Central Bank Digital Currencies

Central Bank Digital Currencies

Nadia Pocher and Andreas Veneris

Abstract Today's societal digitization continues to advance at exponential speeds driven by technology trends. Billions of Internet of Things devices have made their way into our daily lives, but also into healthcare, manufacturing, and supply-chains. In contrast, the financial sector still largely operates on legacy infrastructures, where merchants receive their payments long after they released the digital/physical good to the consumer. In addition, the emergence of Decentralized Finance through blockchain technology, and the accumulation of data in private silos, have demonstrated a capacity to impact national sovereignty and monetary transmission channels. Against this backdrop, many central banks have recently started to research and test the issuance of digitally native fiat money – or Central Bank Digital Currencies (CBDCs) – in an effort to redesign the essence and use of physical cash. CBDCs present a broad variety of designs, which translate into manifold techno-legal and standardization policy questions. In this context, this chapter surveys the state-of-the art with specific focus on "retail" CBDCs. In doing so, it provides an overview of candidate architectures, heeds legal impacts and regulatory compliance issues, presents a set of case-studies and touches upon cross-border CBDC challenges.

1 Introduction

The promise of an electronic version of cash, possibly grounded on blockchain and Distributed Ledger Technologies (DLTs), has electrified the world over the past decade. This prospect has created an excitement for technological disrup-

Nadia Pocher
PhD Candidate – Faculty of Law - Universitat Autònoma de Barcelona • K.U. Leuven • Università di Bologna, e-mail: nadia.pocher@uab.cat

Andreas Veneris
Professor – Department of Electrical and Computer Engineering and Department of Computer Science, University of Toronto e-mail: veneris@eecg.toronto.edu

tion that reminds of the 1990s, when the Internet entered the mainstream. Indeed, cryptocurrency-related developments have been labelled to form an "Internet of Value(s)" [1] or an "Internet of Money" [2]. Their core premise lies in the basic functioning of blockchain systems: as they are not only secured by cryptography and economic incentives, but also governed by decentralized consensus mechanisms, they enable value transfers that transcend the need to rely on a "central" authority. Accordingly, these setups have the potential to replace the legacy financial infrastructure, by eliminating multiple layers of intermediation and informing a new "hype" of direct participation of citizens and businesses to a new global economy [3, 4, 5].

Meanwhile, the prospect of a widespread adoption of decentralized "smart" (or "programmable") money has beguilded and unsettled both governments and the private sector. Not surprisingly, this exogenous and mainly privately-driven innovation has motivated monetary institutions to start rethinking payments, transmission channels, and even the very essence of "physical cash" [6, 7, 8, 9, 10], in a worldwide quest to adapt to a new reality. If the full potential of this value interconnection is fulfilled, the impact will not be limited to payments. They will have ripple effects on the most diverse fields such as privacy, national security, law and regulation, property rights. Besides cryptocurrencies and cryptoassets, in fact, in recent years billions of Internet of Things (IoT) devices have been deployed in our daily lives. These tools continuously collect valuable data related to large economic sectors, such as healthcare, manufacturing, supply-chains, infrastructures [11, 12, 13, 14].

While this data is largely retained in privately-held and tightly-closed silos, often out of the reach of governments and local entities, their rightful owners are not in a position to profit from them [15]. Parallelly, domestic and international commercial micro-payment systems currently lack platforms and economic incentives that could underpin efficient public IoT/AI data marketplaces. Against this backdrop, it does not come as a surprise that also central banks have been investigating the deployment of innovative technologies to their own currencies. Their motivation partly lied in the possible disappearance of cash, which could deprive citizens and businesses of risk-free government-issued money. Further, as noted by an extensive literature [6, 7, 8, 9, 10, 16, 17], digital currencies can create novel payment channels, transactional communities, and novel safe networks-of-relations. Hence, they may potentially secure sovereign monetary identities, nourish past social investments, but also safeguard geopolitical digital boundaries within the global economy [18].

For the sake of convenience, Tables 1 and 2 list the acronyms used in this chapter.

1.1 Central bank money

Following the footsteps of the rapid globalization and digitization of the economy, in the past decades payment transmission systems have evolved significantly. This is related to infrastructural advancements in the institutional domain (*e.g.*, real-time gross settlement/RTGS, fast retail payment systems, instant payments), but also to the activity of an emerging private sector (*e.g.*, Big Techs, FinTech startups) [19].

AI	Artificial Intelligence
CBDC	Central Bank Digital Currency
DeFi	Decentralized Finance
DCRI	Digital Currency Research Institute
DLT	Distributed Ledger Technology
IoT	Internet of Things
M2M	Machine-to-Machine
ML	Machine Learning
mCBDC	Multiple CBDC
NFC	Near Field Communication
P2P	Peer-to-Peer
PET	Privacy Enhancing Technology
PoC	Proof-of-Concept
RF	Radio Frequency
RCC	Range Controlled Communication
RTGS	Real-Time Gross Settlement System
TEE	Trusted Execution Environment

Table 1 Technical Terms

AML	Anti-Money Laundering
BIS	Bank for International Settlements
BoC	Bank of Canada
CBDL	Central Bank Digital Loonie
CBUAE	Central Bank of the United Arab Emirates
CDD	Customer Due Diligence
CPF	Counter-Proliferation Financing
CFT	Counter-Terrorist Financing
DCEP	Digital Currency Electronic Payment
ECB	European Central Bank
FATF	Financial Action Task Force
FI	Financial Institution
FINMA	Swiss Financial Market Supervisory Authority
HKMA	Hong Kong Monetary Authority
IMF	International Monetary Fund
KYC	Know-Your-Customer
MAS	Monetary Authority of Singapore
NB	Narrow Bank
PBoC	People's Bank of China
PoC	Proof-of-Concept
PPP	Public Private Partnership
PSP	Payment Service Provider
SDR	Special Drawing Right
STR	Suspicious Transaction Reporting

Table 2 Monetary and Regulatory Terms

As of today, the vast majority of efforts are pursued jointly, through mechanisms of public-private partnership (PPP). While those innovations have indeed improved the existing system, the advent of decentralized finance (DeFi) and IoT/5G/AI has brought along even more rapid developments. It is within this context that, in the wake of the release of the whitepapers of Bitcoin in 2008 [20], Ethereum in 2013 [21]

and Libra (now Diem) in 2019 [22], legacy monetary institutions and central banks have started entertaining the idea of digitizing – more specifically, tokenizing (*i.e.*, creating a digital representation of) – M0 sovereign money [6, 23, 24].

The literature offers various definitions of "sovereign currency". Namely, [25] assumes that it is one that is "*set as such by a sovereign law, issued by an authorised issuer, and whose value results from a statutory rule*". Traditionally, central banks and monetary authorities issue two types of "central bank money":

- "General purpose money" or "fiat money" – the official and sovereign currency, also known as physical money or cash, consisting of physical coins and banknotes. It is legal tender – *i.e.*, it is legally recognized as a means to satisfactorily meet financial obligations –, which also means it must be accepted as such to extinguish a public or private debt, and it is available to the general public; and
- "Bank reserves" or "settlements accounts" – provided by central banks to authorized institutions that are participants in their RTGS systems – *e.g.,* commercial banks and non-bank payment service providers (PSPs) –, through the opening of *ad hoc* reserves accounts. In practice, they are scriptural deposits recorded on a centralized ledger (*i.e.,* database) held, settled and managed by the central bank.

Central bank money is a liability of the central bank. By extension, it can be considered a liability of the relevant sovereign government. By contrast, the majority of money that is in circulation belongs to the categories of "commercial bank money" or "electronic money (e-money)". Because it is issued by private stakeholders such as commercial banks, non-bank PSPs and e-money institutions (collectively, Financial Institutions or FIs), it essentially becomes a liability of those private entities to the public. When using commercial bank money, the end-user has a claim against an FI to receive central bank money (*i.e.*, cash) upon request (*i.e.*, the relevant monetary value can be redeemed at par). Since it is redeemable on demand, it extends central bank money. For articulate definitions and conceptual disambiguation we refer the interested reader to [6, 25, 26, 27, 28, 29].

1.2 Typology of CBDCs

The idea of digitizing central bank money was originally focused on the mentioned category of "bank reserves" or "settlement accounts", thus limited to interbanking activities. Hence, ordinary public and private financial transactions were not the target of the first explorations. Only later, following the introduction of blockchain-based cryptocurrencies, institutions started to entertain the idea of issuing digital fiat money. Accordingly, as of today there are two subsets of CBDCs, and they are developed in a parallel fashion because they respond to different payment needs.

On the one hand, a *wholesale-CBDC* is a RTGS-like settlement scheme between financial institutions. It is detached conceptually, but also practically, from the daily flows of physical cash. Although manifold designs have emerged over time, and different technologies have been deployed by both the public and the private sector,

the goal behind this type of CBDC is to update or complement solutions in the area of central bank deposits [25]. In contrast, a *retail-CBDC* is offered to the public at large, and it is the most transformative subset of CBDCs. It embodies an evolution towards a more "democratic" public transmission channel to central bank monetary holdings/policies. In this case, a digital form of fiat money is offered in a legal tender fashion, to be used for everyday transactions. From this perspective, retail CBDCs seemingly draw from the features of cryptocurrencies, albeit minimizing related risks such as price volatility, the absence of regulatory compliance, and the limited/complex exchange mechanisms [30]. In other words, retail CBDCs not only expand the concept of central bank money as we have known it for the past centuries, but also require central banks to safeguard monetary stability, efficiency and security when devising the issuance, use-case(s) and distribution of these instruments.

As the new concept of CBDCs lies at the crossroads between different disciplines – more notably economics, policy, technology, law, finance, and sociology – new definitions are necessary but also difficult. Illustratively, [31] provides a tech-oriented definition of a retail-CBDC 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, [32] 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"*. Accordingly, [26] suggests that *"A CBDC is a digital form of central bank money that is different from balances in traditional reserve or settlement accounts"*.

1.3 The Growing Interest in Issuing a CBDC

The discussion above illuminates the complex nature of CBDCs, in all terms of their definition, architecture, regulation, privacy and use-case. Likewise, over the past decade central banks, governments and monetary authorities have motivated a possible issuance in various ways. Indeed, the growing interest of central banks in CBDCs has had many drivers and opinions on their origin vary [7, 8]. However, three core factors seem to have sparked this interest.

First, the use of traditional cash by the general public has been decreasing, in favour of digital alternatives such as debit and credit card transactions and wire/electronic fund transfers. In some jurisdictions, like Sweden or Canada, the decline in the use of cash has arguably been particularly stark. The second factor relates to private altcoins and other tokenization initiatives that followed the advent of Bitcoin and later Ethereum. The latter also provides a Turing-complete smart contract language to build decentralized applications, as well as complex automated cost-effective and globally-reaching financial instruments coined as DeFi [33]. As of today, there are more than 5,000 blockchain-based cryptocurrencies in circulation. Cryptocurrencies trade at free-floating prices relative to fiat currencies and the majority of them feature

volatile price histories, which in-effect limits their usability as "money". Attempts to limit their price volatility led to the development of stablecoins and, more recently, "mega-stablecoins" such as Facebook's Libra/Diem [22].

The development of digitally native finance applications outside of the legacy networks challenges the traditional bank-based payment and monetary policy transmission mechanisms [23]. This is because it poses the so-called risk of "currency substitution" [17, 34]. This fact prompted central banks to protect their raison d'être and financial stability by investigating their own tokenization of fiat currencies. Further, the growing interest in CBDCs mirrors an effort to leverage the programmability of "digital cash" technologies into a new functional form of M0 money. Evidently, this new form of money needs to have the proper technology characteristics to serve an ever-growing digital global economy that shapes a new perception, and relation, between the public and the central bank's monetary instruments [35, 36]. Finally, central banks are reportedly attracted to CBDCs to foster payment efficiency, create new monetary policy transmission channels, advance financial inclusion, safeguard safety/privacy and regulatory compliance [6, 23, 24].

2 Characteristics and Design Choices for CBDCs

General purpose *retail* CBDCs are system-critical technologies that millions of people will be using. Accordingly, far from being a small task, their issuance needs safeguard the local economies but also elicit in geopolitical trends. Reportedly, CBDC systems should namely demonstrate the following core characteristics:

- **Privacy:** maximized but complying with regulations such as Anti-Money Laundering and Counter-Terrorist Financing (AML/CFT);
- **Universal Access:** regardless of user's means, ability or geographical location;
- **Security:** resistant to the most sophisticated cyber-attacks;
- **Resilience:** operating continuously both online and offline; and,
- **Performance:** scaling for daily use within the jurisdiction but also cross-border.

