Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme

Nadia Pocher*, Andreas Veneris†
*Faculty of Law - Universitat Autònoma de Barcelona • K.U. Leuven • Università di Bologna
†Department of Electrical and Computer Engineering and Department of Computer Science, University of Toronto

***Abstract*—Central banks and governments all over the world are increasingly exploring digital versions of fiat money, known as retail Central Bank Digital Currencies (CBDCs). Most initiatives rely on Distributed Ledger Technologies and are presented as alternatives to physical cash. Consequently, anonymity-related regulatory questions arise in terms of Anti-Money Laundering and Counter-Terrorist Financing compliance. Against this backdrop, this paper provides a techno-legal taxonomy of approaches to balance privacy and transparency in CBDCs without thwarting accountability, but it also underlines cross-sectoral impacts. The contribution heeds regulation-by-design as its core methodological foundation, with Privacy-Enhancing Technologies as the relevant use case. Thus, it highlights that not only technology aids legal purposes, but also that some regulatory requirements ought to be designed into technology for one to reach agreed-upon results and/or standards.**

***Index Terms*—central bank digital currency, cryptocurrency, regulation, policy, anonymity, criminal activities, risk management, law and technology, anti-money laundering, compliance**

I. Introduction

Leveraging distributed ledger technologies (DLTs) into decentralized, tamper-resistant and trustless alternatives to traditional financial instruments has fascinated private and public sectors alike since the advent of Bitcoin in 2008 [1]. Over the last decade, the cryptocurrency-driven blockchain "hype" has sponsored collective participation of citizens and businesses in a new digital global economy as embodied by the concepts of "Internet of Money" (IoM) [2] and "Internet of Value(s)" (IoVs) [3]. Today, novel trends erupt in global cross-border "stablecoin" projects in the wake of Facebook's Libra/Diem initiative [4]. These efforts were preceded by exploratory trends of government-backed e-fiat currencies or *Central Bank Digital Currencies (CBDCs)*. This paper addresses CBDCs as institutional frameworks of programmable money investigated by many central banks [5], [6], [7], [8], [9], [10], [11], [12].

Evidently, this tech-steered socio-economic transformation has generated significant new legal and regulatory concerns. Notably, the perceived level of anonymity, ubiquity and smart contracts-driven opportunities presented by DLT-based ecosystems have fuelled fears of exploitation for borderless illicit transactions. This extends into the anti-money laundering and combating the financing of terrorism (AML/CFT) domain which is internationally overseen by the Financial Action Task Force (FATF).[1] AML-wise, CBDC issues differ from those in IoM/IoV, as they have different stakeholders. Nonetheless, with CBDCs usually advertised as "physical cash" substitutes, any desire for a certain share of anonymity needs to be balanced against the integrity of the underlying financial system.

[1]For brevity, in the remaining paper AML refers to both AML/CFT.

978-0-7381-1420-0/21/$31.00 ©2021 IEEE

This paper attempts an introductory taxonomy of approaches in balancing privacy and transparency for CBDCs. It does this by underlining cross-sectoral impacts. Its contributions explore techo-legal questions of CBDC designs for AML compliance. *Regulation-by-design* is its core concept – once trade-offs are identified, they ought to be engineered into actual design plans. Although findings are set within the context of CBDCs, discoveries made here also offer insights to private "alt-coin" ecosystems. Additionally, this work heeds:

- The inherent cross-border dimension of CBDCs: interoperability between sovereign frameworks should be ensured, as well as transnational regulatory validity [13],
- A context-neutral approach immune to a jurisdiction: arguments are placed at a principle-level, and
- A flexible methodology: we focus on general frameworks, to be subsequently tailored to specific requirements.

The remainder of this paper goes as follows. Section II offers background information on the underpinning concepts and problem assumptions. Section III outlines the evolution of CBDCs. Section IV dives into AML and anonymity with Section V tackling trade-offs. Section VI examines regulation-by-design from a Privacy-Enhancing Technology (PET) standpoint. Section VII presents use-cases. Section VIII concludes the paper and pencils directions for future work.

II. Background

A. Problem Definitions

This subsection offers definitions and terminology [4], [5], [14], [15]. From a monetary viewpoint, let the following mean:

- *Central Bank Money (CeBM)*: this can be physical money or cash (*i.e.*, banknotes/coins, general purpose money). It can also be reserves/settlement accounts (*i.e.*, e-CeBM's) to authorized institutions such as commercial banks and Payment Service Providers (PSPs).
- *Commercial Bank Money*: these are liabilities to the general public; that is, a claim against a commercial bank to pay CeBMs and thus an extension of the former.

Past literature classifies CBDCs as follows:

- *Wholesale*: a settlement mechanism between financial institutions for inter bank security transfers between participants by Real-Time Gross Settlement Systems (RTGSs) beyond the tier of physical-cash.
- *Retail*: offered to the public at large. This is also the most transformative subset of CBDCs construed as an evolution towards a more "democratic" public transmission channel to central bank monetary holdings/policies.

Architecturally, a CBDC scheme can be either a *one-layered* system where the central bank directly manages all axles of its lifecycle (distribution, KYC, settlement, etc.), or a *two-layered* one where non-governmental financial institutions (commercial banks, PSPs, NGOs, etc.) act as intermediaries for market placement, compliance, distribution or settlement. Accordingly, CBDC architectures have been labelled as *direct*, *hybrid*, *intermediated* or *indirect/synthetic* [16], and they may involve varied public and private stakeholders [9], [17].

Further, a CBDC can be *account-based* where users open a current account, or "e-wallet", at a central bank or at a PSP. It can also be *token-based* where the CBDC is a digital unit, such as a token stored in a physical device. This type of CBDC is a bearer instrument transferred with secure hardware/software units. Notably, one should be able to transfer CBDCs online but also offline. Just like cash, offline usage has the potential to serve minorities, international travellers and the unbanked [18].

In the context of financial transactions, our contributions address the compound notions of anonymity, pseudonymity, privacy, and transparency. With no formal attempt to offer a comprehensive cross-sector techno-legal definition, and for the sake of conciseness, we set out the below [19]:

- *anonymity*: a subject is anonymous when it is not identifiable (*i.e.*, not distinguishable) within a set of subjects (its "anonymity set");
- *pseudonymity*: the use of pseudonyms as identifiers, where pseudonyms are identifiers other than real names;
- *privacy*: broadly intended as protection from unintended disclosure. Although the concept is manifold, more detail will follow wrt DLT-based monetary instruments; and,
- *transparency*: without necessarily implying publicity in terms of "public availability" of some information, transparency enables (selected) third parties to have access to it. Thus, it relates to openness and accountability. In a DLT context, it refers to the possibility to access data stored on the ledger; from an AML standpoint it relates to its availability and retrievability when legally required.

By means of convenience, Table I lists all the acronyms used in this contribution.

