

Central bank digital currencies: policy and operational perspectives for India

Satish Babu¹  · K M Abraham²

Received: 30 April 2021 / Accepted: 23 June 2021 / Published online: 2 July 2021
© CSI Publications 2021

Abstract Cryptocurrencies are an innovation that brings together computing, networking and an incentive regime to create secure, decentralized, peer-to-peer digital currency that lends itself to be used as a medium of exchange and as storage of value. Most Central Banks have been reluctant to permit cryptocurrencies considering risks to the financial system, and have veered towards Central Bank Digital Currency or ‘Digital Fiat’ that shares several advantages of cryptocurrencies but are entirely mandated and managed by the Central Bank. This paper examines provides a background to CBDCs and discusses some of the policy and operational aspects that an Indian CBDC launch should consider.

Keywords Cryptocurrency · CBDC · Digital fiat · Digital Rupee

1 Introduction

1.1 Technology innovations of the last decade

The combination of computing, networking, communications technologies—including mobile phones—and IoT devices have transformed most domains of human

endeavour in the last two decades. Entirely new sectors have evolved, and existing sectors massively disrupted or made completely obsolete.

One of the new disciplines that have emerged in the last decade is that of cryptoeconomics—together with the related discipline of cryptofinance—which are both founded upon a technological innovation dating back to the late 2000s, cryptocurrencies. These are peer-to-peer digital currencies that are entirely based on network effects—the phenomenon whereby increased numbers of people or participants in a networked community sustains or enhances the value of the goods or services provided.

Cryptocurrencies bring together computing, networking and behavioural economics to create a currency, overcoming the challenges of security, fault tolerance, and integrity through code, and delivering the primary roles of a currency—being a store of value and a medium of exchange—in a sustainable manner. The first of these was Bitcoin, which was announced in a white paper of uncertain authorship in October 2008, and which was globally available from 2009 through an open-source codebase.

While efforts at creating an anonymous digital cash system started much earlier than 2009 [1], none of the attempts was successful enough to be operationalized. Bitcoin’s success stems from a number of factors that are discussed below.

1.2 Early developments in cryptocurrencies: bitcoin, blockchain and beyond

Bitcoin’s vision was to create a secure, safe, censorship-proof currency system that supports peer-to-peer transactions globally. Relying significantly on strong cryptography [2], Bitcoin is backed by a public, global ledger that is cryptographically secured against modification. A system

✉ Satish Babu
sbabu@ieee.org
K M Abraham
km@abrahamdigital.com

¹ Chair, APRALO, ICANN & Founder-Director, International Centre for Free and Open Source Software (ICFOSS), Govt of Kerala, Thiruvananthapuram, India

² Former Chief Secretary to Govt. of Kerala & Former Whole Time Member, Securities and Exchange Board of India (SEBI), Thiruvananthapuram, India

of financial incentives attracts “miners” whose investment in computing hardware and energy is offset by revenues from newly-minted bitcoins as well as transaction fees. Notably, the more the number of miners—and higher competition between them—the safer the currency becomes against attempts to take over the currency. The mining process—where miners compete against each other to solve a hashing problem by brute force—lets the winning miner create new blocks in the ledger consisting of pending transactions. The winning miner is rewarded with a fixed number of new bitcoins (that halves every four years) as well as the transaction fees from the transactions in the block. A new block is produced by the bitcoin network approximately every 10 minutes. The entire network is connected through a robust and fault-tolerant protocol, where it is impossible for any single miner or group of miners to control the network except if they own over 50% of the total computing power of the network. Bitcoin has an embedded scripting language that is limited in power on account of security reasons and is a step towards “programmable money” but smart contracts are not possible on the system by default.

A significant innovation by the Bitcoin ecosystem has been its digital ledger, the Blockchain, which has found utility in many areas outside cryptocurrency as well, ranging from banking to supply chain management to digital attestation ledgers.

Given the fact that the total number of bitcoin is fixed at about 21 million (of which about 18.7 million have already been mined as of Apr 2021), the value of the coin is deflationary, and is expected to steadily rise (also because numerous careless users have lost their private keys without which their coins are lost forever). The current (Apr 2021) exchange rate of bitcoin is approximately US\$ 58,000, in comparison to US\$ 0.39 in 2010.