By formulating the above objectives, CBDC systems should be layered so that third parties can build on top of the core platform. As such, they should rely on flexible, long-run sustainable architectures that separate the core system from the front-end user experience, but also one that is adaptable to new consumer trends, thus accommodating the ever-changing commercial use cases. In contrast to commercial systems that focus on a specific market(s), central bank digital money should guarantee universal access to all citizens irrespective of financial means or sight, dexterity or cognitive impairments, so as to ensure accessibility and financial inclusion. Further, this e-cash should also be usable in remote communities or places, even those without Internet access, and should also serve cross-border travellers.

Although user and transaction privacy should be protected, CBDCs must adhere to strict regulatory standards, in particular with regards to AML regulation, both domestically and internationally [37]. The underlying CBDC systems must also be

resilient and robust without compromise to their fault-tolerance. They must be able to operate continuously and have low-latency while they remain scalable to serve large populations within their jurisdiction but also cross-border. Further, they should be able to communicate with existing retail payment systems and banking ecosystems, so to leverage past technology investments and established payment channels. This compatibility is also necessary to allow users to access their funds from accounts at commercial banks and merchants to accept CBDCs as a means of payment. Additionally, they need to employ architectural designs with service-quality metrics of the highest operational standards and exhibit low-cost efficiency. Finally, those designs should provide traditional seigniorage income to the underwriting central bank but also foster healthy competition in the payments market(s).

2.1 Core-Architecture Considerations

Traditionally, payment systems are classified as either *token-* or *account-based*. This taxonomy also applies to CBDCs, and it translates into how access is granted to the end-user and into the authentication/identification method used to conduct a transaction [29, 38]. On the one hand, access to a token-based means of CBDC-payment relies on the validity of the traded object (*i.e.*, the validity of a token) – hence, in principle, it is an anonymous and a bearer-type instrument grounded solely on cryptographic principles. On the other hand, in an account-based CBDC, access depends on the identification and identity verification of the account holder. This reminds of traditional commercial bank or e-money accounts that require the public to undergo a Know-Your-Customer (KYC) process to use their payment systems [6, 19, 27, 39]. As argued by [19], *"in an account-based CBDC, ownership is tied to an identity, and transactions are authorised via identification. In a CBDC based on digital tokens, claims are honoured based solely on demonstrated knowledge, such as a digital signature"*. Hence, in account-based CBDCs the system comprises a bookkeeping ledger and a payment service, where the latter refers to how payments are initiated, verified, cleared and settled [26, 40, 41].[1]

There are three different ways CBDC systems are currently envisioned in terms of their core layer-architecture and method of distribution to the public. Traditionally, a "payment" refers to the transfer of the liability of the central bank as this is recorded on the ledger. From an architectural perspective, CBDCs have been classified according to their design choices as follows [7, 38, 40]:

1. *Direct*: the central bank holds the CBDC ledger and also handles the transactions. In case of account-based CBDCs this scheme requires the public to somehow hold reserve accounts with the central bank;

[1] In this respect, [14] analyses the repercussions of the distinction between account-based and token-based systems on integration scenarios between CBDC architectures and IoT developments in the context of Machine-to-Machine (M2M) transactions.

2. *Hybrid*: the central bank holds the CBDC ledger, but the payment service is provided by private actors such as FIs or Telcos. Some authors label these systems as *platform* CBDCs [36]; and,
3. *Synthetic*: the private sector updates the CBDC ledger – *i.e.*, the ledger is held indirectly by the central bank by settling the reserve accounts through PPP schemes –, and also handles the transactions [7]. In these cases, FIs hold periodically-settled reserve accounts with the central bank, as it happens with electronic payments today. The three structures are depicted in Figure 1 below.

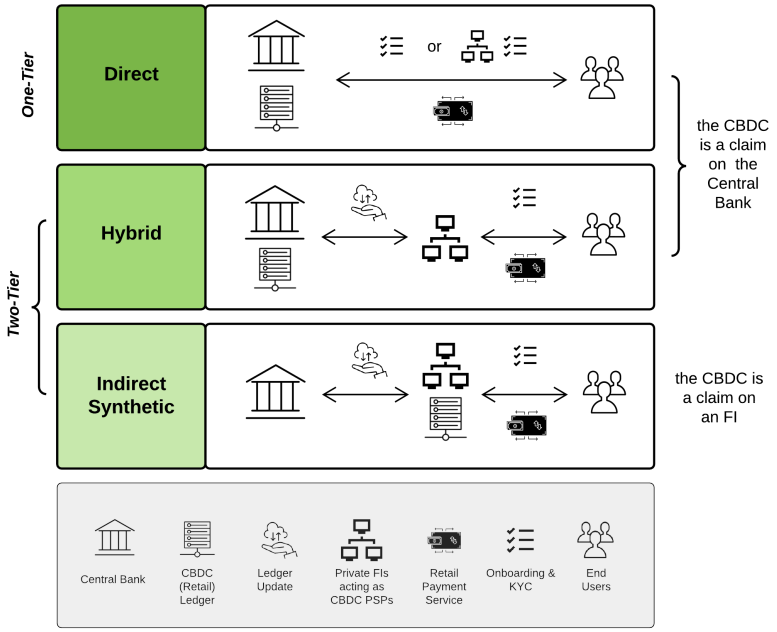

Fig. 1 Source: Elaboration of the authors inspired by various publications by the Bank for International Settlements. Most recently, [17, 38].

The *direct* structure is usually described as "one-tier", as only the central bank is involved and the CBDC is a direct claim of the public. Evidently, this entails the central bank to initiate and continuously serve a relationship with all CBDC users, a move outside of most central banks' traditional and historic core-competencies. On the contrary, *hybrid* and *synthetic* CBDC models are usually labelled as "two-tier" architectures, and their structures are less invasive than their "one-tier" counterpart. Similarly to traditional mechanisms, "two-tier" schemes require a cooperation between the government and private FIs [19, 42]. Notably, in *hybrid* structures the CBDC remains a direct claim on the central bank, even if transactions are managed

by private actors. By contrast, in *synthetic* CBDC schemes end-users interact with intermediaries, as with commercial bank money and e-money. In these cases, one can argue, the CBDC "emulates" a stablecoin offered by a private actor, and the stablecoin is essentially backed by its reserve account with the central bank. Hence, private intermediaries bear a responsibility to cover fully or in part – as provided by the respective jurisdiction – the liability of their stablecoins [29, 41, 43]. Reportedly, such a CBDC scheme resembles special-purpose licences granted to non-bank FinTech firms in jurisdictions such as India, Hong Kong, China, and Switzerland [7].

In the world of CBDCs, the circumstance where end-users do not possess a direct claim on the central bank is seemingly relevant to the definition of the instrument as a CBDC. In more detail, the intricate nature of synthetic CBDCs can be leveraged to argue against their qualification as an actual "grass-roots" CBDC. This is because by definition it is assumed that a CBDC is a direct liability of the central bank [29]. Nonetheless, experts have also commented that if the stablecoin is pegged 1:1 to the sovereign currency by means of regulation, it is ostensibly as if users are holding central bank money – and this after all is the core essence of a CBDC [43].

2.2 The Offline-Usability Conundrum

A necessary requirement for CBDCs is to be usable even when users have (temporarily) no access to the Internet. Facilitating such offline transactions results in a *trade-off* between hardware/software security, costs, and convenience. Intuitively, this trade-off is balanced with the introduction of low-cost cards that can store only a small amount of money. The main security challenge is lost (or stolen) funds. Another equally important concern is an adversary that may attempt to double-spend offline, as they may have not yet been settled through the online system. Finally, offline transactions introduce new challenges when it comes to AML compliance.

One way to implement offline transactions is via tamper-proof hardware [6, 44, 45]. Many processor chips, including those in smartphones, have Trusted Execution Environment (TEE) enclaves/capability (*e.g.,* SGX in Intel, TrustZone in ARM, KNOX in Samsung). With the use of TEE hardware capabilities, one can create appropriate hardware/software cryptographically-secured enclaves that store a small amount of CBDCs good enough for daily transactions and common expenditures (such as supermarket, restaurant, gasoline, and typical entertainment expenses) when access to a network is not available. Further, TEEs allow a smartphone to ensure third-party software applications are running on the hardware in an unmodified and untampered way. This eliminates the risk of adversaries modifying the software to double-spend the money. Although research has demonstrated that TEEs may occasionally exhibit vulnerability, they are widely used for secure transactions today.

An additional approach is to issue debit-like CBDC-cards, pre-loaded with a small number of CBDCs (*e.g.*, $ 200) from the user's wallet when the wallet is online. These cards can be programmed, with the use of NFC or RCC, to store securely in their ROM chips items like a PIN number, or even biometric information.

Afterwards, users can store CBDCs from their own smart device (smartphone, tablet or computer) when that device is online, thus crediting their online accounts. When the hardware of these CBDC-cards is activated by a nearby RF signal, they can perform sufficient power-efficient operations such as two-way cryptographic authentication and/or transmission of the encrypted data stored into them. In effect, external RF signals (like a merchant's terminal) powers them up so they can securely transmit offline the amount of CBDCs that compensates for the particular transaction – no different to what happens with modern credit/debit cards today.

Evidently, in the case of smart devices like smartphones, tablets, laptops, the process is even simpler – they already have their own power source and secured hardware to emulate the behavior of those RF-activated CBDC-cards. Moreover, these devices can act as terminals that can "activate" through RF other CBDC-cash-cards, provided their battery is not emptied. All these novel hardware designs and protocols call for new Design-for-Security embedded chip architectures – a semiconductor research area that demands a more holistic hardware design approach than just a traditional cryptographic implementation(s) [46] – but also global CBDC hardware/software co-design interoperability standards.

If a CBDC-card is lost or stolen, the user will lose the funds stored in this card, just like with physical cash when a wallet is lost or stolen. As these cards require syncing with an online wallet to deposit/withdraw funds [44], and because the amount of e-fiat they can store is rather limited, this aids the AML process as well. In closing, these pre-loaded CBDC-cards act as "cold static storage" for small amounts of quasi-token CBDCs. Further, they can be used by international visitors and tourists, but also by those who don't have access to commercial bank accounts or smart devices, thus contributing to the promotion of financial inclusion.

2.3 The Public-Private Interplay Design Factor

In light of the foregoing, it is clear that different proposed CBDC architectures lead to diverging public-private dynamics from a monetary policy perspective. The topic is increasingly explored, as it relates to a broader discussion on the preferable degree of competition between public (*e.g.*, central banks, government) and private actors (*e.g.*, commercial banks and FIs, commercial corporations) in the deployment of digital currencies. With regard to CBDCs, the main controversy is whether society can best reap the opportunities of digital payments by central banks replacing private FIs/Fintech or by simply joining forces with them [41, 43, 47, 48].

The first policy option is mirrored by *direct* one-layered CBDCs, while the situation is more complex with regard to two-layered design approaches. Intuitively, the deployment of *hybrid* and *synthetic* schemes assumes that the relevant central bank is willing to waive a portion of its power [49]. Nonetheless, two-layered CBDCs enshrine a significant distinction with regard to the boundaries of involvement of private actors in the relevant value chain [50]. Most importantly, in *hybrid* structures central banks still hold the CBDC ledger and manage end-users accounts, while in

both cases – *hybrid* and *synthetic* – payment services and relationships (along with the accompanied KYC/AML processes) with end-users are managed by the private sector – no different to what broadly happens today.

The idea of outsourcing CBDC activities to private actors through PPP mechanisms has generated a lively academic and political debate. The pivotal aspects of the controversy revolve around how to guarantee payment innovation, efficiency, "fair" competition and financial inclusion against the risk this practice may entail to national monetary choices and financial stability – both traditional goals guaranteed by the central banks themselves [41]. Further, as outlined throughout this Chapter, there are issues raised by the collection, use and dissemination of the associated user payments metadata. Clearly, the wobbling consumer confidence in the banking sector exert a significant influence on the debate [49]. More specifically, it was argued that public-private scenarios stimulate competition and disincentivize monopolies thanks to the participation of FIs. Likewise, experts maintain these mechanisms foster innovation, inclusion and credibility, while they ostensibly reduce risks and costs for central banks. By contrast, they may pose financial stability and liquidity risks in case of *synthetic* CBDCs, notably if the responsibility to maintain an adequate asset backing rests on private actors and associated regulation [17, 19, 35, 38, 41, 43, 47, 49, 51].

2.4 Cross-border Perspectives (mCBDCs)

CBDCs are often examined as stand-alone projects, pursued by one central bank or another. This is especially true with regard to the *retail* subset, with the analysis often focusing on specific domestic projects, perhaps in comparison with similar ideas. Nevertheless, the cross-border feature of tokenized money is most relevant, and generates questions that are, for the most part, still to be answered. In the past months, the Bank for International Settlements (BIS) has addressed the interactions between CBDC systems, both *retail* and *wholesale*, by exploring these arrangements [52] and surveying current trends [53]. This sparked interest in academia as well [39, 54]. Two concepts emerge as crucial: "interoperability" and "standardization".