B. Underlying Assumptions

The paper herein makes the following assumptions:

1) CBDCs are *programmable*, which means smart contracts are leveraged to embed them with specific features and capabilities. Although this work chiefly addresses how this state of affairs generates new regulatory opportunities, it is worth bearing in mind that novel sophisticated criminal pathways are opened up as well [20].
2) We focus on *retail-CBDCs*. In contrast, their wholesale counterparts are exclusively in the hands of financial institutions. They may spur reflections on cross-border interoperability, but generate less AML regulatory hurdles. Henceforth, in the remaining paper the term "CBDC" means strictly "retail CBDC".
3) The principle of "tech-neutrality" is at the heart of regulation of new technologies. Moreover, retail CBDCs do not necessarily deploy DLTs. Nonetheless, as most initiatives are built on DLTs, this also pivots our work.
4) CBDCs pose a significant number of multi-faceted legal challenges. Here, we limit analysis to the AML sphere.
5) This work does not address cross-border CBDC interoperability questions.

AML	Anti-Money Laundering
BIS	Bank for International Settlements
BoC	Bank of Canada
BoL	Bank of Lithuania
CBDC	Central Bank Digital Currency
CeBM	Central Bank Money
CDD	Customer Due Diligence
CFT	Counter-Terrorist Financing
DCEP	Digital Currency Electronic Payment
DLT	Distributed Ledger Technology
ECB	European Central Bank
FATF	Financial Action Task Force
IoM	Internet of Money
IoV	Internet of Value
KYC	Know-Your-Customer
MAS	Monetary Authority of Singapore
NGO	Non-Governmental Organization
P2P	Peer-to-Peer
PBoC	People's Bank of China
PET	Privacy Enhancing Technology
PoC	Proof-of-Concept
PSP	Payment Service Provider
RTGS	Real-Time Gross Settlement System
STR	Suspicious Transaction Reporting

Table I: List of Acronyms

III. History and Current Efforts in CBDCs

The growing interest of central banks in programmable M0 money has had many drivers, and opinions on their origin vary [4], [7], [8]. In summary, two primary factors seem to have sparked this interest. Firstly, the use of traditional cash by the general public has been decreasing, in favor of digital claim-based alternatives such as card transactions, wire transfers and other means of electronic payment. As such, in some jurisdictions (like Sweden or Canada) the use of cash as a means of exchange has starkly declined in the past decade. At the same time, private altcoins and other tokenization initiatives are thriving. Today there are more than 5,000 cryptocurrencies in circulation. Further, attempts to limit their price volatility led to global stablecoins and, more recently, "mega-stablecoins" such as Facebook's Libra/Diem [21].

Against the backdrop of this FinTech-driven digitization and associated challenges to the traditional bank-based payment and monetary policy transmission mechanisms [15], central banks started heeding the idea of protecting their raison d'être and financial stability by tokenizing fiat currencies.

A. CBDC essence and goals

The author in [22] provides a tech-oriented definition of retail CBDCs as: *"A credit-based currency in terms of value, a crypto-currency from a technical perspective, an algorithm-based currency in terms of implementation, and a smart currency in application scenarios"*. More broadly, [23] highlights that *"CBDC is not a well-defined term. It is used to refer to a number of concepts. However, it is envisioned by most to be a new form of central bank money. That is, a central bank liability, denominated in an existing unit of account, which serves both as a medium of exchange and a store of value"*. Hence, *"A CBDC is a digital form of central bank money that*

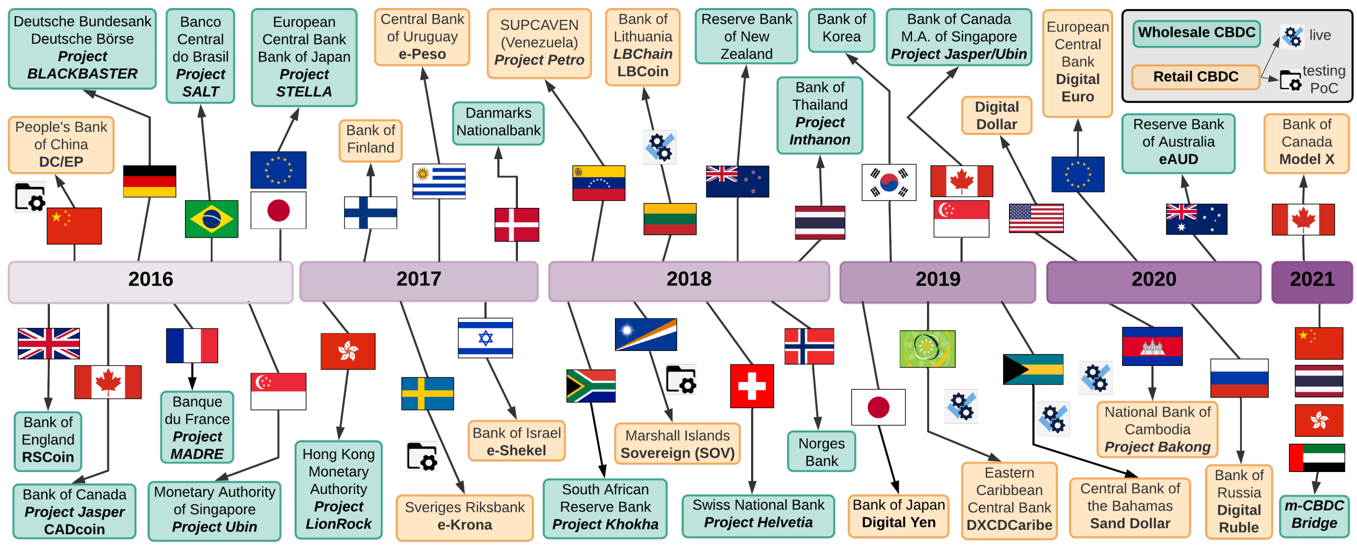

Figure 1: Global roadmap on major *wholesale* and *retail* CBDC projects

is different from balances in traditional reserve or settlement accounts" [6]. Notably, the composite nature of CBDCs set in the previous Section emerges in these definitions as well.

Empirically, CBDC plans offer a diverse set of designs. Most literature agrees that a CBDC is a digital representation of a fiat currency, hence a digital liability of the central bank. Frequently, CBDCs are devised as an "enhanced" version of cash in terms of universal accessibility and transaction capabilities, thus placed in between physical cash (CeBM) and commercial bank money. Pursued goals vary according to the specific needs of the jurisdiction, generally advanced economies rank their goals differently to those by emerging ones. Overall, the underlying idea behind all initiatives is to mimic M0 cash while overcoming its existing inherent need for physical handling and portability limits. In parallel, CBDC plans also envision their potential to foster payment efficiency (including new monetary policy transmission channels), financial inclusion, safety, privacy and compliance [5], [15], [24].