The early success of bitcoin unleashed several waves of innovation in cryptocurrencies many of which are flourishing today, coexisting with bitcoin. Some of these have improved different aspects of Bitcoin such as programmability, scalability, environmental footprint or anonymity. The largest of these is Ethereum, which operates as a Turing-complete global platform that makes it possible to implement Smart Contracts in a sustainable manner.

1.3 Recent innovations in cryptocurrencies

The emergence of numerous new cryptocurrency platforms that are programmable, secure and flexible has led to several innovations in the second half of the last decade. The following is a limited list of innovations that are relevant to the topic of this paper.

1. *Tokenization* The programmability of cryptocurrencies makes it possible to use the platform not just to transfer or hold funds, but also to create new, user-specific cryptocurrencies—usually known as tokens. A token may refer to the currency or more generally, a stand-in for any kind of asset, digital or real-life. Tokenization—which still has several challenges to be fully operationalized for real-life assets—has enormous potential in asset management, making it possible to buy, sell or transfer digital or real-life assets fully or fractionally, thus disrupting a large number of markets from financial services to commodities, apartments, vehicles, real estate of objects of art.
2. *Stablecoins* Stablecoins address a very important issue with cryptocurrencies in general: price fluctuation. Although a section of the market—especially those who are using cryptocurrency as a store of value or investment—would like price appreciation, there are several difficulties in a cryptocurrency that is excessively volatile. Stablecoins are cryptocurrencies that are pegged to a particular fiat currency and retain the value even if the fiat currency fluctuates in value. This requires significant financial buffering with cash reserves. However, stablecoins remove the risk of currency volatility.
3. *Decentralized Finance (DeFi)* DeFi is a decentralized, disintermediated form of cryptocurrency-based finance that uses automated Smart Contracts to manage the lending/recovery/liquidation process. DeFi completely does away with traditional intermediaries such as banks or brokerages, and provides relatively high returns, sometimes with a degree of risk. DeFi emerged in 2020, with MakerDAO allowing users to borrow Dai, their USD-tied stablecoin. The total volume of funds in DeFi rose to US\$ 50 billion in Apr 2021 [6].
4. *Non-fungible tokens* Most tokens are fungible or divisible, which means they can be subdivided fractionally. Non-Fungible Tokens (NFT) are a type of token that is one-of-a-kind, indivisible and unique. NFTs are increasingly used in different contexts where the holder gets a unique attribute such as the ownership (full or fractional) of a digital or real-life asset, a work of art or a collectible. The NFT life-cycle is controlled by Smart Contracts which allows various operations such as selling or transfer of the original asset on the crypto platform. While NFTs have been around for several years (the Cryptokitties fad a few years ago was based on NFTs), they have seen rapid adoption in early 2021, with a painting of the digital artiste Beeple auctioning for US\$ 69.3 million [7].
5. *The diem project* Originally called Libra, Diem was a project conceived by Facebook in 2019 and supported by a consortium now known as the Diem Association.

Diem was to be a permissioned digital payments system that would be privately managed by the consortium, and working towards financial inclusion for the global unbanked population that numbers about 31% of the population. The main vehicle of delivery would be the Facebook family of products (such as the Facebook, Instagram, and WhatsApp apps) which already have large user base (Facebook itself claims to have over 2.7 billion active users [8]). When Diem gets launched the apps used by users of these products will be instantly enabled for digital transfers of Diem Coins, backed by the Diem Blockchain. The Diem coin would be a stablecoin tied to a basket of currencies, but since the project has still not been launched, it is unclear if it would effectively be a set of stablecoins, each tied to a particular currency (such as Diem USD, Diem GBP or Diem INR), or just a single token. The Diem project has been delayed due to significant regulatory scrutiny in several parts of the world, which is to be expected given the sweeping global reach of the project and its potential ability to undermine sovereign monetary policy of different countries. In particular, the Diem project has caused alarm at different Central Banks (See Section 3 “Cryptocurrencies and Central Bank Policy” below) leading them to consider an accelerated adoption of Central Bank Digital Currencies (CBDCs).