From the first perspective, the world of DLTs/blockchain is increasingly permeated by debates on interoperability – *i.e.*, broadly speaking, the compound of "*any characteristics of systems that could help them exchange information*" [52]. In the CBDC realm, the notion is at least twofold. On the one hand, the systems devised by different jurisdictions ought to be able to communicate, also in terms of offering cross-currency capabilities. On the other hand, when CBDCs are developed through PPPs, it is crucial the various providers guarantee interoperability in the way they design the payment architecture, so not to generate closed payment silos and ensure users of different providers may transact with each other.

Secondly, interoperability relies on "standardization" – *i.e.*, the development of industry-wide technical standards within the framework of international cooperation. In the words of [52], "*common technical standards, such as message formats, cryptographic techniques, data requirements and user interfaces can reduce the op-*

erational burden of participating in multiple systems. Aligned legal, regulatory and supervisory standards can simplify know-your-customer and transaction monitoring processes". Nonetheless, there are three different options to set up a cross-border and cross-currency CBDC mechanism: *(i)* developing compatible standards, *(ii)* interlinking different systems, *(iii)* creating a single multi-currency system. Only in the latter case the outcome is an integrated CBDC "payment system" – *i.e.*, as outlined in [52, 53], a single set of participants, a single infrastructure, ledger, rulebook and governance. In the other cases, CBDC "payment arrangements" allow interoperability. For details on the pros and cons of these strategies, we refer to [52, 53].

In this context, the BIS argues through its CPMI working group for central banks to include cross-border and internationally-oriented considerations in their CBDC projects early on [52, 55]. Along these lines, the setup of "multi-CBDC" (or *mCBDC*) arrangements would deliver on the promise of improving cross-border payments efficiency against the backdrop of the increasing globalization. Arguably, the choice is between fostering communication between sovereign currencies (*e.g.*, by handling settlement in different currencies) and witnessing the creation of a global private sector stablecoin, where the first option seems preferable [52]. It is against this backdrop that important joint CBDC sandbox initiatives have been put forward by major monetary institutions all over the world [52, 53].

3 History of CBDC Projects

Central bank interest in "digital money" started emerging in 2014. However, only the People's Bank of China (PBoC) initiated work for its e-CNY platform at the time – most other R&D pilots/reports on *retail* CBDCs gained notoriety over the last 2-3 years. As of today, central banks and governments continue to scrutinize both reasons and plans to issue a digital sovereign currency. Accordingly, extensive commentaries are published by a broad range of stakeholders on a regular basis, touching upon different aspects such as security, privacy, technology infrastructure, public opinion polls, regulation and cross-border challenges [7, 8, 9, 10, 16, 26, 56, 57].

Indeed, central banks are no novices at the e-fiat expedition. The first pilots in wholesale interbanking CBDCs, DLT-based stock trading settlement and cross-border transfers started to emerge in 2015-16. The vast majority of those pioneers experimented with some form of blockchain technology. The work of [24] classifies CBDC projects as *early adopters*, *followers* and *new entrants*. Similarly, below we provide a historical summary, starting with blockchain-based settlement systems, and moving to CBDC products and other sandboxes today, as depicted in Figure 2.

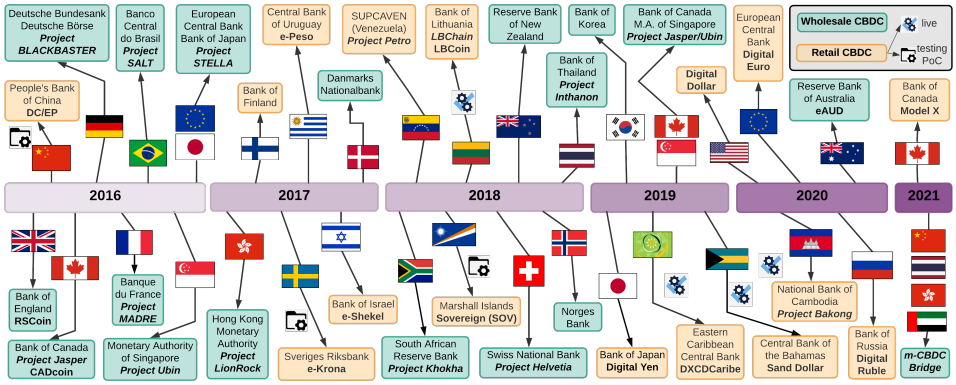

Fig. 2 Global roadmap on major *wholesale* and *retail* CBDC projects (figure taken from [58]).

3.1 The Research Pioneers: 2015-16

In 2015-16, research pioneers started exploring CBDCs by addressing wholesale interbanking use-cases. Notable references are led by the PBoC as early as in 2014 – *e-CNY*, also coined as the *Digital Yuan* or *Digital Currency Electronic Payment (DCEP)* system – and by the Bank of England (*RSCoin* [59]). Around the same time, the Bank of Canada (BoC) piloted the four-phased *Project Jasper*, one of the most comprehensive efforts up to date. As the Jasper series remains representative of sandboxing initiatives by other central banks, we provide reference to each phase:

- *Jasper I (2016)*: In this phase, the BoC experimented with DLT-based RTGS systems using the newly released permissionless platform of Ethereum.
- *Jasper II (2017)*: The BoC repeated the sandboxing from Phase 1 introducing additional liquidity requirements to the commercial banks for settlement. However, a main characteristic of that project was that the underlying network moved to the permissioned Corda one.
- *Jasper III (2018):* In the third cycle, the Bank partnered with a set of commercial Canadian banks to extend the complexity/functionality of the Corda system from Phase 2. In particular, the new system allowed not only for RGTS settlement between commercial banks, but also for settlement of stock trades from the Toronto Stock Exchange.
- *Jasper IV (2018-19):* In this last phase, the BoC partnered with the Monetary Authority of Singapore (MAS) – that had just completed three phases of its own *Project Ubin* – to experiment on a cross-border, cross-currency, and cross-platform international payments system. Another interesting aspect of this joint expedition was that one Bank used the Corda network while the other utilized Quorum, so to test the interoperability of two foreign platforms.

During that same era, 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 MAS launched *Project UBIN* and the four-phased *Project Stella* was piloted by the European Central Bank (ECB) and the Bank of Japan.

3.2 The Next Wave: 2017-19

While wholesale CBDCs remained in the limelight, with *Project LionRock* of the Monetary Authority of Hong Kong (HKMA) still addressing interbank settlements, the 2017-18 period saw the onset of *general purpose* CBDCs projects. Notably, central banks started exploring the relation between digital fiat money and cash, with one noteworthy example being the *e-Krona Project* initiated by the Sveriges Riksbank in Sweden, one of the trailblazers of the CBDC arena up to today. This is because cash usage in Sweden had dramatically declined in favor of e-payments.

The 2017-18 pilot initiatives are in both the retail and the wholesale domain, structured around CBDC concepts that are often diverse [9]. Wholesale plans were presented by the central banks of Denmark, South Africa with *Project Khokha*, Switzerland with *Project Helvetia*, New Zealand, Norway, and Thailand with *Project Inthanon*. Meanwhile, different understandings of retail use-cases were explored by the central banks of Finland (Project *E-hryvnia*), the National Bank of Ukraine, *Project Bakong* by the National Bank of Cambodia, Uruguay with *Project e-Peso*, Israel with *Project e-Shekel*, Venezuela with *Project Petro*, and the Marshall Islands.

In early 2019 around 70% of central banks responding to a BIS survey declared to be engaging in some CBDC-related activity [23]. 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 headlines. With little doubt, the watershed moment for this was the political and economic spark provided by Facebook's announcement of the Libra coin in late June 2019. In the same year, the ECB started to analyze the implications of cryptoassets on monetary policy [60] and in October 2020 a report [61] was issued on principles and configurations for a candidate retail *Digital Euro*. The goal was not to outline a specific design, but rather to gather insights from experts and the public at large. Following the reports of the Bank of Korea and the Bank of Japan, the first cross-border interbank settlement mechanism between two DLT-based currency platforms was concluded by the BoC and the MAS, noted earlier as *Project Jasper/Ubin IV*.

3.3 The Age of Maturity: 2020-21

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 smaller number with actual pilot projects [62]. Later in July, the Bank of Lithuania issued the first state-backed digital

collector coin, LBCOIN, which can be transferred in a peer-to-peer fashion. LBCOIN is no legal tender (the Bank of Lithuania belongs to the Eurosystem) and can only be exchanged into a physical collector coin. The U.S. that had remarkably been quite silent on its plans showed the first signs of life – in May 2020 the non-profit *Digital Dollar Project Initiative* released its whitepaper reasoning why the Fed should release a digital USD counterpart. Later, in June U.S. congressional hearings took place in with regard to CBDCs that continued on April 15, 2021. Earlier that year, the Boston Fed had announced a collaboration with MIT's Media Lab on a digital dollar with an expected report to be released by the fourth quarter of 2021.

The month of October 2020 also saw the landmark 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, the Eastern Caribbean Central Bank launched its CBDC labelled *DXCDCaribe*, in November 2020 Brazil's central bank launched the *PIX* instant-payment platform, and the Bank of Russia unveiled interest in a *Digital Ruble*. Also in 2020, the Reserve Bank of Australia started considering a wholesale CBDC system labelled *eAUD*.

Admittedly, the first half of 2021 testifies not only to the increasing interest in CBDCs, but also to their growing maturity. Notably, 86% of central banks surveyed by BIS were exploring CBDCs: 60% of them at an advanced experimental or PoC stage and 14% at a pilot phase [63]. In January, the European Commission and the ECB announced a cooperation on a possible *Digital Euro* upon the conclusion of a public consultation. This report was published in April [64]. In February 2021, the *Digital Dollar* debate rekindled significantly in the U.S. and the Swedish *e-Krona Pilot Project* was extended [65]. In the meantime, PBoC's testing of the *e-CNY* was widened to four cities and its launch was announced by the Winter Olympics at Beijing in early 2022. Concurrently, in February, the BoC unveiled three design proposals under their *Model X* challenge for a CBDC denominated in Canadian dollars (the *Digital Loonie*) by three universities [44]. In May 2021 the Bank of Korea issued an open competition for a PoC CBDC system to the private sector.

This era also demonstrates more mature projects in wholesale- and retail mCBDCs. These projects examine the cross-border behavior of local RTGS CBDC systems by commercial and central banks. More notable is the 2019-20 *Project Aber* by the Saudi Arabian Monetary Authority and Central Bank of the UAE (CBUAE), and *Project Inthanon-LionRock* by the HKMA and the Bank of Thailand. It is certainly not a coincidence that in February 2021 the announcement by the HKMA, CBUAE, Bank of Thailand and PBoC for a major "mCBDC bridge" collaboration was not a surprise for those experienced players. Similarly, other projects address cross-border CBDC use in 2021 – illustratively, *Project Dunbar* and *Project Jura* [53, 66].

3.4 Trends and Future Expectations

Along with the efforts by central banks to digitize fiat money, one cannot ignore the moves and associated geopolitical impact by commercial players. Most notably, Facebook's Diem consortium of more than 20 corporations, as viewed in terms of *(i)* strength in public cross-border reach and cross-border payments, and *(ii)* data protection/surveillance policies. Facebook has more than 1.5B active daily users, trending to 2.4B active users per month. Upon launch, it becomes a corporation with an international reach large enough to compare to any central bank. For historical reference, in early 2020 Facebook renamed its Libra effort to Diem, and pursued a Swiss payment licence by the Financial Market Supervisory Authority (FINMA). As the effort to attain such a license has not proved successful, in April 2021 Facebook announced Diem will focus only on the US public. In recent releases, they tap into their native coin as an "interim digital USD" backed 1:1 with assets to the US dollar.

PBoC's e-CNY launch by February 2022 and its aggressive moves to cross-border partnerships with regional players cannot also be underestimated. It has the potential to change the influence of the Remninbi, global payment systems and currencies, and the standardization of CBDCs. With no other major central bank having announced a CBDC launch, we should expect the next few years to be dominated by headlines and research from those two players – but also other independent actors. Further, one should expect the BIS, in its role of *"central bank to the world's central banks"* [34], to continue lead the standardization playground for CBDCs, notably through its CPMI working group and newly introduced Innovation Hubs [67]. Indeed, in its June 2021 report the BIS has voiced the belief that, with more than 50 central banks entertaining the idea of issuing a digital currency, the time for the monetary system to reap the benefits of CBDC-related R&D has finally come [17]. All in all, CBDCs promise exciting new challenges and innovation over the next decade.