B. Overview of Proof-of-Concepts

CBDC Proof-of-Concepts (PoC) have gained prominence over the last years and extensive commentaries were published by diverse stakeholders [6], [7], [8], [9], [10], [11], [12], [25]. The work of [24] classified central bank projects as early adopters, followers and new entrants. In this subsection we give a historical summary, as also illustrated in Figure 1.

In **2015-16**, research pioneers started exploring CBDCs, albeit by addressing wholesale interbanking use-cases. Notable references are led by the Bank of England (*RSCoin*) and the People's Bank of China (PBoC), the latter coined as *Digital Yuan* or *Digital Currency Electronic Payment (DCEP)*. Around the same time, the Bank of Canada (BoC) piloted the four-phased *Project Jasper*, one of the most comprehensive efforts up to date. In Europe, the Deutsche Bundesbank and the Banque de France put forward projects *BLOCKBASTER* and *MADRE*, respectively. After the Banco Central do Brasil set up *Project SALT* and the U.S. Federal Reserve started scouting the CBDC realm, two initiatives climaxed the first wholesale CBDC era in late 2016: the Monetary Authority of Singapore (MAS) launched *Project UBIN* and *Project Stella* was piloted by the European Central Bank (ECB) and the Bank of Japan.

Between **2017** and **2018** retail CBDC projects started to evolve. While *Project LionRock* of the Monetary Authority of Hong Kong still addressed interbank settlements, other central banks started to explore general purpose CBDCs and their relation to cash, most notably the *e-Krona Project* by the Sveriges Riksbank in Sweden. Other research/pilot initiatives also followed in this period, shown in Figure 1, around diverse –sometimes– CBDC concepts [9].

In early **2019**, around 70% of central banks responding to a survey of the Bank for International Settlements (BIS) declared to be engaging in some PoC CBDC-related activity [15]. Although only 30% voiced an intention to issue such instruments within the medium term, that year was arguably a breakthrough one in which research in CBDCs reached a new level of maturity, but also this of news headlines, in part due to the spark by Facebook's announcement of the Libra coin in late June 2019. Following the reports of the Bank of Korea and the Bank of Japan, the first cross-border interbank settlement mechanism between two different DLT-based currency platforms was concluded by the BoC and the MAS in the fourth joint phase of project *Jasper/Ubin*.

In 2019, the ECB started to analyze the implications of cryptoassets on monetary policy [26] and in October **2020** a report [27] was issued on principles and configurations for a candidate retail *Digital Euro*. At the beginning of 2020, central banks working on CBDCs had risen to 80% with nearly half of them at the PoC phase, and a lower number of pilot projects [28]. In May the *Digital Dollar Project* released a whitepaper and in June congressional hearings took place in the U.S. with regard to CBDCs. In July the Bank of Lithuania (BoL) issued the first state-backed digital collector coin, LBCOIN, which can be transferred Peer-to-Peer (P2P). LBCOIN is no legal tender (BoL belongs to the Eurosystem) and can only be exchanged into a physical collector coin.

Later, October 2020 saw the launch of the first CBDC by the Central Bank of the Bahamas through the *Sand Dollar* platform. The *Sand Dollar* is pegged to the Bahamian dollar, which in turn is pegged to the U.S. dollar on a 1:1 basis under currency board-like rules. This move also validates claims that smaller countries may want expedite implementation of their respective CBDCs due to risk of competition by CBDCs from larger foreign economies. That is, if foreign CBDCs are easier (or more "stable") to use, they may intermediate or present a risk of displacement to "local money" with whatever dramatic impact this may have on said domestic monetary/fiscal policies for those smaller economies. Meanwhile, Brazil's central bank launched the Pix instant-payment platform, and the Bank of Russia unveiled interest in a *Digital Ruble*.

Finally, the early months of **2021** testify not only to the wide interest in CBDCs, but also to their growing maturity. Notably, 86% of central banks surveyed by BIS are exploring CBDCs, where 60% of them at an advanced experimental or PoC stage and 14% at a pilot phase [29]. In January the European Commission and the ECB announced a cooperation on a possible *Digital Euro* upon the conclusion of the relevant public consultation. A decision whether to launch a project is expected by April. In February, the *Digital Dollar* debate rekindled significantly in the U.S. and the Swedish *e-Krona Pilot Project* was granted a one-year extension. In China, the testing scope of the *Digital Yuan* was widened. A beta version is expected to launch in the second half of 2021. Meanwhile, the PBoC joined a cross-border payment project with the central banks of Thailand, United Arab Emirates and Hong Kong to develop a Multiple CBDC Bridge (*m-CBDC Bridge*). Concurrently, in February the BoC unveiled three design proposals under their Model X challenge for a CBDC denominated in Canadian dollars (or, a *Digital Loonie*) by three universities [30].

IV. The Quest for AML/CFT Compliance

The term "AML/CFT" describes a set of laws, regulations and procedures aiming to protect the integrity of the financial system by preventing criminals from enjoying illicit profits. The goal is hindering concealment of the origin of ill-gotten proceeds through preventive measures and sanctions. From 1989 onward, international efforts have been coordinated by the Financial Action Task Force (FATF). The FATF is an intergovernmental, policy making, monitoring and enforcement organization that sets standards and provides comprehensive guidance, *e.g.*, through its Recommendations. In 2001 CFT was further added to FATF's mission.

Although most countries and supranational organizations provide their specific frameworks, the general structure of AML measures is fairly harmonized. In most cases, a set of regulated entities is required to give "active cooperation" to the authorities in light of their perceived oversight capacity. These obliged/reporting entities range from commercial banks and financial institutions, to professionals (such as lawyers and notaries), to casinos and art galleries. Virtual Asset Service Providers, such as a subset of providers of exchange and wallet services, were later added to the list. Illustratively, cryptocurrencies are at the core of the EU 5$^{\text{th}}$ AML Directive [31].

Key AML duties are outlined in Figure 2. They encompass licensing regimes, Customer-Due-Diligence (CDD) obligations such as Know-Your-Customer (KYC) and ongoing monitoring (*e.g.*, transaction scrutiny), as well as record retention and Suspicious Transaction Reporting (STR). Most of these obligations are informed by the Risk-Based Approach, *i.e.*, preliminary risk assessments tune consistent controls. As enshrined by Article 33 of the EU AML Directive, the ultimate goal is for authorities to be informed when a regulated entity

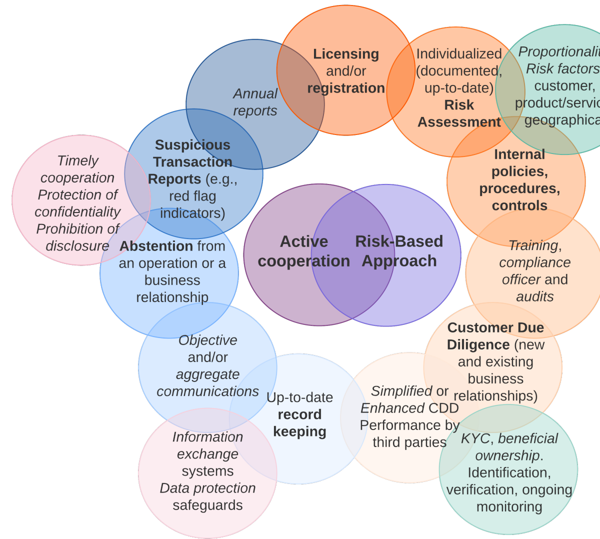

Figure 2: Overview of the major AML/CFT duties imposed on regulated entities

"... knows, suspects or has reasonable grounds to suspect that funds, regardless of the amount involved, are the proceeds of criminal activity or are related to terrorist financing" [31].

