplification of diverse jurisdiction-specific scenarios.

34 Alexandros A. Papantoniou, "Regtech: Steering the Regulatory Spaceship in the Right Direction?" *Journal of Banking and Financial Technology*, 6: 1–16, https://doi.org/10.1007/s42786-022-00038-9.

35 FATF (Financial Action Task Force), *Consolidated FATF Standards on Information Sharing*, updated November 2017, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Consolidated-FATF-Standards-information-sharing.pdf.

36 FIAU, *Suspicious Transaction Report* (STR), https://fiaumalta.org/wp-content/uploads/2020/06/STR.pdf and NCA (National Crime Agency), "Guidance on Submitting Better Quality Suspicious Transaction Reports (STRs)," October 2016, 4 https://www.clc-uk.org/wp-content/uploads/2018/01/Guidance-on-Submitting-Better-Quality-STRs.pdf.

37 In Hyperledger Fabric, we consider endorsers to be part of the validation process. Although the final ordering service (which creates an ordered ledger out of transactions) cannot see private transaction data, the endorsers are responsible for checking funds availability, and are able to see private transaction data.

38 "Public and Private Transactions," GoQuorum, last updated March 10, 2022, https://consensys.net/docs/goquorum/en/stable/concepts/privacy/private-and-public/#private-transactions.

39 Eli Ben Sasson et al., "Zerocash: Decentralized Anonymous Payments from Bitcoin" *in SP '14: Proceedings of the 2014 IEEE Symposium on Security and Privacy*, 459–474, DOI:10.1109/SP.2014.36; Sean Bowe et al., "Zexe: Enabling Decentralized

Private Computation" in *2020 IEEE Symposium on Security and Privacy* (SP), DOI: 10.1109/SP40000.2020.00050; and Daira Hopwood et al., *Zcash Protocol Specification*, August 2, 2022, https://zips.z.cash/protocol/protocol.pdf.

40 Benedikt Bünz et al., "Zether: Towards Privacy in a Smart Contract World" in Financial Cryptography and Data Security, 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020, https://doi.org/10.1007/978-3-030-51280-4_23.

41 Karl Wüst et al., "Platypus: A Central Bank Digital Currency with Unlikable Transactions and Privacy-Preserving Regulation," 2021, https://eprint.iacr.org/2021/1443.pdf.

42 Bank of Canada and Monetary Authority of Singapore, "Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies," Jasper-Ubin Design Paper, https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf?la=en&hash=EF5857437C4857373A9287CD86F56D0E7C46E7FF.

43 Auer et al., "CBDCs Beyond Borders," 10; and World Economic Forum, "The Role of the Public Sector and Public-Private Cooperation in the Era of Digital Currency Growth," White Paper 1/8, Digital Currency Governance Consortium White Paper Series, November 2021, https://www3.weforum.org/docs/WEF_Role_of_Public_Sector_and_Public_Private_Cooperation_2021.pdf.

44 Dirk A. Zetzsche et al., "DLT-Based Enhancement of Cross-Border Payment Efficiency – a Legal and Regulatory Perspective," BIS Working Papers No. 1015, May 20, 2022, https://www.bis.org/publ/work1015.htm.

45 BIS Innovation Hub, *Project Dunbar;* Tsang and Chen "Policy Responses," 237–238; and Adina Popescu, "Cross-Border Central Bank Digital Currencies, Bank Runs and Capital Flows Volatility," IMF Working Papers, International Monetary Fund, May 6, 2022, 3, https://www.imf.org/en/Publications/WP/Issues/2022/05/06/Cross-Border-Central-Bank-Digital-Currencies-Bank-Runs-and-Capital-Flows-Volatility-517625.

46 BIS Innovation Hub, *Project Dunbar*; and Zetzsche et al., "DLT-Based Enhancement." It would help to combine GDPR data minimization with risk-based AML (see Laurinaitis, Štitilis, and Verenius, "Implementation of the Personal Data," 670).

47 He, Milne, and Zachariadis, "Central Bank," 3, 19; Tsang and Chen "Policy Responses," 32; and Nadia Pocher and Andreas Veneris, "Central Bank Digital Currencies," in *Handbook on Blockchain*, eds. Duc A. Tran, My T. Thai, and Bhaskar Krishnamachari (Springer International Publishing, 2022).