4 Regulatory and Compliance Issues

The socio-economic (r)evolution brought about by cryptocurrencies has raised legal and regulatory questions, many of which remain unanswered to this day. Indeed, these innovations do not only challenge most areas of the law, but they do this in an ever-evolving fashion. As such, experts have been pursuing the best approach to the transformations inspired by DLTs/blockchain, cryptoassets, tokenization and DeFi, among others. To this end, efforts were made to taxonomize policy options with regard to the interplay between law and technology. Accordingly, the following regulatory options were identified: *(i)* do nothing (*i.e.,* a permissive "wait and see" approach), *(ii)* introduce tight restrictions (*e.g.,* outlaw certain activities or the provision/acquisition of certain products/services), *(iii)* issue flexible "case by case" permissions, *(iv)* set up structured, albeit restricted, experiments (*e.g.*, sandboxes), and *(v)* devise new regulatory frameworks [68, 69, 70].

When CBDCs started to emerge, it was clear their innovative techno-legal character was accompanied by a certain degree of traditionality in terms of the type of stakeholders involved (*i.e.,* central banks, regulated/regulatable intermediaries). Thus, issues originated in the context of blockchain-driven developments are channelled into a more familiar structure of overseen and regulated environments. Nonetheless, CBDCs are far from being unfettered by regulatory questions. In this section we outline a few outstanding dilemmas, with no attempt to offer a comprehensive account. Naturally, CBDCs raise manifold other issues, most of which belong to areas traditionally less harmonized across jurisdictions than the ones addressed here, as highlighted by [27, 29]. Illustratively, they relate to private and property law, contract law, tax law, insolvency law, private international law.

4.1 CBDCs and Monetary Law

Given the hype surrounding CBDC projects, it is interesting that almost no jurisdiction would currently allow their issuance without amending domestic laws. Indeed, a 2020 study by the International Monetary Fund (IMF) [29] highlighted how CBDC issuance itself poses several risks for the central banking community, burdening it with legal, financial and reputational questions. The two public law domains investigated by the report, "central bank law" and "monetary law", are crucial to warrant CBDCs a sound legal basis. The experts approached these domains separately, to conclude that while the first one could be rather addressed through legal reforms, the latter field poses structural policy challenges with a less straightforward solution.

First, if a CBDC is to be a liability of the central bank (*i.e.*, in the *direct* and *hybrid* forms described above), its issuance must be regulated by "central bank laws", as defined by [29]. This is for the CBDC to be warranted a legal basis in compliance with the principle of attribution of powers and the central bank "mandate" (*i.e.*, its "objective(s), functions and powers" [29]). Likewise, the qualification of a CBDC as "currency" must be regulated under "monetary law". If it is to be used as a mean of payment to extinguish monetary obligations, "monetary law" must treat is as such.[2]

Overall, according to [29] the legal treatment in both fields will largely depend on the specific design, from a technical and operational perspective. Namely, account vs. token-based, wholesale vs. retail, direct vs. indirect, centralized vs. decentralized, and the interrelations between these dichotomies. Hence, different reforms may be required to ensure the soundness of the underlying framework. Notably, controversies arise in relation to the lack of legal basis to issue *(i)* "token-based" instruments, and *(ii)* "account-based" CBDCs to the general public. Both aspects would require *ad hoc* amendments to the relevant "central bank law" and "monetary law" provisions.

[2] In the words of [29], *"monetary law is the legislative and regulatory framework that provides the legal foundations for the use of monetary value in society, the economy and the legal system"* and *"the basic principle of monetary law provides that it is for a sovereign State"* (or monetary union) *"to determine and establish its own currency system"*.

4.2 Anti Money Laundering and Counter Terrorist Financing

In the law and technology domain, DLT-related literature underlines how ubiquity and smart contracts-driven opportunities have fuelled fears of cryptocurrencies being misused for illicit purposes. Due to their purported traits of anonymity and untraceability, they have been linked to transactions on the dark web, online gambling, money laundering, and to the financing of criminal activities and terrorism.[3] This extends into the regulatory frameworks to fight money laundering and combat the financing of terrorism and proliferation (AML/CFT/CPF), internationally overseen by the Financial Action Task Force (FATF).[4] These rules aim to protect the integrity of the financial system by preventing criminals from enjoying the profits of their deeds, and this compliance domain exerts a significant influence on CBDC projects.

Although most jurisdictions provide their specific provisions, the structure of AML measures is fairly harmonized. Usually, a set of regulated entities is required to give "active cooperation" to the authorities in light of their position as "gateways" with (perceived or actual) oversight capacity on monetary/value transactions. These entities range from commercial banks and financial institutions, to professionals (*e.g.*, lawyers and notaries), to casinos and art galleries. In the crypto sphere, Virtual Asset Service Providers – *i.e.*, a subset of providers of exchange and wallet services – were recently added to the list. In brief, AML duties revolve around licensing, Customer-Due-Diligence (CDD) obligations such as Know-Your-Customer (KYC) and ongoing monitoring, record retention and Suspicious Transaction Reporting. The overall framework is informed by the risk-based approach, which means compliance duties are to be molded to preliminary risk assessments.[5] Ostensibly, the ultimate goal is for the competent authorities to be informed of suspicions of money laundering or financing of terrorism or proliferation.

Despite the fact that AML aspects of CBDCs are discussed extensively, these instruments are understandably not treated as cryptocurrencies in this regard, but as a form of fiat currency [8]. Nevertheless, and although CBDC-related AML considerations are detached from those for cryptocurrencies, several studies outline how different CBDC architectures may lead to various AML repercussions. A key question concerns the allocation of the responsibility for compliance duties, end-user account management, and related identity/transaction checks. As central banks do not traditionally interact with public end-users, two-layered CBDC structured may be favored. Indeed, two-tier models allow to outsource compliance aspects to PSPs and commercial banks, to be either managed directly or delegated. This intermediated access model is reportedly favored to leverage existing customer-facing services and avoid unnecessary duplication of resources.

---

[3] The Silk Road case, followed by the shutdown of Darknet markets (*e.g.*, Alphabay, Valhalla, Wall Street Market), added to this skepticism and fear. For more information [58, 71, 72].

[4] The FATF is an intergovernmental, policy making, monitoring and enforcement organization that sets standards and provides comprehensive guidance, *e.g.*, its Recommendations. Its mandate was extended to combating the financing of terrorism in 2001 and of proliferation of weapons of mass destruction in 2020. In the remainder of the Chapter, AML refers to AML/CFT/CPF.

[5] For instance, CDD must be "enhanced" in specific cases identified as posing noteworthy risks.

4.3 Cash, Anonymity and Identification

Even if the technology underpinning Bitcoin is largely acknowledged to inform a *pseudonymous* means of payment, rather than an *anonymous* one, a significant set of altcoins has increasingly evolved toward higher levels of anonymity and cryptographic complexities. Accordingly, the FATF emphasized growing money laundering concerns in terms of virtual-to-virtual "layering" mechanisms [73]. Concurrently, tech advancements in "privacy coins", such as Monero and ZCash, and pervasive transaction obfuscation mechanisms (*e.g.*, mixers/tumblers) were complemented by the advent of decentralized exchanges, unhosted wallets and cross-chain atomic swaps [72, 74, 75]. In this context, the FATF identified several concrete examples of *anonymity* as "red flag indicators" of suspicious activities in the crypto sphere [76].

When it comes to electronic transactions, controversies on *anonymity* well preceded cryptocurrencies and CBDCs. Indeed, the debate dates back to the '90s, and targeted anonymous digital cash and e-cash [77, 78, 79]. To be more precise, the core issue had already flourished with regard to physical cash. As the trait of *anonymity* is inherent to latter, which is one of the purest examples of a fungible asset, the fight against financial crime has long faced the "anonymity problem", and has addressed it leveraging identification and traceability aspects. Indeed, (some form of) "identification" is argued to be necessary to safeguard the payment system. In a CBDC scenario, the issue is interlinked to the opportunities offered by digital identities (digital IDs) and digital identification, as recently underlined by [17]. More specifically, [19] shows how AML and anti-fraud practices may imply a trade-off between access to the means of payment and traceability. If CBDCs are designed to replicate a situation that is similar to cash-like anonymity, but at the same time they overcome the material physical limitations of coins and banknotes, significant concerns may arise. In the words of [17], *"a token-based CBDC which comes with full anonymity could facilitate illegal activity, and is, therefore, unlikely to serve the public interest. Identification at some level is hence central in the design of CBDCs"*. What is interesting, however, is that cash being dangerous from an AML perspective was one of the reasons why e-money solutions, and the degree of control they can enable through their programmability, were sponsored in the first place [6, 47].

Indeed, monitoring and/or limiting the use of cash is a widespread means to counter criminal activities. Thresholds for customs declarations are provided and cash transactions above certain volumes trigger compliance duties and other measures. In the EU, CDD obligations arise for FIs upon the establishment of a business relationship or when the customer carries out transactions that amount to EUR 15,000 or more. In Canada and in the U.S., obliged entities must report transactions of CAD/USD 10,000 or more within 24-hours [80, 81]. The EU has considered to introduce restrictions to payments in cash [82], and the recent 2021 "AML Package" is proposing a EU-wide limit of 10,000 EUR to payments in cash, including

bearer-negotiable instruments, for professional purposes [83, 84].[6] Meanwhile, some countries already limit its use between private individuals if no regulated intermediary is involved in the transaction [85]. Bearer's instruments, such as bearer's checks and passbooks, are often equated to cash. Illustratively, in Italy cash transactions that exceed EUR 1,000 are prohibited, 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, similar strategies are applied to specific types of transactions in Jamaica, Mexico, Uruguay and India.

4.4 Privacy and Data Protection

A major driver behind the onset of cryptocurrencies has been the desire to exchange money privately, without the involvement of a third-party intermediary. Additionally, after the adoption of the EU General Data Protection Regulation (GDPR) in 2016, a wave of global-scale sensitivity to privacy and data protection concerns started to inform the law and technology domain. At times, AML frameworks and privacy/data protection may seem at odds. Scholars have focused on this possible contrast, especially when it comes to permissionless blockchains [86], and with reference to specific concepts (*e.g.*, Privacy Enhancing Technologies (PETs), de-anonymization techniques). An extensive array of contributions addresses the interplay between blockchain, privacy and data protection [69, 86, 87, 88, 89]. The topic appears as most relevant to the discussion on CBDCs, and it is at the heart of heated debates in the context of the initiatives put forward by central banks.[7]

Additionally, the public-private dynamics of different CBDC designs originate diverging questions, as private stakeholders may be made part of mechanisms of information exchange possibly detrimental to the individual privacy of end-users. Indeed, one of the reasons why AML aspects are discussed in CBDC projects is that they are seemingly opposed to privacy and data protection safeguards. The more information *is* or *can be* disclosed to obliged entities and law enforcement authorities, the more intrusive this may be with regard to financial aspects of end-users' lives.[8] By contrast, a system with full privacy would thwart compliance regimes. These considerations are mirrored by CBDC research, with manifold attempts to build anonymity-oriented scenarios while ensuring a certain degree of oversight to avoid dangerous criminal repercussions. Relatedly, [91] puts forward a CBDC architecture

[6] This is an example of the application of the risk-based approach to the threat posed by cash-intensive businesses. Meanwhile, EU Member States would still be able, if not encouraged, to maintain lower thresholds and/or adopt stricter provisions.

[7] The final report of the ECB public consultation on a candidate Digital Euro [64] is an example of the debate on the interplay between privacy, security and AML rules.

[8] As argued by [90], transaction privacy is severely hampered by user-level payment history datasets. The latter are increasingly generated by commercial payments platforms, while other dangers arise from subsequent monetization and/or clustering. Progress in AI/ML techniques amplifies the risks.

that aims to combine privacy with regulatory oversight by holding CBDCs outside of custodial relationships, while [14] explores M2M scenarios.

The relevance of this debate is not exclusive to CBDCs, but to digital payments at large [90, 91]. Nonetheless, CBDCs have a significant potential to impact on the individual from a twofold perspective. As argued by [36], they may "*diminish individual privacy, whether defined as freedom from intrusion into private life or the ability of an individual to control her or his own personal information and protect against its misuse, or with reference to data protection, security and safety, or even freedom from mass monitoring, profiling or surveillance*". Indeed, *"the combination of transaction, geolocation, social media and search data raises concerns about data abuse and even personal safety. As such, protecting an individual's privacy from both commercial providers and governments has the attributes of a basic right"* [17].

Relatedly, [36] highlights how the issues raised by CBDCs are informed by a broad conceptualization of "privacy".[9] Indeed, albeit often voiced as if they were a single concept, CBDC-related "privacy" concerns different stakeholders – *e.g.*, the central bank, settlement and payment providers, retailers. In this sense, experts have focused on the governance of how network participants can access the CBDC system. This is crucial upon establishing the respective roles of public and private stakeholders in guarding identity and transaction data [19].