A. Illicit Transactions in the IoM

Since birth, the risk of cryptocurrencies being misused for illicit purposes emerged as a common thread [32]. Due to their purported anonymity/untraceability, they have been linked to transactions on the dark web, online gambling, money laundering, and to the financing of criminal activities and terrorism. Popular controversies concerning the Silk Road case, followed by the shutdown of Darknet markets (*e.g.*, Alphabay, Valhalla, Wall Street Market), added to this skepticism and fear.

Even if the technology underpinning Bitcoin was acknowledged to shape a pseudonymous means of payment, a significant set of altcoins have evolved toward higher levels of anonymity and cryptographic complexities. Accordingly, the FATF acknowledged the growing money laundering concerns in terms of virtual-to-virtual "layering" mechanisms [33]. Later, "privacy coins" (such as Monero and ZCash) and transaction obfuscation mechanisms (such as mixers/tumblers) were complemented by P2P decentralized exchanges, unhosted wallets and cross-chain atomic swaps. In this context, the FATF identified anonymity as a "red flag indicator" of IoM-related suspicious activities [34].

Although the anonymity level is not sufficient to suggest a transaction is illicit, the FATF urged to be careful with some vulnerabilities inherent to specific Privacy-Enhancing Technologies (PETs) and/or enhanced decentralization. Likewise, Europol highlighted how privacy-enhanced wallets are currently among such top threats [35], while experts underlined the extent to which opportunities steered by CBDC-related programmability may be seized by criminals in innovative ways, *e.g.* through intricate money laundering strategies to evade AML checks [20]. In summary, regulators face major challenges and ubiquitous global-stablecoins worsen this fear.

B. CBDCs, Cash and Anonymity

Anonymity is inherent to the nature of physical cash: the level of privacy cash can reach is unparallelled and it is perhaps one of the purest examples of a fungible asset. Thus, the fight against financial crime has long faced the "anonymity problem", against which identification and traceability have been heralded. If CBDCs are to replicate a similar situation, while at the same time overcoming material limitations, significant concerns may arise. Interestingly, however, cash being dangerous from an AML perspective is one of the reasons why e-money solutions, and the degree of control they can enable, were sponsored in the first place [5].

Nonetheless, one should not forget that anonymity is not a binary zero-sum property, but rather *ranges* within a spectrum. In [36] experts explored the difference between anonymous, identified and pseudonymous clients and also how this reflects on the underlying transactions with regard to AML rules. With the advent of "crypto" digital payments, we argue here that the intrinsic complexity of this characterization has increased.

The issue of online anonymity is one of socio-technical nature [37], [38]. On the technical side, and within a DLT context, it is influenced by the available privacy tools (*e.g.*, PETs), by governance (*e.g.*, centralized vs. decentralized systems), and by the broader system architecture (*e.g.*, relationship with other on/off-chain layers). On the social side, it refers to (1) the actual possibility for identification/traceability and forensic techniques to "follow the (crypto) money" vs. (2) the backdrop of the public's skills to prevent this and its right to do so.

As an example, pseudonymity implies to be neither anonymous nor identified. While the identity of pseudonymous users is unknown, that is, there are no direct identifiers, it may still be possible to link it when a warrant is issued with additional data to trigger identity associations. The same can be argued for records of transactions or the transactions themselves, as it is the case for commercial numbered bank accounts.

C. AML/CFT in CBDCs

In light of the foregoing, two remarks are necessary. If CBDCs are intended to mirror cash flexibility/usability, it might make little sense for procedures to resemble those of traditional bank accounts. Hence, it is not a surprise that token-based CBDCs could be argued as more conducive to financial inclusion than account-based ones. At the same time, if a CBDC design underestimates AML compliance, this does not also imply that users can operate beyond such principles. Instead, one would expect that compliance burdens would be shifted to the private entities offering CBDC product/services to the end-users — no different to what happens today with the "active cooperation" by commercial banks, etc. These observations lead to either a two-layered CBDC structure or one where the CBDC itself offers strong anonymity (thus making KYC impossible at this layer) but regulators require private service-providers converting CBDCs to other currencies to implement KYC on their customers. Of course, a central bank may also undertake the costly compliance effort herself and keep records anonymous if she is the sole processor of CBDCs' settlement.

It is important to note that although AML aspects of CBDCs have been extensively discussed, these instruments have so far not been treated as cryptocurrencies, which means AML for CBDCs is disjoint to that for cryptocurrencies. On the contrary, CBDCs are viewed as a form of fiat currency [8]. Rightfully though, several studies outlined how different CBDC architectures may lead to various AML repercussions.

A key question relates to the responsibility for compliance duties, account management, and identity/transaction checks. To this end, two-tier structures may be favored by central banks, as they do not traditionally interact with public end-users other than a handful of financial institutions. Hence, two-layer models allow to outsource compliance aspects to PSPs and commercial banks to be managed either directly or delegated. This intermediated access model is favored to leverage existing customer-facing services and avoid unnecessary duplication of KYC resources.

V. The Privacy vs. Transparency Trade-off

Monitoring and/or limiting the use of cash is widespread across the globe as a way to combat money laundering, terrorist financing and tax evasion; thresholds for customs declarations are provided and cash transactions above a certain volume trigger compliance duties, among other measures. Pursuant to Article 11 of EU's 5$^{\text{th}}$ AML Directive, for instance, Customer-Due-Diligence (CDD) obligations are triggered for financial institutions either upon the establishment of a business relationship or when the customer carries out transactions that amount to EUR 15,000 or more (in a single operation or many seemingly interlinked). As another example, in Canada and in the US obliged entities must report transactions of CAD/USD 10,000 or more within 24-hours [39], [40].

Further, the EU has considered to introduce restrictions to payments in cash [41], and some countries already limit its use between private individuals if no regulated intermediary is involved in the said transaction [42]. Illustratively, this happens in Italy, where cash transactions between people that exceed EUR 2,000 are prohibited (this limit will decrease to EUR 1,000 in 2022), but also in France (EUR 1,000), Portugal (EUR 1,000), Belgium (EUR 3,000), Slovakia (EUR 15,000), Spain (EUR 2,500), Bulgaria (EUR 5,000), and Greece (EUR 500). In those jurisdictions, transfers of higher values must be made through regulated intermediaries. Outside Europe, a similar tactic applies to some types of transactions in Jamaica, Mexico, Uruguay and India.