2 Cryptocurrencies: benefits and risks

Cryptocurrencies constitute a significant innovation in currency. However, there is considerable variation in how these advantages manifest themselves for different cryptocurrency platforms. Cryptocurrencies also have disadvantages are risks, also variable across platforms. The lists below are indicative of the general nature of cryptocurrencies.

2.1 Advantages

1. *Anonymity* Cryptocurrencies provide weak or strong anonymity for parties depending on the platform. Bitcoin uses pseudo-anonymization that has been breached in the past using a combination of on-chain and off-chain analytical techniques. Other platforms such as Monero, Zcash or Dash provide much stronger anonymity.
2. *Privacy* Overall, anonymity is helpful for maintaining user privacy although transactions are publicly recorded on the blockchain.

3. *Censorship resistance* Since cryptocurrencies are built on a peer-to-peer model without a central controlling agency, it is impossible for Governments to freeze cryptocurrency in a way similar to freezing a bank account.
4. *Disintermediation of intermediaries* Given its peer-to-peer nature, cryptocurrency platforms connect each party directly to the counterparty. There are no intermediaries and consequently no loss of information, fees or consumption of time.
5. *Convenience and ease of use* Cryptocurrencies are easy to use and often is used from mobile- or PC-based wallets. Any amount of money can be stored in a wallet, and any amount can be transferred directly to any other user whose address is known. Money can be received in new addresses (in fact, some people receive every payment in a new address for security reasons). Overall, the ease of use is considerable.
6. *Low transaction costs* Each transaction has a fee, but this is often very much lower than what banks charge on funds transfer. On bitcoin, fees for a single transaction can be as low as US\$ 0.15. However, transaction fees may vary with the number of pending transactions and is not generally dependent on the quantum of funds being transferred (In Dec 2017, Bitcoin touched a record transaction fee of US\$ 37, on account of large number of new users joining the network)
7. *High Speed of transfer* Most bitcoin transactions take an hour to get the minimum number of confirmations by which the network “approves” the transaction. Ethereum takes about 5 minutes. However, settlement uncertainty may be a factor for proof-of-work consensus models (See “Settlement Finality” in Sect. 2.2 for more details.)
8. *Programmability and smart contracts* Cryptocurrencies, especially Ethereum and later, provide a Turing-complete implementations that permit programming of smart contracts. This programmability permits flexible use of the platform for numerous new applications that involve transfer, purchase or sale of any kind.
9. *Low barriers to entry* Anyone can start using a crypto and no permission from any entity or KYC is required.
10. *Availability of credit* Ownership of existing cryptocurrency enables the generation of credit, as discuss above in DeFi.
11. *Irreversibility of transactions* All cryptocurrency transactions are irreversible. While this means a transfer done by mistake cannot be rectified, it also

means that several dubious practices that make use of reversal cannot also take place.

12. *Currency policy decided by community* The policy trajectory of a particular platform is decided in a bottom-up manner by the community of that platform, and not by Governments.
13. *A single global currency* Since cryptocurrencies are global, international travel or trade does not involve converting between currencies. Similarly, transfers also do not distinguish between national boundaries.
14. *Security* All Distributed Ledger Technologies (DLTs) use cryptography to render their historic transactions immutable. It is generally considered infeasible to breach this using existing technologies.