4.5 Privacy-Transparency Trade-Offs

CBDC-related AML issues diverge from those arising in cryptocurrencies. However, if e-fiat money is advertised as a "physical cash" substitute, any desire for a certain share of anonymity needs to avoid any detriment to the integrity of the financial system. Nonetheless, anonymity is not a binary zero-sum property, but rather *ranges* within a spectrum.[10] Further, online anonymity has a socio-technical nature [15, 93]: on the technical side, and within a DLT context, it is influenced by the deployment of specific privacy tools (*e.g.*, PETs), governance considerations (*e.g.*, centralized vs. decentralized systems), and the broader system architecture (*e.g.*, relationship with other on/off-chain layers); on the social side, it refers to the actual possibility of identification and traceability and to the use of forensic techniques to "follow the (crypto) money", against the backdrop of the strategies to prevent this [58].

Although a tension between privacy and transparency seems to be inherent to CBDCs, at a closer look it appears as a *trade-off* [15]. Indeed, all means of payment provide varying degrees of privacy/anonymity, ranging from methods requiring the bank to monitor transaction/identity data (*e.g.*, wire transfers), to anonymous transactions in physical cash. As opposed to the latter, digital cash allows to exert control, which means sensitive information may also be exposed [6]. Against this backdrop, not only CBDCs can be designed to embed various "privacy vs. transparency" trade-

[9] On some of the privacy and data protection concerns raised by CBDCs, see also [35].

[10] [92] addresses the difference between anonymous, identified and pseudonymous clients and the AML impacts. "Crypto" digital payments enhance these complexities [58].

offs, but DLTs themselves are conducive to balancing the individual right to privacy against AML public interests. While a fully-transparent CBDC, with real-world identity transactions fully visible to law enforcement, may violate human rights, if privacy is provided without limitation (*i.e.*, no information can be revealed about transactions) misuses for illicit purposes may not be averted. This option is not viable to regulated stakeholders, as it may generate dangerous societal impacts.[11]

Luckily, nuanced solutions are available, and most CBDCs position themselves in the *middle*, offering some privacy to end-users and some visibility, in terms of auditability, to authorities. The work in [58] addresses this trade-offs and elaborates on the findings of [94] with regard to confidentiality and auditability. As outlined in Figure 3, different CBDC designs can be classified accordingly. While they entail different trade-offs, a correlation is to be noted between the latter and AML anonymity-related provisions. An interlink between technical and regulatory compliance assumes the latter can be embedded into technology. This concept informs *design-based* regulatory techniques and *regulation-by-design*, as a means to foster desirable outcomes by devising inherently compliant instruments.[12] In closing, research currently shows different data privacy preferences across the globe and CBDC initiatives embody context-specific inclinations, as shown in [19].

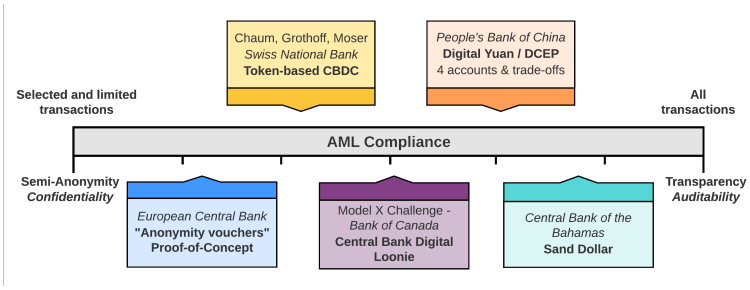

Fig. 3 Source: Elaboration of the authors in [58].

5 A Deep Dive: Three CBDC Case Studies

The previous sections retraced the evolution of CBDCs from a techno-legal and historical perspective. Some specific projects, however, have played a particular technical and geopolitical role with regard to the trends and future development of the global CBDC ecosystem. In this section we detail three of these instances, in a case-study fashion. First, we dive into the PBoC's *DCEP* – it is not only the first

[11] Additionally, history shows that a regulated access of financial authorities to information on monetary/data flows resonates positively with citizens and businesses.

[12] [14, 58] show how law and technology experts address this notion [47, 68, 95, 96, 97].

fully-operational CBDC system, but also projects a major influence in the domestic and cross-border digital payment arenas, as also indicated by recent U.S. Senate hearings. Next, we move to Facebook's *Diem*. Although one may argue Diem is not a CBDC – it is not offered by a central bank, but by a private consortium of corporations –, Diem holds most elements of a synthetic CBDC platform and, as noted earlier, it is now "advertised as such" by its founders. Finally, we outline an academic proposal to the BoC's February 2021 *Model X* challenge. At the time of this writing, we respectfully submit that the BoC has not publicly committed to issue a CBDC. Hence, the three *Model X* challenge proposals reflect only the opinions of their academic authors. As this published CBDC-related *Model X* challenge was the first of its kind by a central bank, but also due to its intricate design details, it warrants this third case study in a complementary position to the first two.

5.1 China's DCEP/e-CNY

The rapid rise of China's DCEP, also labelled e-CNY, as a CBDC leader is a natural outcome of the country's fast-paced mobile-based economy digitization in the past decade, even by the most competitive Western standards. According to a brief by Deloitte Digital [98], in 2018 more than 70% of China's 829 million netcitizens use mobile devices to make payments, a swift 60% increase in just three years. In the first nine months of 2020, mobile payments exceeded $48B in value – an 135x increase since 2012 [99]. The amount of data generated by China's commercial sector has already surpassed that of the U.S. and is expected to grow to 48.6 ZB by 2025 – in contrast to an expected 30.6 ZB projection for the U.S. [98]. As another example, more than 96% of the revenue during China's Double 11 Festival in 2019 came from mobile payment systems. The maturity of this system now allows the public to utilize their personal IDs to essentially "individualize" their e-commerce experience.

With those digital cultural trends already spilling abroad, China's technology companies today claim more than 40% of their revenue sources from foreign actors. A main driver in this digital revolution has been the widespread adoption of the Alibaba and WeChat e-payment methods in the past decade. Today these platforms serve the vast majority of those commercial interactions/transactions.

Rationale and History for the DCEP: Until July 2021, the PBoC had issued no comprehensive published research paper that explained the technical architecture details behind the e-CNY and its underlying motives. Hence, over the past years information has been mainly derived from public talks by Chinese officials, such as Mu Changchun (Director of the Digital Currency Research Institute (DCRI) of PBoC) and Qian Yao (former Head of the Institute of Digital Money at PBoC), or from newswires and Chinese/Western opinion articles. Under those conditions, the motives and drivers of DCEP seemed to include:

- The rapid digitization of the economy by private actors (WeChat, Alibaba, etc) and the risks generated by those companies as they silo the associated user-data;

- The additional risks to China's monetary policy, capital flows and currency sovereignty by the emergence of alternative coins such as Bitcoin, Ethereum, Facebook's Libra/Diem – but also from other forthcoming CBDCs;
- The need for a SWIFT-alternative to cross-border payments as the network has been claimed to be using its underlying data for U.S. geopolitical interests [100];
- An add-on to China's recent Cross-Border Inter-Bank Payments System; and,
- The natural progression of China's efforts in the past 20 years to expand the internationalization and influence of its own currency, more notably to countries within the Road & Belt Initiative.

In a speech on December 25, 2020 at the Chinese Winter Olympics Group, [13] Mu Changchun said the PBoC's adventure into the world of digital currencies first started in 2014. Back then, the designated working group concluded there was no need to issue a digital currency, partly because 3G networks were not sufficient to support such a novel expedition. However, Mr. Changchun continued, due to the threat of Bitcoin to countries with closed capital controls like China, the Bank had formed the e-M0 group to further investigate the matter and to first build a prototype borrowing from Bitcoin's architecture. Later in that talk, he added that Facebook's 2019 Libra announcement had increased initial concerns. In 2016, the PBoC formed the DCRI working group. In the same year, the e-M0 group determined blockchain-based technology cannot serve the needs of a national digital currency. This is because the one-tier Bitcoin-based archetype does not prove adequate to the technical needs of a modern e-payment platform such as the one China's economy commands.

Later, in 2017, the DCRI expanded its efforts by including more blockchain, legal and hardware-design expert staff. In the dawn of 2018, it announced the introduction of China's CDBC as a main priority. By mid-2019, the PBoC declared it was ready to launch DCEP, and by April 2020 pilot tests were conducted in four geographical regions: the Xiongan area in the Hebei Province, Suzhou in the Jiangsu Province, Chengdu in the Sichuan Province, and Guangdong's Shenzhen. This occurred by "airdropping" a limited number of e-CNYs to the public for use, and user-experience feedback, at a few merchant locations. Meanwhile, mCBDC *Project Inthanon/LionRock* was initiated by the HKMA and Bank of Thailand. In the following months, pilot tests were conducted in more targeted environments such as Shanghai's Tong Ren Hospital and Beijing's Metro Daxing Airport Express, while the state-owned Agricultural Bank of China launched the first e-CNY ATM machines. As the official launch of e-CNY is set for the Winter Olympics in Beijing in February 2022, a year earlier the UAECB, Bank of Thailand, HKMA and PBoC announced a cross-border DLT-based mCBDC project. On May 22, 2021, former PBoC governor Xhou Xiaochuan at a speech at the Tsinghua Wudaokou Global Financial Forum underlined how the DCEP is not built to displace existing payment systems, nor to replace the U.S. dollar as a currency reserve. [14] The interested reader is referenced to [99] for an elaborate chronology of DCEP's history and deployment.

---

[13] https://www.youtube.com/watch?v=U6tUrUpDCW4&t=2126s&ab_channel=PlusToken

[14] https://mp.weixin.qq.com/s/OWkVaWw0-f2wSSFFH979rg

As anticipated, in July 2021 the e-CNY Working Group at the PBoC released its first R&D white paper [101]. Its main goals are to clarify the position of the PBoC and to explain its objectives and visions, as well as e-CNY's design frameworks and policy considerations, to the end of engaging into multi-stakeholder communication. Accordingly, the expert group highlights:

- the link between the rapid evolution of the digital economy and digital payments, and the need for new, safe, inclusive and adaptive retail payment infrastructures;
- the profound change in China's use of cash – according to a 2019 survey, "*the number and value of transactions via mobile payment accounted for 66% and 59% of the total, while those paid in cash accounted for 23% and 16%, and those paid by card 7% and 23%, respectively. Among those surveyed, 46% used no cash in any transaction during the survey period*" [101] – and the consequent need for digitalization to safeguard access to cash itself and financial inclusion;
- the rapid development of global stablecoins; and
- the attention paid by the international community to CBDCs and their different design options, as well as the the importance of the internationalization of e-CNY and its role in cross-border payment programs.

Architectural DCEP Considerations: As defined in [101], the e-CNY"*is the digital version of fiat currency issued by the PBOC and operated by authorized operators. It is a value-based, quasi-account-based and account-based hybrid payment instrument, with legal tender status and loosely-coupled account linkage*". The model features a centralized management and a two-tier operational system, where the PBoC is positioned at the centre. The PBoC issues e-CNY – in parallel to the physical RMB – to "authorized operators" (*i.e.*, commercial banks and licensed non-bank payment institutions) that, in turn, exchange and circulate it to end users.

Hence, the e-CNY is reportedly a direct cash-like claim on the central bank, with client onboarding and payment services managed by intermediaries. As Mu Changchun had added on December 25, 2020, DCEP is a "two-tier" architecture where the PBoC does not directly issue it to the public, but to a second tier of commercial players coined as "designated operating institutions", most likely in exchange for central bank reserves. Currently, the designated operating institutions are state-owned commercial banks, Alibaba (Ant Group), and WeChat (Tencent), together with the three major telcoms, namely China Unicom, China Mobile and Telecom. Later, Mr. Changchun commented, with the State Council's approval, Postal Savings Bank and Bank of Communications may be added. He further claimed a main reason for the system to be two-tiered is that there can be data breaches or hacking risks if it was built as an one-tier; the two layers prevent this with their diversification. In another report [42] it is claimed the infrastructure entails a mix of a conventional database and DLTs, where a copy of holding and transaction data is received and settled by the PBoC on a regular basis. To that end, it remains to be seen how China's President Xi Jinping's December 2019 promise for a national initiative to "seize blockchain opportunities" globally may materialize [102].