A. A balance in the making

In light of the foregoing, there is a clear inherent tension in CBDCs between privacy and transparency. This *trade-off* however, is not a zero-sum game [37]. All means of payment provide varying degrees of privacy/anonymity, ranging from methods requiring the bank to monitor transaction and identity data (*e.g.*, wire transfers), to anonymous transactions in cash. In turn, digital cash allows to exert control, but it may also possibly expose other sensitive information [5].

Against this backdrop, CBDCs can be designed to embed various privacy trade-offs. Further, DLT is inherently conducive to balancing the individual right to privacy vs. traditional public interests in AML compliance. The extent to which users' privacy is safeguarded, in fact, depends on the preferred balance between individual rights and public interests. Starting from extreme examples, if we imagine a fully-transparent CBDC with real-world identity transactions fully visible to law enforcement, the applicable solution(s) may violate human rights law on privacy and data protection. If privacy is provided without any limitation, so that no information can be revealed about transactions, this may invite misuse for illicit purposes that cannot be averted. This option is not viable to CBDC-regulated stakeholders, as it may generate dangerous societal impacts. History also shows how a regulated access of financial authorities to information on monetary/data flows resonates positively with citizens and businesses.

Luckily, nuanced solutions are available, and most CBDCs position themselves in the *middle*, offering some privacy to consumers and some visibility to authorities.

B. Privacy in Digital Currencies

Since many CBDC PoCs are built on DLTs to leverage their programmability, novel privacy-level questions emerge [43]. For blockchain-based cryptocurrencies this issue was tackled by breaking it down to pieces of information embedded in the blockchain to assess whether they are private or public. This particular problem appears to be threefold. On the one hand, there is:

- *user-identity privacy* or *identity privacy*: it relates to transaction participants and concerns the ability (or lack thereof) to link an activity to the relevant senders or recipients; this is the area where *privacy* relates to *anonymity*. Arguably, the difficulty (or dilemma) to equip CBDCs with cash-like anonymity is mostly at this level, as pseudonymity proves to be insufficient;

while, on the other hand, there are:

- *privacy of transaction data/information*: it concerns transaction details (*e.g.*, amount) and the ability (or lack thereof) to learn its nature. This concept is malleable and handled through cryptographic principles [37]; and,
- *privacy of the global ledger state*: different attributes can be private at various degrees to the DLT parties involved (*e.g.*, PSPs, NGOs, end-users, etc.).

Furthermore, identity and transaction privacy levels within DLT-based ecosystems are influenced by multilayered solutions and by also storing different data on-chain or off-chain.

VI. A Regulation-by-Design Approach

As mentioned earlier, CBDC designs entail different trade-offs. Likewise, there is a correlation between those trade-offs and AML provisions when it comes to anonymity. The interlink between technical and regulatory compliance builds on the assumption that the latter can be embedded into technology itself. This concept is at the root of *design-based* regulatory techniques as a means to foster socially and legally desirable outcomes. This is in contrast to traditional "command and control" approaches such as prohibitions and sanctions [44].

Illustratively, if the latter refers to setting crypto-related AML duties and penalties for violations, *regulation-by-design* strives to devise inherently compliant instruments. The notion that compliance aspects not only can, but they *ought to* be taken into account from the early stages of the system design or process is gaining momentum among law and technology experts today. Embedding legal principles and values into technology lies at the core of privacy-by-design spilling into *compliance by* or *through design* [19], [45], [46].

Notably, design-based regulation has evolved from Lessig's "code is law" [47], claiming cyberspace behavior is controlled by software code. Although caution is recommended from a legal standpoint, this notion prompted the new understanding of *embedded regulation* [48]. Namely, regulation can be approached proactively (rather than reactively) by addressing the code itself [49]. Meanwhile, a branch of legal informatics known as *computational law* focuses on bridging the gap between legal knowledge/reasoning, natural language

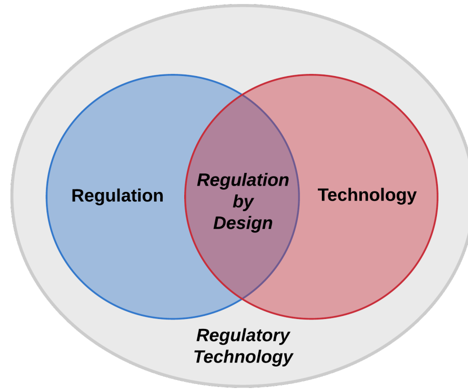

Figure 3: The interplay between regulation and technology in *RegTech* and *Regulation by Design / Embedded Regulation*

and machine-readable formats (*e.g.*, through formal semantic representation) [50], [51], [52].

Outlined in Figure 3, as "design" and "code" are becoming regulatory instruments, this takes RegTech (*i.e.*, regulatory technology, generally leveraging new technologies to aid legal purposes) to the next level. This *forward-looking* approach requires preliminary engineering and standard setting as to said regulatory goals and available tools. Choices are seldom binary and need to be made early in the design cycle with interdisciplinary teams cooperating from the beginning.

A. Towards Accountability in Privacy Enhancing Technologies

Privacy-by-design was first formalized with regard to PETs [46], [53], so to exemplify how technology can be tailored to regulatory goals. This section outlines how privacy, just like anonymity, is twofold. On the one hand, PETs are implemented to safeguard individual privacy against intrusions. Likewise, it serves the purposes of data protection, where the application of the EU General Data Protection Regulation (GDPR) 2016/679 is now arguably ubiquitous. On the other hand, however, similar techniques have been exploited to pursue sheer anonymity in "privacy coins" such as Monero, ZCash, or Dash, whose degree of untraceability cripples the fight against illicit financial activities.

Data protection must be balanced with accountability and various PETs present different techno-legal compromises. Many of these tools can support privacy and transparency in manifold forms, but the balance is technically challenging. Further, trade-offs grow harsher when PETs are applied concurrently [11]. Consistently, experts have analyzed the ways privacy attitudes can be coded into blockchain systems [54] and the compatibility of diverse PETs with regulation. The goal is not only to enable proactive compliance, such as balance and payment limits, but also retroactive one (*e.g.*, data retention and mandated disclosure). Because not all PETs allow to retrieve information, some are ruled out.

More specifically, Phase 4 of *Project Stella* by the ECB and Bank of Japan [55] focused on the implementation of PETs to balance confidentiality and auditability of transaction information in payment and settlement DLT-based systems. They also offer the following contextualization and classification:

A) Segregating PETs. Information is shared on a "need to know" basis, such as in:

- *Corda*: transaction information is protected at the network communication level, where each communication can be partaken solely by authorized and identified participants; network services, *i.e.* (validating or non-validating) notaries, receive (all or part) of the information to avoid double-spending;
- *Hyperledger Fabric*: transaction information is safeguarded by dividing the network into subnetworks and respective ledger subsets, with each channel requiring authentication and authorization; a network service, *i.e.* an ordering service, orders transactions;
- *Off-ledger payment channels*: confidentiality is fostered by allowing a specific network to transact off-ledger, with relevant funds being temporarily in escrow on the ledger for security; this may become a payment channel hub when an intermediary is involved. Similar setups are offered by Bitcoin (Lightning) and Ethereum (Raiden).