2.2 Disadvantages

1. *Environmental costs* Most of the proof-of-work cryptocurrency platforms (such as bitcoin) use an enormous amount of power around the world for hashing. When exchange rates rise, it attracts new investments which further push up the power consumption. The environmental impact of such promiscuous consumption of electricity is often invisible, but needs to be factored in. New consensus models such as proof-of-stake or proof-of-authority would be much more sustainable.
2. *Need for security* Since there are no intermediaries, each user has to safeguard their bitcoin (which effectively means their cryptographic private keys, since the actual "coin" is on the blockchain). There have been numerous cases where individuals have lost their cryptocurrency by accident (hard disk crashes) or by intruders who break into their computers. Users can choose to store their currency in exchanges, but even exchanges have lost money accidentally or by malicious intent.
3. *Fluctuation in value* Unless it is a stablecoin, the exchange value of a cryptocurrency tends to fluctuate, leading to considerable stress for its users. While long-term investors ("Hodlers" [9]¹) depend on the deflationary nature of their cryptocurrency to make long-term gains, it's the regular users who use currency for e-commerce that are impacted by the day-to-day fluctuations.
4. *Poor scalability* As of now, the scalability of most cryptocurrency platforms, in terms of transaction volume per second, is much lower than traditional systems such as credit cards. As more users join the platform, transactions take longer (and may also involve a higher fees). There have been several efforts to enhance capacities with technologies such as *sharding* and *side-chains*. Bitcoin's Lightning Network plans to raise the transaction rate to several hundred thousands each second.
5. *Lack of settlement finality* In the case of proof-of-work consensus models, there is the probability that two independent miners located in different parts of the network solve the hashing problem simultaneously. This leads to a temporary division in the network that is usually resolved by the "longest chain" policy, whereby transactions on the shorter chain are rolled back. In principle, there is an extremely low probability that an actor armed with sufficient hashing power can carry out a brute force attack, causing the rollback of all confirmed transactions. In practice, such platforms depend on a pragmatic interpretation of settlement rather than that of absolute finality used in traditional banking. However, doing so violates the Principle 8 of "Principles for financial market infrastructures" of the Bank of International Settlements (BIS) which recommends real-time or intra-day settlement finality [10].
6. *Enabler of money laundering and illegal trade* There is significant concern that cryptocurrencies could be used for money laundering, terrorism and illegal trade (such as drugs, arms, or counterfeit fiat currency). This is potentially true, and consequently most countries have put in place KYC mechanisms with cryptocurrency exchanges, whereby they are intimidated each time a user converts funds from or to a national fiat currency. This means that Central Banks are unaware of bitcoin-to-bitcoin transactions, but they would be aware of bitcoin-to-fiat conversions. A new form of conversion is peer-to-peer where individuals buy and sell directly without an exchange as intermediary, in which case Central Banks may not be notified.
7. *Dependence on exchanges* Many users prefer to use Cryptocurrency Exchanges to buy, sell, swap and hold cryptocurrency. Historically several exchanges have folded up (eg., MtGox, Bitfinex) leading to thousands of users losing money. The problem is partly on account of the absence of national legislation over cryptocurrency exchanges.
8. *Poor public awareness* Most members of the public are unaware of the true nature of cryptocurrency, and in the past, have fallen for scams and Ponzi schemes that sound like cryptocurrency but are completely unrelated (for example, the OneCoin scam [3] that cheated users around the world to the tune of US\$ 4 billion, which had little to do with cryptocurrencies beyond the name).

¹ The term "Hodl" is an accidental mis-spelling of 'hold' (referring to holding the coin rather than selling) made during the early days of cryptocurrencies.

9. *Threat to sovereign fiat currency* Cryptocurrencies operate under the radar of national Central Bank policies, and have the potential—if the scale of use is significant—to subvert the sovereign monetary policy of a country, especially if it is a smaller economy.

3 Cryptocurrencies and central bank policy

Different countries have adopted different policies *vis-à-vis* cryptocurrencies: many developed countries have allowed them to coexist with fiat currency, while others—including India—have policies that discourage or outright ban them. A senior official of the Bank of International Settlements has been quoted saying that Cryptocurrencies should face more regulation. [4] The Singapore Central Bank has pointed out that Cryptocurrencies are “Certainly Not Suitable for Retail Investors” [5]. Turkey has recently sought to ban cryptocurrency as a form of payment citing the high risk of non-recoverable losses due to the anonymous nature of the instrument [11].

The first Government in the world to support cryptocurrency through legislation is El Salvador, where the Congress voted in favour of a law permitting the use of Bitcoin as legal tender in Jun 2021 [28]. It is to be noted that El Salvador receives as much as 20% of its GDP through cross-border remittances, and the move may benefit many citizens who are recipients of such remittances.