Interesting insights are provided by [101] with regard to the concept of "*controllable anonymity*" or "*managed anonymity*". Indeed, as commented by [58], the

e-CNY is informed by the principle of "*anonymity for small value and traceable for high value*" and may offer four or five types of accounts/wallets. The decision on which account to assign to a given user rests on characteristics such as CBDC amounts, anticipated use, and other information provided during registration. Reportedly, the two most anonymous types of account – *i.e.*, the "*least privileged wallets*" [101] – require few identifying information and no real-name identity. In these cases, risks of money laundering and other criminal abuses are mitigated by imposing strict balance and transaction limits – a daily transaction limit and a relatively low balance limit. On the contrary, depending on the provided information, the least anonymous types of wallets must be opened at a counter, can be linked to a bank account or even used as one. Further, the implemented restrictions (if any) vary, depending on the "*strength of customer personal information*", with regard to both types of transactions that can be performed and relevant amounts.

The e-CNY offers both software and hardware wallets [101]. Offline transactions are designed in a way that resembles the CBDL report [44] and the 2019's commentary by the Mount Union of Science and Technology. [15] Nonetheless, even in the most anonymous scenario among the account types, some identifying information is given when the account is opened. Hence, one may be expecting that the true identity of the user can always be retrieved. In any case, by implementing this multi-layered structure 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 can de-anonymize suspicious transactions for AML purposes. Privacy and data protection issues raised by the e-CNY's two-layered structure are addressed by [35], although [101] argues e-CNY is expected to collect less transaction information than other e-payment systems, and to disclose information to third parties or other governmental agencies only if mandated by law. To this end, China's central bank plans to prohibit arbitrary use of e-CNY data and to set up an internal firewall, as well as to implement security and privacy protocols – *e.g.*, separation of e-CNY from other business lines, tiered authorization system, internal audits.

Although on the surface the DCEP seems like a hybrid CBDC architecture, one should examine this statement under a prism of China's domestic policies/practices. Considering that major Chinese banks are state-owned/controlled, but also the history of authoritative power/actions by the Communist Party of China onto the domestic commercial sector, it becomes a belief that DCEP borrows many elements from a direct CDBC architecture that only borderlines to a typical hybrid model.

Domestic and Global Implications of the DCEP: Although denied in public speeches by China's government officials, the overwhelming rhetoric by news media from both the East and the West is that the DCEP presents a challenge to the U.S. monetary system but also to the USD's currency reserve status. Some even take the view that DCEP's emergence will be used as a "digital weapon" against the U.S. in economic, trade and geopolitics as it will eventually allow China to obtain the data and track (or even block) international transactions just like the U.S. has done

[15] https://www.mpaypass.com.cn/news/201912/06094420.html

with the SWIFT network in the past.[16] According to statistics by the World Bank, more than 1.7B adults around the world use cash because they don't have access to a bank account. Nevertheless, more than two-thirds of this population use mobile phones that can be eventually used to conduct mobile payments. Indeed, this is what happened in China (but also India) during the past decade: it is not uncommon in both large-population countries to see street merchants using QR-codes to sell their products. Along with China's technology investment in the emerging Belt & Road initiative region, it becomes a realistic scenario for the e-CNY to enjoy distribution/adoption to those countries after it proved its maturity domestically.

The tremendous "early adopter" impact of the DCEP could likely go much further to establish novel e-commerce channels for China, as artfully articulated in [104]:

- *Business-to-Customer flows:* the e-CNY has the potential to massively level the operations between banks and big tech, while further squeezing merchant acquiring businesses. It also opens up new opportunities for licensed e-CNY providers looking to provide banking services to supply chains and end-consumers;
- *Cross-border Business-to-Business flows:* this relates to cross-border trade settlements, with China being already one of the larger exporters/importers in the global economy, but also a leader in global foreign direct investments; and
- *Consumer-to-FIs flows:* this relates to domestic and international e-service innovation due to the cost-competitive and tech-efficient nature of the DCEP.

5.2 Libra/Diem by Facebook et al.

As widely acknowledged, the watershed moment for central banks was June 18, 2019 when Facebook and its associated consortium – the "Libra Association" – unveiled the forthcoming introduction of the Libra coin [22]. The announcement brought shock-waves across the globe to governments and the private sector alike. Within hours, the U.S. Senate and Congress called Facebook testify on their plans. During those hearings, members from both chambers were critical of Facebook's past practices on data protection, but also of their plans to obtain regulatory clearance. The next day, both the EU and China made similar succinct commentaries.

It therefore comes as no coincidence that on June 23, 2021 the BIS in its Annual Economic Report [17] urged central banks to issue CBDCs as soon as possible, as "*the most significant recent development has been the entry of big techs into financial services. Their business model rests on the direct interactions of users, as well as the data that are an essential by-product of these interactions . . . the user data in their existing businesses in e-commerce, messaging, social media or search give them a competitive edge through strong network effects. The more users flock to a particular platform, the more attractive it is for a new user to join that same network, leading to a Data-Network-Activities or DNA loop*". The report emphasizes additional concerns

[16] For example, see [103].

if central banks delay their CBDC introduction – notably, if digital currencies are introduced by the private sector first, the risk of "currency substitution" [17].

History and Economics of Libra/Diem: The Association's first Libra-coin revelation in June 2019 [22] intended to design it as a basket of the five sovereign currencies that compose the Special Drawing Right (SDR) by the IMF, no much different to what described in [105] a year earlier. The announcement displayed an Association of corporate and non-profit organizations – a list that included Visa, PayPal and Mastercard – that planned to support the ecosystem after an initial deposit of a minimum of $10M in return for Libra Investment Tokens. Following the backlash by domestic and foreign governments, by fall 2019 some members dropped out of the Association. In the spring of 2020, the project shifted to offering a set of stablecoins – USD, EUR, GBP and the SGD – and also abandoned its plans for a permissionless system. In December 2020, it rebranded itself as Diem. By April 2021, the Association petitioned for a payment service license from FINMA. A year later they dropped trying to obtain it, and focused on the U.S. via a USD stablecoin.

For the sake of simplicity, in the coverage below we use the term "Diem" to indicate the project from infancy. Diem is the base currency in the system. At the time of writing, it appears to be pegged to the USD only. Each coin is backed by a reserve that contains mostly low-risk liquid assets (like highly-rated U.S. government securities) but also cash accounts. This reserve protects the coin from the highly volatile price distributions of traditional cryptocurrencies. The Diem Association manages the currency reserves, with its members acting as liquidity providers during on-boarding and off-boarding periods. The Association mints and burns the Diem-coin based on the fiat deposits and withdrawals in its reserve. Frequent auditing provides continued public confidence into the ecosystem, while other designated dealers and regulated virtual asset providers are added as the network matures.

According to [99], the main use-cases of Diem include:

- *Local Payment & Commerce Systems*: bringing a unified experience in e-commerce – *e.g.* Facebook, Instragram, WhatsApp and other e-commerce platforms are powered by Diem to eliminate the costs and multiple layers of other existing and expensive payment mechanisms today;
- *A CBDC Sandbox*: this is the case where smaller countries choose the Diem ecosystem as a sandbox to build their own CBDCs, no different to typical open library-based software development practices today; and,
- *Cross-border Payments*: with recent shifts in U.S. markets, [17] this task may come into a jeopardy. With time though, Facebook's 2.5B reach is expected to promote system adoption, including audience in U.S. "politically friendly" jurisdictions. As cross-border payments today remain expensive (it is estimated they cost up to 7% of the remitted amount – in less advanced economies this climbs above 12%), Diem has a potential to disrupt this sector economically but also geopolitically.

One cannot but only observe the stand-out parallels between Diem and the DCEP in their root motives, use-cases and objectives.

[17] Diem's announcement was posted shortly after the release of the said Citibank report

Diem's Baseline Architecture: At the outset, Libra was designed as a permissioned DLT, governed and operated by its consortium of private organizations. The DLT is maintained by the consortium members termed as *validators* in terms of the consensus protocol. Using a state replication paradigm designed on top of the Diem Byzantine Fault Tolerant (BFT) consensus mechanism, the validators preserve an identical database. Diem's BFT is a variant of the Hotstuff protocol [106] – also used in Ethereum's Casper and the Tendermint protocols: it guarantees safety and liveness in a partially synchronous system. Its conservative nature ensures that agreement over the state of the system is reachable by the validators at any point in time – even in the presence of byzantine faults. All the rules around validator management, governance, transaction processing, security policies, and incentives are implemented as smart contracts in Diem's programming language *Move* [107].

Indeed, the Move language – or, the "programming language of money" as it is advertised – is one of the core contributions of the Diem ecosystem. Designed by Facebook's Novi team, Move is a safe and flexible bytecode-based programming language with which one can create transaction scripts and smart contracts that can affect the system's state. A key feature of Move is the notion of "first-class resource types". Here, resource types have pre-defined semantics around their logic: they cannot be copied or discarded. This makes them secure and protected by definition. Move's other highlight is its inherent ability to prove the smart contracts' properties formally. In particular, along with the semantics of Move, a specification language and a formal prover has been provided by the Novi team to allow developers to add properties and formally verify that their contracts are functionally correct.

Overall, Diem's open-source implementation and the completeness of Move are ingrained with features that are arguably essential to any CBDC "programmable money" infrastructure. With modularity as one fundamental design feature, it allows usability in other protocols as well. Given that a complete functional Move verification toolset/methodology is also provided, the language certainly stands out compared to other high-level smart contract languages like Solidity and Vyper. As of today, the project is at a testnet stage, with the network set to go live by late 2021. Once it proves maturity, one should expect open access to third parties (*i.e.*, regulated virtual asset providers) to submit Move-based decentralized-apps – no different to what happens today with Google Play (Android) and Apple Store (iOS) apps.

Is Diem a CBDC? Diem is not a CBDC in the traditional sense of the definition, as it is not issued by a central bank. With no doubt, its goal is to serve the business interests of its private consortium members and its virtual asset provider partners. However, considering its recent partnership with the Silvergate Bank [108], but also the patronage by its leading economist Dr. Catalini as an "interim digital dollar" until the Fed "acts" [109], Diem is positioning itself with "proxy CBDC features". As synthetic CBDCs are usually compared to stablecoins, Diem's architecture and operation arguably bears strong similarity to synthetic CBDCs.

5.3 Model X: a Canadian Central Bank Digital Loonie

Soon after completing the four phases of *Project Jasper*, on February 25, 2020 the BoC published its *Contingency Planning for a Central Bank Digital Currency* [110]. In this plan, the BoC disclaimed it has no plans to launch a CBDC, but only wants to build the capacity to issue a general purpose, cash-like, CBDC should the need to implement one arises. It also noted that it will consider launching a CBDC if certain scenarios materialize, or appear to be likely triggered, such as:

- A continuous decline in the use of banknotes to the point where Canadians no longer can use them for a wide range of transactions; and/or,
- A situation where one or more alternative private sector digital currencies start to become widely used as an alternative to the Canadian dollar as a method of payment, store of value and unit of account.

Two months later, in April 2020, the Bank issued an academic competition-for-proposals under the *Model X* title, addressing the five policy objectives noted in Section 2 – Privacy, Universal Access, Security, Resilience and Performance. The BoC also specifically requested a solution with an accompanied "business plan" that does not put it in direct contact with the end-users (*e.g.*, services such as identity verification or account opening/servicing), although it remained open to providing a baseline service to them. Further, the solution should adhere to the highest service-quality metrics and foster healthy competition in the payments market.

The remainder of this subsection outlines a techno-legal economic proposal submitted by a team from the *University of Toronto* and *York University* [44] for a *Central Bank-issued Digital Loonie*, or *CBDL*. In brief, the proposal argues for a *two-phased* account-based KYC-backed approach. In the first phase, the BoC establishes a digital cash mechanism based on a *centralized platform* with an authentication protocol based on existing resources that safeguards users' privacy/data. In the second phase, the BoC expands this platform to a backbone that allows private enterprise to build *a decentralized messaging platform* under the auspices and supervision of the BoC and transforms CBDLs into "programmable e-money". Offline transactions are served through a quasi-token-like portable CBDL-card, similar to what described earlier. Finally, the proposal contains extensive reference to legal/regulatory considerations.

CBDL Principles: CBDLs have the following physical-cash characteristics: *(i)* they are a liability on the BoC's balance sheet where each CBDL is equivalent to one Canadian dollar, *(ii)* they are available to every registered Canadian resident and corporation, *(iii)* they transfer quasi-anonymously among verified e-wallets that require one-time e-KYC so they initially get set, *(iv)* transfers are in real-time with minimum fees, *(v)* they allow offline transactions, *(vi)* they generate seignorage income for the BoC at creation, and *(vii)* they comply with AML regulations. Whether CBDLs bear interest or not, it is a viable system option yet a policy question.