48 Tsang and Chen "Policy Responses," 32.

49 Auer, Haene, and Holden, "Multi-CBDC Arrangements"; and Pocher and Veneris. "Central Bank."

50 *MI Forum Magazine*, "The Harmonised Approach to ISO 20022 Adoption," SWIFT, June 2017, https://www.swift.com/swift-resource/116946/download?language=en; SWIFT, "ISO 20022 Harmonization Best Practices," Info Paper, 2016, https://www.swift.com/resource/iso-20022-harmonisation-best-practice-information-paper; He, Milne, and Zachariadis, "Central Bank," 41; and Financial Stability Board, *Enhancing Cross-Border Payments*: Stage 3.

51 Financial Stability Board, *Enhancing Cross-Border Payments*: Stage 3, 10 and 12.

52 KYC, identity information sharing, and consistent AML rules are listed in Financial Stability Board, *Enhancing Cross-Border Payments*: Stage 3.

53 Zetzsche et al., "DLT-Based Enhancement."

54 Pauline Affeldft and Ulrich Krüger, "You Are What You Pay – Personal Profiling with Alternative Payment Data and the Data Protection Law," *Vierteljahrshefte zur Wirtschaftsforschung* 89 (4) (October 2020): 73–78, 74, DOI:10.3790/vjh.89.4.73.

55 Previous research assessed different CBDCs accordingly. See, Nadia Pocher and Andreas Veneris, "Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme," *IEEE Transactions on Network and Service Management* 19 (2) (June 2022), https://doi.org/10.1109/TNSM.2021.3136984. Auditability can be defined as "the understanding of transaction information by the authorized third parties, or the degree to which a given environment allows an authorized entity to audit confidential transaction information by viewing and interpreting the information." See European Central Bank and Bank of Japan, *Balancing Confidentiality and Auditability in a Distributed Ledger Environment*, STELLA Joint Research Project of the European Central Bank and the Bank of Japan, February 2020, 1, https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical200212.en.pdf.

56 This resembles cash usage limitations in some jurisdictions. See Pocher and Veneris, "Privacy and Transparency."

57 https://home.treasury.gov/news/press-releases/jy0882 Accessed 6 September 2022

ANNEX

Glossary

AML	Anti-Money Laundering
CBDC	Central Bank Digital Currency
CFT	Combating the Financing of Terrorism
CPF	Counter Proliferation Financing
DLT	Distributed Ledger Technology
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
GDPR	General Data Protection Regulation
KYC	Know Your Customer
LEA	Law Enforcement Agency
MiCA	Markets in Crypto Assets
SAR	Suspicious Activity Report
STR	Suspicious Transaction Report
UTXO	Unspent Transaction Output
ZKP	Zero Knowledge Proof

Giulia Fanti is an Assistant Professor of Electrical and Computer Engineering at Carnegie Mellon University. Her research interests span the security, privacy, and efficiency of distributed systems. She is a two-time fellow of the World Economic Forum's Global Future Council on Cybersecurity and a member of NIST's Information Security and Privacy Advisory Board. Her work has been recognized with best paper awards, a Sloan Research Fellowship, an Intel Rising Star Faculty Research Award, a U.S. Air Force Research Laboratory Young Investigator Grant, and faculty research awards from Google and JP Morgan Chase. She obtained her Ph.D. in Electrical Engineering and Computer Science from U.C. Berkeley and her B.S. in Electrical and Computer Engineering from Olin College of Engineering.

Nadia Pocher received the five-year master's degree in European and transnational law from the University of Trento, Italy, in 2016, where her dissertation on how to enhance cross-border opportunities for SMEs in the framework of EU company law was completed in collaboration with Utrecht University, The Netherlands. She is a Doctoral Researcher with the Law, Science and Technology Joint Doctorate—Rights of Internet of Everything, funded by the European Union under the Marie Skłodowska-Curie Actions. Her Ph.D. research on DLTs, cryptocurrencies, Central Bank Digital Currencies, anonymity and AML/CFT/CPF regulation takes place with the Autonomous University of Barcelona, Spain, in collaboration with the University of Bologna, Italy, and KU Leuven—CiTiP, Belgium.

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Please direct inquiries to: Atlantic Council
1030 15th Street, NW, 12th Floor Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org