In the case of India, the Central Bank has been hinting at very restrictive policy measures relating to cryptocurrencies, including a possible ban on mining, trading, dealing or even holding cryptocurrency assets [12]. If such a law is approved, it would make India the first major world power to declare cryptocurrency as illegal, as even China, which has banned mining and trading, has not made possession of cryptocurrency illegal. Further, it will also result in shutting out the country from one of the most innovative high-tech sectors in the world, and reduce competitiveness of the Indian IT services sector that is one of the largest provider of software services in the world. While the risks—especially to the general public—are clear, and must be mitigated, such a policy is thought to be overly restrictive, and there is a need for a more progressive policy [13].

The subtext to India’s position on cryptocurrency refers to Central Bank Digital Currencies (CBDCs) as the possible way ahead [14]. CBDCs share many of the advantages of cryptocurrencies, but is fiat currency that’s mandated and managed by the respective Central Bank. However, CBDCs and cryptocurrencies are not necessarily mutually exclusive, and can coexist provided the necessary policy safeguards are put in place². In this context, it is also interesting note that the co-founder of Ethereum, Vitalik

Buterin, has made a donation of over USD 600,000 in Eth and MKR tokens to support India’s COVID-19 response, perhaps subtly highlighting the need for more accommodating policies towards cryptocurrencies [25].

4 Central bank digital currencies (CBDCs)

One of the significant responses to the emerging popularity of cryptocurrencies, as well as private currency initiatives such as Diem (), from the side of Central Banks has been Central Bank Digital Currencies. The Bank of International Settlements (BIS) has defined it thus: “A CBDC is a digital payment instrument, denominated in the national unit of account, that is a direct liability of the central bank.” [15]³.

4.1 Vision, principles and advantages

While CBDCs share several features with cryptocurrencies, they are very different in their vision, implementation and intended use. We examine below some of the distinctive features of CBDCs when approached from the side of cryptocurrencies (as opposed to from the side of traditional Central Bank functions).

1. *Continued access to Central Bank funds* The COVID-19 global pandemic has highlighted the need and importance of digital payment mechanisms. A CBDC provides fiat currency in a digital form, which could be important for the future.
2. *Fine-grained control* CBDCs provide Central Banks with fine-grained control over the CBDC life-cycle including supply, movement, and holding patterns. It may also make it easy to compute and collect taxes and ensure compliance to Anti-Money Laundering (AML) and other regulations (See Section 4.3 on for privacy implications of personal information used for AML-related purposes).
3. *Enhanced payment diversity and operational resilience* CBDCs would enhance the diversity of payment mechanisms in a country, and make the currency system more resilient, at the same time making it more efficient and reducing costs associated with paper currency.

² On 14 Apr 2021, Coinbase became the first cryptocurrency exchange platform to be listed on Nasdaq, providing significant regulatory legitimacy not just for Coinbase, but for cryptocurrency as a whole. This may have some impact on India’s future policy directions as well.

³ *Synthetic CBDC*, where a Central Bank authorizes payment service providers to issue digital currency (backed by deposits), is not a claim on the Central Bank and hence not considered as CBDC although they would share some features of genuine CBDCs.

4. *Controlling explosive growth of cash* As economies grow, a purely cash-based approach leads to significant growth in cash, which has multiple problems associated with it. CBDCs provide a payment instrument that is relatively low-cost, and can scale quickly.
5. *Enhanced financial inclusion* CBDCs can be easily used, stored, and transferred using mobile phone wallets without the need to travel to a bank or an ATM, making financial inclusion possible even for remote communities.
6. *Direct fiscal transfer enabled* During the global pandemic, several Governments had made direct transfers of funds to personal accounts, but doing this by the traditional paper route would be an enormous challenge in terms of logistics, time and costs. CBDCs would enable this quickly and without error.
7. *Supporting user privacy* As digital cash, CBDCs would enable privacy for users. However, it is also possible to enhance surveillance on citizens depending on the implementation and intent.
8. *Enabling cross-border payments* CBDCs can be made interoperable between countries, enabling quick and automatic settlement of cross-border payments.
9. *Programmability as a Foundation for Innovation* CBDCs are a kind of programmable money and just as innovations such as DeFi are built on programmability, CBDCs will also be able to provide similar innovations. CBDCs therefore have the potential to significantly disrupt not only payment tech but also financial services, and asset management services.