B) Hiding PETs. Confidentiality is fostered at transaction level by implementing cryptographic techniques against unauthorised interpretation. This is the case of:

- *Quorum*. Besides public transactions, participants can opt for transacting privately; in the latter case, information is stored in private ledgers with only the relevant one-way hash value being stored publicly;
- *Pedersen commitment*. Participants share, instead of transaction amounts, only relevant commitments. The latter are uninterpretable to third parties, while it is possible to verify equivalence between inputs and outputs;
- *Zero-knowledge proofs*. They enable third parties to verify information without participants revealing or disclosing the content. In particular, the zk-SNARK subset (implemented in Ethereum and Quorum, for instance) sees a trusted party setting up a secret parameter that generates two public parameters, *proving and verification keys*, where the first is used by senders and the latter enables validation. Improvements are constantly put forward.

C) Unlinking PETs. They allow concealment of either the *(i)* identity of transacting parties from pseudonyms stored on the ledger, or *(ii)* any transacting relationship. Notably:

- *One-time address*: different pseudonyms or addresses may be used for different transactions. Its implementation is common, with deterministic wallets mitigating address management drawbacks;
- *Mixing* and *Tumbling*: multiple transactions are shuffled for relationships to be unlinkable, with confidentiality degrees resting on the amount of mixed data. If *centralized*, service providers are entrusted with original information. This can be averted in *P2P* schemes, although they require to timely find parties willing to mix data. As transaction amount is still stored in the clear, this method is often combined with *hiding techniques*;
- *Ring- and multi-signatures*. They allow to prove a signer is part of a group of signers without disclosing its identity. To this end, transactions are signed with both private key and public keys of the group members. Again, transaction amount is still visible and other methods may be added.

As outlined in Figure 4, the study in [55] shows how, on the one hand, effective auditability may be allowed by segregating PETs, Quorum's private transaction, Perdesen commitment and centralized mixing. Hence, their implementation may enable balancing anonymity and transparency in a CBDC-wise desirable way. By contrast, on the other hand, Zero-knowledge proofs, one-time address and multi/ring-signatures prohibit accessibility of transaction information to auditors. Nonetheless, multiple PETs may be combined to deliver the desired balance(s).

	Segregating PETs	Hiding PETs	Unlinking PETs
Effective Auditability	Corda Hyperledger Fabric Off-ledger payment channel (with payment channel hub)	Quorum Pedersen Commitment (blinding factor and amount)	Centralised Mixing
		Pedersen Commitment (only blinding factor)	
	Off-ledger payment channel (no payment channel hub)		Peer-to-peer Mixing
Weak Auditability		Zero-Knowledge Proof	One-time address Ring signatures

Figure 4: Classification of types of PETs in terms of auditability as per findings in [55]

VII. A Case-Study Taxonomy of Selected CBDCs

In light of the above, the way regulatory requirements are embedded into CBDC designs reveals trade-offs between privacy and transparency. Different use-cases are emblematic of diverging choices of sovereign institutions in the context of their monetary policy. Due to space limitation, the goal of this section is not to provide a taxonomy of how all CBDC projects have so far managed the balance at hand. Conversely, we highlight a few concrete examples of how technology is leveraged to reach various objectives. Projects are placed across a spectrum of conceivable privacy vs. transparency nuances, as outlined by Figure 5. In detail, we argue how full anonymity is difficult to achieve technologically and possibly inconsistent with established and essential legal principles. To reach full anonymity, users' identity should not to be verified upon access to a service, just like with cash — a practice not feasible in AML regulated jurisdictions.

A. From semi-anonymity

Research studies on identity privacy by the stakeholders has focused on pseudonyms and on the elimination of pseudonymous identifiers. Even in these cases, a solution has not yet been found to make it impossible to gather information about the identity of senders/recipients if the CBDC ledger is available publicly or selectively. Hence, it may not be feasible to achieve full cash-like anonymity [5].

If we focus on transaction privacy, validators must be able to verify that transaction amounts are consistent with account balances and compliant with predefined requirements. This is often pursued through computationally costly cryptographic techniques broadly labelled as Zero-knowledge proofs. Other solutions leverage secure multiparty computation, rotation of public keys and Trusted-Execution-Environment hardware-enclaved computing [5]. From a more practical CBDC perspective, a common way to offer anonymity while reaching a legally desirable level is to provide different solutions for different types of transactions. For instance, one may allow higher degrees of anonymity for transactions of low values. This CBDC model is usually token-based, being intrinsically more conducive to anonymity, as described earlier. Accordingly, [56] argues that token-based systems are the only avenue to reach a cash-like degree of transaction privacy.

Any trade-off will need to be identified at the beginning of the CBDC design cycle. In 2019, the ECB explored anonymity in CBDCs [57], leading to a DLT-based simplified PoC where a degree of privacy for low-value transactions is ensured (Figure 5) with no detriment to AML controls for higher values. Users are equipped with limited "anonymity vouchers" that allow the transfer of a specific amount within a given timeframe. These thresholds are automatically enforced, and an ad-hoc AML authority is in charge of the vouchers and the associated checks. Bearer-type token-based CBDCs may provide higher degrees of transaction anonymity, notably when payment devices are physical such as prepaid cards storing digital tokens whose transfers are P2P.

B. Through mixed solutions

In theory, privacy can be tackled selectively, meaning certain types of transactions could be undertaken without the acquisition of payer- and payee-related identity information. Nevertheless, for reasons mentioned above, registration and identity verification in terms of KYC are likely to take place when a user signs up. In the case of e-devices, identity checks can be also conducted through biometrics.

PBoC's *DCEP* seems to offer four levels of accounts based upon characteristics such as CBDC amounts, anticipated use, and other information provided during a wallet registration. Even if we consider the most anonymous scenario among the four account types (minimal functionalities and strict balance limits) some identifying information is given when the account is opened. In this manner one can achieve a limited degree of user-to-user anonymity which is both controllable and tiered. Within this framework, commercial banks hold identifying information and they can deanonymize suspicious transactions for AML. However, the rumored information available today indicates that the user's identity and transaction history are visible to the PBoC and most likely her intermediaries.