Phase 1 Operation: In the first phase, the BoC establishes an entity that provides CBDL-accounts and processes all CDBL transactions within a tightly-closed centralized system. This phase also disrupts and establishes a new status-quo in cash-like

payments by introducing CBDLs. In doing so, it requires an expansion of BoC activities by incorporating and overseeing an entity that provides CBDL-accounts to millions of residents and businesses, but it is also responsible for the processing of large numbers of transactions of BoC-issued CBDLs per day and conducts overnight AML – namely the *"Narrow Bank" (NB)*. The NB will have no physical location to serve end-users and its staff can reside within the BoC premises, for instance. Further, CBDL transaction messages in the first phase trigger push transactions providing immediate settlement by the NB. This is possible because those transactions are direct transfers between fully-funded CBDL-wallets that involve no credit

An important proposal argument is that the CBDL platform should secure Canadians' privacy by default but also allow them to monetize their data. It is also suggested for AML to leverage existing public infrastructure (*e.g.,* provincial service agencies, or Canada Post) and private sector solutions by Canadian-owned FINTRAC FI firms for KYC. Eligible Canadian residents and businesses obtain their wallet addresses after under-going this e-KYC. Wallet addresses are represented by a quasi-anonymous identifier, built to not identify the user identity or the respective transaction-data to other system parties. However, CBDL users are not anonymous when the homomorphic encrypted AML process triggers compliance flags, or to court orders that direct to reveal certain information. This onboarding and transaction processes bear similarities to India's Adhaar system [111] that provides each citizen with a digital biometric identity allowing them to transact without releasing identities or transaction-data between the parties. Finally, it is proposed user-wallets have upper limits (*e.g.,* 10,000 CBDLs) sufficient for typical cash-like transactions, and special provisions, such as reduced functionality or with preset-expiration dates, for tourists or business visitors. It is also suggested e-KYC should not contract international parties to safeguard Canada's sovereignty and ensure data does not leave Canada.

Phase 2 Operation: The second phase introduces a permissioned quasi-decentralized payment messaging programmable layer on top of the Phase 1 infrastructure to improve scalability and promote digital and economic innovation. A select number of entities (such as major FIs) with experience in handling technology, AML and data will be invited to join the network as "validator nodes", to process CBDL-related transactions but also the execution of archetypal smart contracts. These private entities will bear the cost of this new phase while the NB will remain as a validator that ensures "everyone plays by the rules". The proposal goes at length to describe the lucrative opportunities at a global scale and respective incentives for FIs to participate. In this setup, the NB will transition to be one of the validator nodes but it will also be the single entity that performs overnight AML "housekeeping". Finally, the system could collapse back to a centralized platform in the rare case of a systemic crisis, exclusively operated by the NB under the basic operations of Phase 1.

The messaging layer in Phase 2 will be open-source, it will follow tight domestic/international standardization for interoperability, and it will continue releasing entry-level public APIs for third-parties. This setup will enable the platform's core functionality to allow commercial parties that are non-validator nodes – such as other FIs, FinTechs/PayTechs, and service providers (non-FI corporations) – to build digital commerce services but also participate in the enhanced CBDL sys-

tem. Evidently, to allow private entities offer technical services to increase and/or capture new markets, the NB will need to mandate *programmable-CBDC standardization* to allow third-parties to build network overlay fintech/data services, but also to "communicate" with other emerging foreign CBDC projects. Examples of these services include further data-protection/data-mining mechanisms, digital-authorizations and e-signatures, asset-tokenization ecosystems, low-latency system processing/markets for IoT/AI operators, account and spending management tools, perks for users to exchange private data for services, and other overlay networks to permissionless/permissioned systems and/or foreign CBDCs.

The Business Rationale of CBDLs: CBDLs are a mix of *direct* CBDCs, with Phase 2 introducing "contained" elements from *hybrid* platforms, as the BoC (NB) still retains system control and distribution of CBDLs. The authors rationalize this architecture having a "carrot and stick" approach to positively disrupt established FI payment practices, and replace them for ones that benefit the public in a new global digital economy where one needs to remain innovative and relevant [112] while protecting their citizen's data. They also argue that current (outdated) payment systems are unreasonably expensive to the public acting as revenue "cash cow" streams for the FIs. Further, by concept and by architecture, CBDLs are intended as a digital complement for *cash* and it is only proper to be advertised as a competition to current cash payments. In contrast, commercial bank main service is to provide market liquidity through credit arrangements (*e.g.*, loans, overdraft arrangements, lines of credit).

The authors urge against the use of synthetic CBDCs; they believe it does not balance the public's privacy interests, may dilute national sovereignty, and may not intrinsically promote healthy innovation in the private sector. They argue that, whatever contingency condition triggers BoC's plans, it is both necessary and sufficient to introduce CBDLs "stand alone", not to involve FIs in the distribution of Phase 1 and limit their operational jurisdiction in Phase 2 with close supervision. The reason is that FIs do not have incentives to cannibalize existing revenue streams by spearheading a new CBDC system. Following the authors' extensive analysis, there's a claim to be made that CBDLs resemble (within a geopolitical and policy regional context) the practices and implementation doctrines of the DCEP.

CBDL Legal Considerations: The CBDL report complements its techno-economic plan with an extensive set of legal recommendations. The latter are here summarized to the extent they mirror legal issues other central banks will likely face upon issuing a CBDC. At early CBDL design stages, the BOC should address the following issues:

1. The legal authority of the BoC to issue CBDLs;
2. Regulation and oversight of e-wallets and the exchange/settlement network;
3. Considerations relating to AML regulations.

The first question asks whether the BoC has explicit authority to issue digital currency under the current version of the Bank of Canada Act. Any related legal or political challenges may result in reputational damages and implementation delays,

which should be averted. The second question pertains to the appropriate regulatory body to oversee the network, including the establishment of the NB. Phase 1 presents the following two critical legal issues: *(i)* to support CBDL transactions, the model envisions the need for the BoC to issue CBDLs to the NB, or equivalently, a reserve account within the BoC, and *(ii)* the legal environment in which the NB should be subject to regulatory oversight. Phase 2 involves expanding the network to BoC/NB-licensed private service providers that are permitted to develop innovative fintech/data services by creating proxy/service-wallets that connect with the end user verified CBDL-wallets with the NB. These licenced service providers and network validators should still be brought into the regulatory framework.

Finally, the third question pertains to changes to AML requirements under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. This exploration should also include offline transactions through the quasi-token CBDL-cards that present additional issuance considerations as well as new AML concerns. The legal section of the CBDL proposal closes with additional aspects the BoC should be mindful in later stages of the design process, such as deposit insurance, consumer protection, privacy and tax implications.

6 Conclusions

Research in digital currencies and decentralization in this emerging digital world is a multi-disciplinary endeavor; technologists, regulators, economists, political scientists and sociologists, among others, need to gather together and listen to each other to properly shape the "history of things to come". Even more, research for digital currencies by central banks is an exciting field that promises to occupy headline news stories and scientific practices in this drastically changing decade for our society. Along those lines, this Chapter attempted to outline the key elements of central bank digital M0 money evolution, as mirrored by publications of leading institutions, private actors, and monetary authorities. As seen, the debate is heated and complex. Although many central banks declare they are not yet fully convinced that CBDC benefits outweigh their risks/costs, they still run PoCs and pilots as those words are typed here. From this angle, the case-studies of the PBoC's *DCEP* and Facebook's *Diem* provide topical insights to assess the imminence of this worldwide shift in monetary policy, payment system modernization and geopolitical trends.

Section 1 set off by disambiguating "central bank money", to review the difference between *wholesale* and *retail* use-cases and the drivers underpinning their interest. Section 2 addressed different perspectives on candidate architectures for *retail* CBDCs, as emerging in a vast body of literature. In this context, dimensions such as public-private interplay, offline usage, and cross-border efforts were heeded. In Section 3, the reader could follow the history of CBDC projects, starting from pioneer efforts to existing initiatives and future trends. By pursuing a more specific avenue, Section 4 outlined a set of questions pertaining to the regulatory and compliance domains – *i.e.*, monetary law considerations, AML scenarios and cash-like

anonymity, privacy and data protection concerns, privacy-transparency trade-offs. Finally, Section 5 dived into the details of three major projects, pinpointed on the grounds of their key role within the global CBDC arena.

Even if the topic is subject to major developments on a daily basis, some conclusions may already be drawn at this stage. Evidently, CBDC systems are bound not only to serve millions of users but also to exert enormous influence on many aspects of the public's life from a techno-legal and socio-economic perspective. Further, they are strongly linked to risks of collected/siloed data and relevant publicly-available monetization practices. Likewise, their impact should be foreseen with regard to their economic/social influence from a domestic and international geopolitical viewpoint. Against this backdrop, it can be argued the deployment of e-fiat money involves a vast range of considerations that go way beyond the argument of "a new way of making purchases without using physical banknotes". It remains to be seen whether and how today's major economies will leverage CBDC-related innovations to capitalize on their position. Alternatively, it is to be expected that the strength of proactive private players and certain sovereign countries "over others" will further unfold.

Acknowledgements While this Chapter is the result of joint research and editing effort carried out by both authors, Nadia Pocher is the author of Subsections 1.1, 1.2, 2.1, 2.3, 2.4, 3.2, 3.3, Section 4, and Andreas Veneris is the author of Subsections 1.3, 2.2, 3.1, 3.4., Section 5. The remainder is the result of joint drafting. 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. 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
2. A. M. Antonopoulos, *The Internet of Money - Volume Two*. Merkle Boom LLC, 2017.
3. K. Werbach, "The Siren Song: Algorithmic Governance by Blockchain," *After the Digital Tornado: Networks, Algorithms, Humanity*, 2020.
4. A. Walch, "In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains," in *The Blockchain Revolution: Legal and Policy Challenges*, 2018, pp. 1–27. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3203198
5. M. Casey, J. Crane, G. Gensler, S. Johnson, and N. Narula, "The impact of blockchain technology on finance: a catalyst for change," Tech. Rep., 2018.
6. 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.
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. P. Sandner, J. Gross, L. Grale, and P. Schulden, "The Digital Programmable Euro , Libra and CBDC : Implications for European Banks," no. July, 2020.
11. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.
12. B. Ahlgren, M. Hidell, and E.-H. Ngai, "Internet of things for smart cities: Interoperability and open data," *IEEE Internet Computing*, vol. 20, no. 6, pp. 52–56, 2016.
13. J. Manyika, M. Chui, J. Bughin, R. Dobbs, P. Bisson, and A. Marrs, *Disruptive technologies: Advances that will transform life, business, and the global economy*. McKinsey Global Institute San Francisco, CA, 2013, vol. 180.
14. N. Pocher and M. Zichichi, "Towards CBDC-based Machine-to-Machine Payments in Consumer IoT," 2021. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3974838
15. P. Rogaway, "The Moral Character of Cryptographic Work," 2016.
16. European Central Bank, "Tiered CBDC and the financial system," no. 2351, p. 42, 2020. [Online]. Available: https://www.ecb.europa.eu/
17. Bank for International Settlements, "CBDCs: an opportunity for the monetary system," Tech. Rep., jun 2021. [Online]. Available: https://www.bis.org/publ/arpdf/ar2021e3.pdf
18. L. Swartz, *New Money: How Payment Became Social Media*. Yale University Press, August 2020.
19. A. Carstens, "Digital Currencies and the Future Monetary System," *Hoover Institution policy seminar*, vol. 89, no. 1, p. 17, 2021. [Online]. Available: https://www.bis.org/speeches/sp210127.pdf
20. S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *www.bitcoin.org*, 2008.
21. V. Buterin, "Ethereum whitepaper," Ethereum Foundation, https://ethereum.org/en/whitepaper/, Tech. Rep., 2013.
22. Z. Amsden, R. Arora, S. Bano, M. Baudet, S. Blackshear, A. Bothra, and G. Cabrera, "The Libra Blockchain - White Paper," pp. 1–29, 2019. [Online]. Available: https://diem-developers-components.netlify.app/papers/the-diem-blockchain/2019-06-25.pdf
23. 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.
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. ITU-T Focus Group on Digital Currency including Digital Fiat Currencies, "Taxonomy and definition of terms for digital fiat currency," ITU-T, Tech. Rep., jun 2019. [Online]. Available: https://www.itu.int/en/ITU-T/focusgroups/dfc/Documents/DFC-O-012_Taxonomy and definition of terms for DFC.pdf
26. Bank of International Settlements, "Central bank digital currencies : foundational principles and core features," Tech. Rep. 1, 2020. [Online]. Available: www.bis.org
27. C. Brummer, *Cryptoassets: Legal, Regulatory, and Monetary Perspectives*. Oxford University Press, 2019.
28. B. Geva, "Banking in the Digital Age - Who is Afraid of Payment Disintermediation?" *EBI Working Paper Series*, no. 23, 2018.
29. W. Bossu, M. Itatani, C. Margulis, A. Rossi, H. Weenink, and A. Yoshinaga, "Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations by," Tech. Rep., nov 2020.
30. E. L. Sidorenko, S. V. Sheveleva, and A. A. Lykov, "Legal and Economic Implications of Central Bank Digital Currencies (CBDC)," in *Economic Systems in the New Era: Stable Systems in an Unstable World*. Springer International Publishing, 2021, pp. 496–502.
31. Q. Yao, "A systematic framework to understand central bank digital currency," *Science China Information Sciences*, vol. 61, no. 3, 2018.
32. CPMI-MC, "Central bank digital currencies," Tech. Rep. March, 2018.