4.2 Taxonomy of CBDCs

CBDCs are divided into multiple categories depending on the factors being considered.

Based on their type of use, CBDCs are often divided into *Wholesale*, where the CBDC is used for inter-bank transactions, and *Retail*, where it is used by end-users. Retail CBDCs are further divided into Direct (where the CB directly runs CBDCs without intermediaries), Indirect (where the CB only received data from commercial Banks that operate the CBDCs), or Hybrid. In the Hybrid case, commercial banks or payment operators run the same of competing CBDC implementations, where the CB may own the back-end ledger updated in real-time or in the batch mode [20].

Based on their back-end implementation, CBDCs are classified as Token-based and Account-based. Token based CBDCs are represented internally as digital token, very similar to cryptocurrency implementations. Token-based implementations make it easier to provide privacy and anonymity of users. Account-based implementations rely

on a central ledger which is implemented directly or indirectly by the Central Bank, wherein the Central Bank is aware of the current balances and transfers, and may permit surveillance of user activity.

The Money Flower (Fig. 1) [16] illustrates several key aspects of fiat currency, CBDCs and cryptocurrencies, including the issuer (Central Bank or intermediaries), Form (Digital or legacy fiat), accessibility (widespread use or specialized use), and technology (token-based or account-based). In the illustration, Private Digital Tokens represent cryptocurrencies.

Based on the technology used, CBDCs may be Digital Ledger Technology (DLT)-based or RDBMS-based. DLT or Blockchain-based technology is not an absolute requirement, but offers a rigorous and provably-secure implementation, but may suffer from a lack of scalability. For large countries, using mature DLTs that can scale may pose a challenge. While RDBMSes can address the scalability issue, there is no implementation that is as “trustless” as that of cryptocurrency⁴.

4.3 Challenges and risks

CBDCs come with their own challenges that may relate to monetary policy, technology, usability and security.

1. *Financial stability risks* The main concern that is often quoted in the context of CBDCs as a claim on the Central Bank is that this feature makes CBDCs a safer store of value than bank deposits which are not guaranteed. Potentially, this could cause a run on banks. The risk is further elevated if CBDC wallets are interest-bearing. It has been argued that this risk can be offset by the CB re-lending CBDCs to banks and also by carefully adjusting the interest rates (which can be positive, zero or even negative). However, three major central banks, Bank of Japan, Bank of Korea and the Reserve Bank of Australia, appear to have delayed their CBDC roll-out plan based on this risk [18]. It has been pointed out that a tiered-approach to interest, with low-to-zero interest rate for user-held CBDCs, together with a penal (negative) interest beyond a quantity cap may address this problem adequately.
2. *Technology and usability risks* CBDCs are a very demanding use of technology, especially for larger economies. The need to be available 24x7 and capable of many million transactions each day in a secure and

⁴ *Trustless* in the cryptocurrency jargon means not having to depend on a trusted source such as the Government or another authority. Historically, the problem has been that many of the so-called trusted entities have betrayed the trust of its users. Cryptocurrencies address this problem through cryptography and the blockchain, so that users are not required to blindly trust any agency or intermediary.

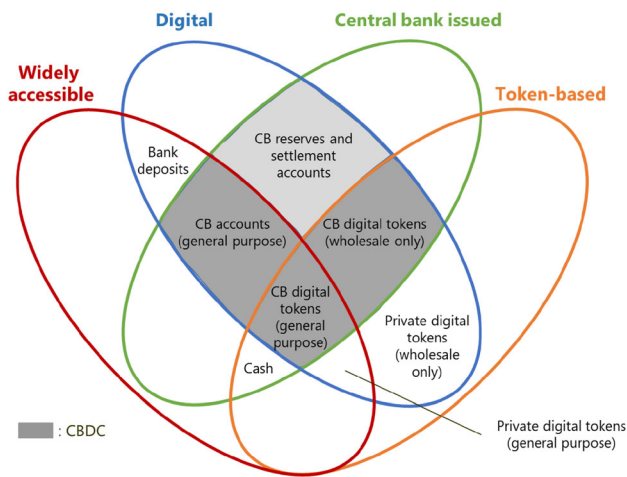


Fig. 1 The Money Flower: The taxonomy of money [16]

responsive manner is a challenge although not impossible. For a country like India, there would also be a need to ensure that the system works even without the Internet (at least for short periods), and the system has to be usable by even less educated citizens. These risks could be mitigated by a phased launch with a multiple pilots.