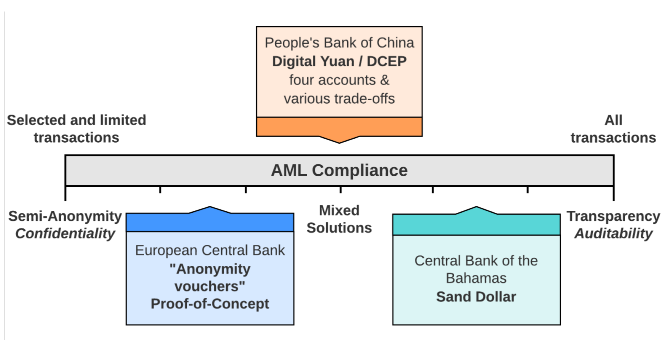

Figure 5: Selected CBDC projects from an AML compliance standpoint, from *accountable anonymity* to *transparency*

C. To transparency

We noticed how it is impossible to ignore trade-offs and fully comply with regulation even in the mentioned anonymity-oriented scenarios. An alternative option is that of accountable anonymity (Figure 5). In the solution put forward by the ECB [57], an AML authority is still involved and anonymity is limited to a restricted number of untransferable vouchers. At the same time, privacy is provided to the extent thresholds are enforced automatically, with no need to record the amount. Even when users are identified upon the first access, both the central bank and intermediaries can grant them different degrees of privacy subsequently.

If one proceeds along the "anonymity to transparency" spectrum, we find transparency-oriented solutions that closely resemble current regulatory frameworks for electronic payments. Obviously, data protection requirements still need to be met, but transactions could be fully transparent to the entity operating the underlying infrastructure. A high level of transparency is already offered by one of the very few known CBDC projects already operating, launched by the Central Bank of the Bahamas (Figure 5) in late 2020. Its CBDC tokens represent a claim on the central bank and they are digital cash. They are recorded and transferred on a private and permissioned DLT with all parties being identifiable [28].

VIII. Conclusion and Future Directions

This contribution proposes techno-legal methods to balance privacy and transparency in retail CBDCs for AML compliance within a *regulation-by-design* scheme, *i.e.,* regulatory trade-offs are embedded early into technology design plans. It further argues that by leveraging PETs one can provide a selected taxonomy of how CBDCs are placed within a range from accountable anonymity to transparency. All in all, CBDCs show some limitations when balancing this trade-off. Namely, issues arise when the envisaged solution cannot concurrently provide the desired levels of privacy and transparency. To address this, some existing CBDC projects split the problem into a compound design of two (or more) structures with different characteristics pursuant to a risk-based methodology. Notably, they select to implement anonymity-oriented token-based solutions for small transactions, and a privacy-preserving transparency-oriented account-based system for higher amounts. Thus, transaction and volume limits seem to be held as compliance benchmarks. Although focused on CBDCs, the findings here have a wider application across other blockchain assets (cryptocurrencies, stablecoins, etc.).

A potential avenue for future work ponders over multifold opportunities opened up by the *programmability* of CBDCs, chiefly in terms of smart contracts-driven evolution of AML enforcement, but also new criminal strategies. Consequently, it may tackle the issue of techno-regulatory interoperability in a cross-border CBDC world. Further, the arguments presented here could benefit from examining at length the technical role of PETs in CBDC compliance, and how they can be tailored to pursue different AML trade-off metrics. Finally, in a world where AI, machine learning and IoT technologies are increasingly linked to the financial and AML sphere, this paper remains agnostic to them. Similarly, to a certain extent this contribution implicitly assumes that those we define as "auditors" do not abuse their powers. Hence, possible extensions could dive deeper into how *regulation-by-design* may foster citizen protection against potential "abuse" of CBDCs and their accompanying data for various purposes.

IX. Acknowledgment

The contribution of Nadia Pocher received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie International Training Network European Joint Doctorate G. A. No 814177.

References

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *www.bitcoin.org*, 2008.

[2] A. M. Antonopoulos, *The Internet of Money - Volume Two*. Merkle Boom LLC, 2017.

[3] D. Tapscott and J. Euchner, “Blockchain and the Internet of Value: An Interview with Don Tapscott Don Tapscott talks with Jim Euchner about blockchain, the Internet of value, and the next Internet revolution.” *Research Technology Management*, vol. 62, no. 1, pp. 12–19, 2019. [Online]. Available: https://doi.org/10.1080/08956308.2019.1541711

[4] Group of 30, “Digital currencies and stablecoins: Risks, opportunities, and challenges ahead,” 2020. [Online]. Available: https://group30.org/

[5] S. Allen, S. Capkun, I. Eyal, G. Fanti, B. Ford, J. Grimmelmann, A. Juels, K. Kostiainen, S. Meiklejohn, A. Miller, E. Prasad, K. Wüst, and F. Zhang, “Design Choices for Central Bank Digital Currency: Policy and Technical Considerations,” Tech. Rep. 13535, jul 2020.

[6] Bank of International Settlements, “Central bank digital currencies : foundational principles and core features,” Tech. Rep. 1, 2020. [Online]. Available: www.bis.org

[7] T. Adrian and T. Mancini-Griffoli, “The Rise of Digital Money,” Tech. Rep., jul 2019. [Online]. Available: https://www.imf.org/

[8] J. G. Allen, M. Rauchs, A. Blandin, and K. Bear, “Legal and Regulatory Considerations for Digital Assets,” CCAF, Tech. Rep., oct 2020. [Online]. Available: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/legal-and-regulatory-considerations-for-digital-assets

[9] R. Auer, G. Cornelli, and J. Frost, “Rise of the central bank digital currencies: drivers, approaches and technologies,” Tech. Rep., aug 2020. [Online]. Available: www.bis.org

[10] Bank of Canada, “Contingency planning for a central bank digital currency,” Tech. Rep., 2020. [Online]. Available: https://www.bankofcanada.ca

[11] European Central Bank, “Tiered CBDC and the financial system,” no. 2351, p. 42, 2020. [Online]. Available: https://www.ecb.europa.eu/

[12] P. Sandner, J. Gross, L. Grale, and P. Schulden, “The Digital Programmable Euro , Libra and CBDC : Implications for European Banks,” no. July, 2020.

[13] D. Duffie, “Interoperable Payment Systems and the Role of Central Bank Digital Currencies,” *Finance and Insurance Reloaded, Institut Louis Bachelier Annual Report*, 2020.

[14] European Central Bank, “ECB Glossary.” [Online]. Available: https://www.ecb.europa.eu/home/glossary/html/glossa.en.html

[15] C. Barotini and H. Holden, “Proceeding with caution - a survey on central bank digital currency,” *Bank for International Settlements*, vol. 101, no. 1682-7651, pp. 1–15, 2019.

[16] R. Auer and R. Böhme, “The technology of retail central bank digital currency,” *BIS Quarterly Review*, no. March, pp. 85–100, 2020.

[17] C. Viñuela, J. Sapena, and G. Wandosell, “The future of money and the central bank digital currency dilemma,” *Sustainability (Switzerland)*, vol. 12, no. 22, pp. 1–21, 2020.

[18] J. Miedema, C. Minwalla, M. Warren, and D. Shah, “Designing a CBDC for Universal Access,” Bank of Canada, Tech. Rep., 2020.