33. Amler, Eckey, Faust, Kaiser, Sandner, and Schlosser, "DeFining the DeFi: Challenges & Pathway," Tech. Rep., 2021. [Online]. Available: https://arxiv.org/abs/2101.05589
34. A. Golubova, "BIS backs central bank digital currencies: Their time 'has come'," 2021. [Online]. Available: https://www.kitco.com/news/2021-06-23/BIS-backs-central-bank-digital-currencies-Their-time-has-come.html
35. I. Neroni Rezende and N. Pocher, "Co-Governing Emerging Socio-Technical Systems: Investigating the Implications of Public-Private Partnerships in Smart Cities and Central Bank Digital Currencies [Unpublished]."
36. E. Rennie and S. Steele, "Privacy and Emergency Payments in a Pandemic: How to Think about Privacy and a Central Bank Digital Currency," *Law, Technology and Humans*, vol. 3, no. 1, pp. 6–17, 2021.
37. 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*, pp. 1–23, November 2020. [Online]. Available: https://www.lawfareblog.com/
38. R. Auer and R. Böhme, "The technology of retail central bank digital currency," *BIS Quarterly Review*, no. March, pp. 85–100, 2020.
39. D. Kochergin and V. Dostov, "Central Banks Digital Currency: Issuing and Integration Scenarios in the Monetary and Payment System," *Lecture Notes in Business Information Processing*, vol. 394, pp. 111–119, 2020.
40. 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.
41. Group of 30, "Digital currencies and stablecoins: Risks, opportunities, and challenges ahead," 2020. [Online]. Available: https://group30.org/
42. R. Auer and R. Böhme, "Central bank digital currency: the quest for minimally invasive technology," Bank for International Settlements, Tech. Rep., jun 2021. [Online]. Available: https://www.bis.org/publ/work948.pdf
43. A. Kriwoluzky and C. H. Kim, "Public or Private? The Future of Money," Tech. Rep. December, 2019. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/IDAN/2019/642356/IPOL_IDA(2019)642356_EN.pdf
44. 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
45. X. Gang and Mount Union of Science and Technology, "Analysis of the Central Bank's Digital Currency DC/EP Dual Offline Payment Scenarios and Solutions," Tech. Rep., 2019. [Online]. Available: https://www.mpaypass.com.cn/news/201912/06094420.html
46. K. Yang, D. Blaauw, and D. Sylvester, "Hardware Designs for Security in Ultra-Low-Power IoT Systems: An Overview and Survey," *IEEE Micro*, vol. 37, pp. 72–89, 2017.
47. 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.
48. M. K. Brunnermeier and D. Niepelt, "On the equivalence of private and public money," *Journal of Monetary Economics*, vol. 106, pp. 27–41, 2019. [Online]. Available: https://doi.org/10.1016/j.jmoneco.2019.07.004
49. S. Jagati, "CBDCs With a Twist: The Public-Private Solutions Needed for Adoption," 2020. [Online]. Available: https://cointelegraph.com/news/cbdcs-with-a-twist-the-public-private-solutions-needed-for-adoption
50. T. Adrian, "Evolving to Work Better Together: Public-Private Partnerships for Digital Payments," 2020. [Online]. Available: https://www.imf.org/en/News/Articles/2020/07/22/sp072220-public-private-partnerships-for-digital-payments
51. M. Ojo, "Balancing public-private partnerships in a digital age: CBDCs , central banks and technology firms," *Munich Personal RePEc Archive*, 2021. [Online]. Available: https://mpra.ub.uni-muenchen.de/107716/
52. R. Auer, P. Haene, and H. Holden, "Multi-CBDC arrangements and the future of cross-border payments," Bank for International Settlements, Tech. Rep., mar 2021.
53. R. Auer, C. Boar, G. Cornelli, J. Frost, H. Holden, and A. Wehrli, "CBDCs beyond borders: results from a survey of central banks," Tech. Rep., jun 2021.

54. H. Jung and D. Jeong, "Blockchain Implementation Method for Interoperability between CBDCs," *Future Internet*, 2021. [Online]. Available: https://doi.org/10.3390/fi13050133
55. D. Duffie, "Interoperable Payment Systems and the Role of Central Bank Digital Currencies," *Finance and Insurance Reloaded, Institut Louis Bachelier Annual Report*, 2020.
56. Bank of Canada, "Contingency planning for a central bank digital currency," Tech. Rep., 2020. [Online]. Available: https://www.bankofcanada.ca
57. T. Khiaonarong and D. Humphrey, "Cash Use Across Countries and the Demand for Central Bank Digital Currency," Tech. Rep., mar 2019.
58. N. Pocher and A. Veneris, "Privacy and transparency in cbdcs: A regulation-by-design aml/cft scheme," *IEEE Transactions on Network and Service Management*, 2021.
59. G. Danezis and S. Meiklejohn, "Centrally banked cryptocurrencies," in *Network and Distributed System Security Symposium 2016*, 02 2016.
60. 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.
61. European Central Bank, "Report on a digital euro," European Central Bank, Tech. Rep. October, 2020. [Online]. Available: https://www.ecb.europa.eu/
62. C. Boar, H. Holden, and A. Wadsworth, "Impending arrival - a sequel to the survey on central bank digital currency," Tech. Rep. 107, jan 2020.
63. 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
64. European Central Bank, "Eurosystem report on the public consultation on a digital euro," no. April, 2021.
65. Sveriges Riksbank, "E-krona pilot Phase 1," Tech. Rep., apr 2021. [Online]. Available: https://www.riksbank.se/globalassets/media/rapporter/e-krona/2021/e-krona-pilot-phase-1.pdf
66. BIS Innovation Hub Hong Kong Centre, HKMA, Bank of Thailand, Digital Currency Institute PBoC, Central Bank UAE, "Inthanon-LionRock to mBridge: Building a multi CBDC platform for international payments," Tech. Rep., sep 2021. [Online]. Available: https://www.bis.org/publ/othp40.htm
67. PYMNTS, "BIS To Open Four New Innovation Hubs Over Next Two Years," jul 2020.
68. D. A. Zetzsche, D. W. Arner, and R. P. Buckley, "Decentralized Finance," *Journal of Financial Regulation*, vol. 6, no. 2, pp. 172–203, 2020.
69. M. Finck, *Blockchain Regulation and Governance in Europe*, 2019.
70. D. A. Zetzsche, R. P. Buckley, D. W. Arner, and J. N. Barberis, "Regulating a Revolution: From Regulatory Sandboxes to Smart Regulation," 2017.
71. 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.
72. N. Pocher, "The open legal challenges of pursuing AML/CFT accountability within privacy-enhanced IoM ecosystems," in *CEUR Workshop Proceedings*, vol. 2580, 2020.
73. 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/
74. N. Pocher, "Self-hosted Wallets: The Elephant in the Crypto Room?" 2021. [Online]. Available: https://www.law.kuleuven.be/citip/blog/self-hosted-wallets/
75. ——, "Crypto-wallets and the new EU AML package: where are the battle lines drawn?" 2021. [Online]. Available: https://www.law.kuleuven.be/citip/blog/crypto-wallets-and-the-new-eu-aml-package/
76. FATF, "Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing," Tech. Rep. September, 2020. [Online]. Available: http://www.fatf-gafi.org/
77. D. Chaum, "Blind signatures for untraceable payments," 1998.
78. 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/

79. W. Magnuson, *Blockchain Democracy: Technology, Law and the Rule of the Crowd*, 2020. [Online]. Available: https://www.cambridge.org/core/books/blockchain-democracy/1E3D5E83BC932319E38BA622026C6239
80. FINTRAC, "Canada's Legislation: The Proceeds of Crime (Money Laundering) and Terrorist Financing Act," 2019.
81. "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."
82. 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/
83. European Commission, "Anti-money laundering and countering the financing of terrorism legislative package," 2021. [Online]. Available: https://ec.europa.eu/info/publications/210720-anti-money-laundering-countering-financing-terrorism_en
84. ——, "Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing," 2021. [Online]. Available: https://ec.europa.eu/finance/docs/law/210720-proposal-aml-cft_en.pdf
85. 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.
86. I. Karasek-wojciechowicz, "Reconciliation of anti-money laundering instruments and European data protection requirements in permissionless blockchain spaces," *Journal of Cybersecurity*, pp. 1–28, 2021.
87. C. Salmensuu, "The General Data Protection Regulation and Blockchains," 2018. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143992
88. M. Berberich and M. Steiner, "Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers ? I . Technical Core Features and Use Cases of the Blockchain Technology," *European Data Protection Law Review*, vol. 2, no. 3, pp. 422–426, 2016.
89. G. Goodell and T. Aste, "Can Cryptocurrencies Preserve Privacy and Comply With Regulations?" *Frontiers in Blockchain*, vol. 2, no. 4, may 2019.
90. R. J. Garratt and M. R. van Oordt, "Privacy as a Public Good: A Case for Electronic Cash," *Bank of Canada Staff Working Paper*, no. 2019-24, 2019.
91. G. Goodell, H. D. Al-Nakib, and P. Tasca, "A Digital Currency Architecture for Privacy and Owner-Custodianship," *Future Internet*, no. 13, 2021. [Online]. Available: https://arxiv.org/abs/2101.05259
92. 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.
93. T. Sardá, S. Natale, N. Sotirakopoulos, and M. Monaghan, "Understanding online anonymity," *Media, Culture and Society*, vol. 41, no. 4, pp. 557–564, 2019.
94. 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/
95. V. Torra, *Data Privacy: Foundations, New Developments and the Big Data Challenge*, 2017, vol. 28.
96. 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.
97. A. Cavoukian, "Privacy by design," *Office of the Information and Privacy Commissioner*, 2011.
98. D. Digital, "Technology trends: How do they translate in the Chinese market?" Tech. Rep. April, 2020.
99. Citi, "Future of Money," Tech. Rep. April, 2021.

100. RT, "Digital currencies may challenge SWIFT global payment network, says Russian central bank," 2020. [Online]. Available: https://www.rt.com/business/510534-digital-currencies-swift-challenge/
101. Working Group on E-CNY People's Bank of China, "Progress of Research Development of e-CNY in China," jul 2021. [Online]. Available: http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf
102. A. Kharpal, "With Xi's backing, China looks to become a world leader in blockchain as US policy is absent," 2019. [Online]. Available: https://www.cnbc.com/2019/12/16/china-looks-to-become-blockchain-world-leader-with-xi-jinping-backing.html
103. U.S.-China Economic and Security Review Commission, "An Assessment of the CCP's Economic Ambitions, Plans, and Metrics of Success," 2021.
104. J. Ekberg and M. Ho, " A New Dawn for Digital Currency: Why China's eCNY will change the way money flows forever," Tech. Rep. April, 2021.
105. A. Veneris and A. Park, "Special Drawing Rights in a New Decentralized Century," Tech. Rep., 2019. [Online]. Available: https://arxiv.org/abs/1907.11057
106. M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, "HotStuff: BFT Consensus in the Lens of Blockchain," pp. 1–23, 2018. [Online]. Available: http://arxiv.org/abs/1803.05069
107. S. Blackshear, E. Cheng, D. L. Dill, V. Gao, B. Maurer, T. Nowacki, A. Pott, S. Qadeer, D. Russi, S. Sezer, T. Zakian, and R. Zhou, "Move: A Language With Programmable Resources," pp. 1–26, 2020. [Online]. Available: https://diem-developers-components.netlify.app/papers/diem-move-a-language-with-programmable-resources/2020-05-26.pdf
108. Diem Association, "Diem Announces Partnership with Silvergate and Strategic Shift to the United States," may 2021. [Online]. Available: https://www.diem.com/en-us/updates/diem-silvergate-partnership/
109. Ledger Insights, "Diem plans to replace USD stablecoin with gov digital dollar," may 2021.
110. Bank of Canada, "Contingency Planning for a Central Bank Digital Currency," feb 2020. [Online]. Available: https://www.bankofcanada.ca/2020/02/contingency-planning-central-bank-digital-currency
111. R. Abraham, E. S. Bennett, N. Sen, and N. B. S. S. Francis, "State of adhaar report 2016-17," ID Insight, Tech. Rep., May 2017.
112. M. Ricks, J. Crawford, and L. Menand, "Fedaccounts: Digital dollar," Vanderbilt Law, https://ssrn.com/abstract=3192162, Research Paper 18-33, UC Hastings Research Paper No. 287, 2020.