[19] V. Torra, *Data Privacy: Foundations, New Developments and the Big Data Challenge, volume = 28, year = 2017*.

[20] Y. J. Fanusie, “Central Bank Digital Currencies: The Threat From Money Launderers and How to Stop Them,” *The Digital Social Contract: A Lawfare Paper Series*, no. November, pp. 1–23, 2020. [Online]. Available: https://www.lawfareblog.com/

[21] Z. Amsden, R. Arora, S. Bano, M. Baudet, S. Blackshear, A. Bothra, and G. Cabrera, “The Libra Blockchain - White Paper,” pp. 1–29, 2019.

[22] Q. Yao, “A systematic framework to understand central bank digital currency,” *Science China Information Sciences*, vol. 61, no. 3, 2018.

[23] CPMI-MC, “Central bank digital currencies,” Tech. Rep. March, 2018.

[24] E. A. Opare and K. Kim, “A Compendium of Practices for Central Bank Digital Currencies for Multinational Financial Infrastructures,” *IEEE Access*, vol. 8, pp. 110 810–110 847, 2020.

[25] T. Khiaonarong and D. Humphrey, “Cash Use Across Countries and the Demand for Central Bank Digital Currency,” Tech. Rep., mar 2019.

[26] ECB Crypto-Assets Task Force, “Crypto-Assets: Implications for financial stability, monetary policy, and payments and market infrastructures,” European Central Bank, Tech. Rep., may 2019.

[27] European Central Bank, “Report on a digital euro,” European Central Bank, Tech. Rep. October, 2020. [Online]. Available: https://www.ecb.europa.eu/

[28] C. Boar, H. Holden, and A. Wadsworth, “Impending arrival - a sequel to the survey on central bank digital currency,” Tech. Rep. 107, jan 2020.

[29] B. Codruta and A. Wehrli, “Ready, steady, go? – Results of the third BIS survey on central bank digital currency,” Tech. Rep. 114, jan 2021. [Online]. Available: https://www.bis.org/publ/bppdf/bispap114.pdf

[30] A. Veneris, A. Park, F. Long, and P. Puri, “Central Bank Digital Loonie: Canadian Cash for a New Global Economy,” 2021. [Online]. Available: https://ssrn.com/abstract=3770024

[31] Directive (EU) 2018/843, “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,” 2018.

[32] S. Foley, J. R. Karlsen, and T. J. Putnins, “Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?” *Review of Financial Studies*, vol. 32, no. 5, pp. 1798–1853, 2019.

[33] FATF, “Guidance for a risk-based approach: virtual assets and virtual asset service providers,” FATF, Paris, Tech. Rep. June, 2019. [Online]. Available: www.fatf-gafi.org/

[34] ——, “Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing,” Tech. Rep. September, 2020. [Online]. Available: http://www.fatf-gafi.org/

[35] Europol, “Internet Organised Crime Threat Assessment 2020,” Tech. Rep., oct 2020. [Online]. Available: https://www.europol.europa.eu/

[36] L. de Koker, “Anonymous Clients, Identified Clients and the Shades in between Perspectives on the FATF AML/CFT Standards and Mobile Banking,” *SSRN Electronic Journal*, no. d, 2015.

[37] P. Rogaway, “The Moral Character of Cryptographic Work,” 2016.

[38] T. Sardá, S. Natale, N. Sotirakopoulos, and M. Monaghan, “Understanding online anonymity,” *Media, Culture and Society*, vol. 41, no. 4, pp. 557–564, 2019.

[39] FINTRAC, “Canada’s Legislation: The Proceeds of Crime (Money Laundering) and Terrorist Financing Act,” 2019.

[40] “31 U.S.C. Title 31 - Money and Finance, Subtitle IV - Money, Chapter 53 - Monetary Transactions, Subchapter II - Records and Reports on Monetary Instruments Transactions, Sec. 5331 - Reports relating to coins and currency received in nonfinancial trade or.”

[41] Ecorys and Centre for European Policy Studies, “Study on an EU initiative for a restriction on payments in cash,” Tech. Rep. December, 2017. [Online]. Available: https://ec.europa.eu/

[42] P. Sands, H. Campbell, T. Keatinge, and B. Weisman, “Limiting the use of cash for big purchases: Assessing the case for uniform cash thresholds,” Tech. Rep. September, 2017.

[43] S. Darbha and R. Arora, “Privacy in CBDC technology,” Bank of Canada, Tech. Rep., 2020.

[44] K. Yeung, “‘Hypernudge’: Big Data as a mode of regulation by design,” *Information Comm. and Society*, vol. 20, no. 1, pp. 118–136, 2017.

[45] P. Casanovas, J. González-Conejero, and L. De Koker, “Legal compliance by design (LCbD) and through design (LCtD): Preliminary survey,” *CEUR Workshop Proceedings*, vol. 2049, pp. 33–49, 2018.

[46] A. Cavoukian, “Privacy by design,” *Office of the Information and Privacy Commissioner*, 2011.

[47] L. Lessig, *Code v. 2.0*. Basic Books, 2006.

[48] D. A. Zetzsche, D. W. Arner, and R. P. Buckley, “Decentralized Finance,” *Journal of Financial Regulation*, vol. 6, no. 2, pp. 172–203, 2020.

[49] H. Nabilou, “Testing the waters of the Rubicon: the European Central Bank and central bank digital currencies,” *Journal of Banking Regulation*, vol. 21, no. 4, pp. 299–314, 2019.

[50] T. Athan, G. Governatori, M. Palmirani, A. Paschke, and A. Wyner, “LegalRuleML: Design principles and foundations,” in *Lecture Notes in Computer Science*, vol. 9203, 2015, pp. 151–188.

[51] L. Cervone, M. Palmirani, and F. Vitali, “The Intelligible Contract,” in *53d Hawaii International Conference on System Sciences*, 2020.

[52] M. Genesereth, “Computational law: The cop in the backseat,” *CodeX - The Stanford Center for Legal Informatics*, pp. 1–5, 2015. [Online]. Available: http://logic.stanford.edu/complaw/complaw.html

[53] P. Hustinx, “Privacy by design: delivering the promises,” *Identity in the Information Society*, vol. 3, no. 2, pp. 253–255, 2010.

[54] R. Renwick and R. Gleasure, “Those who control the code control the rules: How different perspectives of privacy are being written into the code of blockchain systems,” *Journal of Information Technology*, 2020.

[55] European Central Bank and Bank of Japan, “Balancing confidentiality and auditability in a distributed ledger environment,” Tech. Rep. February, 2020. [Online]. Available: https://www.ecb.europa.eu/

[56] D. Chaum, C. Grothoff, and T. Moser, “How to issue a central bank digital currency,” Swiss National Bank, Tech. Rep., 2021. [Online]. Available: https://www.snb.ch/

[57] European Central Bank, “Exploring anonymity in central bank digital currencies,” ECB, Tech. Rep. 4, 2019. [Online]. Available: https://www.ecb.europa.eu/