3. *Cybersecurity risks* Cybersecurity is a significant concern, especially when there are large numbers of users who are new techno-literates.
4. *Privacy and surveillance risks* The anonymity that we are used to with cash may be adversely impacted with CBDCs depending on the kind of implementation. Privacy and data protection must be considered as an important factor at the time of design of the CBDC. However, personal information may be required for AML purposes and this could de-anonymize CBDCs. This could be avoided by a cap above which AML/KYC information would be mandatory, which upholds privacy for retail users⁵.
5. *Regulatory risks* Some Central Banks may require new laws in order to be able to issue CBDCs. Additional legislation as well as amendments to existing legislation may be required in India in order to ensure that CBDCs are able to function fully well as legal tender.
6. *Identity management* Identity management is an important aspect of a CBDC implementation that has ramifications on security, data privacy, confidentiality of information and usability of CBDCs. While multiple models exist for Identity Management it must be noted that it is a specialized service that will be used in multiple purposes beyond CBDCs. Given that India already has a

⁵ The E-CNY CBDC project of China uses the concepts of *Controlled Anonymity* and *Data Islands* to separate identity data from transaction data, as explained in Section 5.

technologically robust identity service in place, the logical step would be to extend it to a Digital Self-Sovereign Identity (SSI) model that is multi-purpose, with CBDCs being one of the areas where it is used.

4.4 Implementation options

This paper does not examine the technology options for CBDCs in detail, as RBI has not made any announcements on the possible technology directions for India's CBDC. The subject is dealt with in other published work [27].

It must be stated clearly that it is not easy to move from a cryptocurrency implementation (whether blockchain platforms such as Ethereum or those based on high-throughput technologies such as Hashgraph) to a CBDC on account of several unique challenges.

To begin with, CBDCs are a sovereign function, and Central Banks may not want to work with an existing platform whose governance is vested with a separate group or community, even if the underlying technology is 'trustless'. On the other hand, running an in-house instance within a Central Bank goes against the philosophical and pragmatic approaches of most decentralized cryptocurrencies.

Secondly, Central Banks require fine-grain control over digital fiat currency including—but not limited to—wallet or transactions caps, negative interest rates, and expiry dates. These will be hard to retrofit on any cryptocurrency.

Thirdly, users are not expected pay transaction fees for CBDC-based transactions. For cryptocurrencies, transaction fees are an important revenue stream without which the cryptocurrency may be infeasible.

Finally, CBDCs are expected work even without the Internet for short periods subject to transaction caps, which would be useful in case of network disruption, for instance after a natural disaster.

In summary, implementation options for CBDCs must accommodate these special requirements so that Central Banks are able to ensure the stability of their financial systems and also enable financial inclusion through useful features.

5 CBDCs: the current status

Different countries are in different stages of design, launch or piloting phases of their digital fiat currencies [21]. These include China, which is perhaps the most advanced in terms of its progress to a full-scale implementation of the E-CYN system (previously called the Digital Currency Electronic Payment system or DC/EP) launched by the People's Bank of China (PBOC), also called the Digital

Yuan. After initial trials in Beijing and Chengdu, it is presently being piloted in Shanghai, Changsha, Qingdao, Xi'an, and Dalian [22]

E-CYN is a two-tier system, with the PBOC as the primary tier responsible for issuing and settlement of the CBDC, and a secondary tier that consists of existing commercial banks and payment processors (such as Alipay and WeChat Pay) who are responsible for distributing it to individual users⁶. E-CYN uses an arrangement known as *controlled anonymity* to balance privacy with AML/KYC reporting requirements. While the system has not been described in detail, preliminary indications are that the KYC/AML information provided on a one-time basis resides in a separate 'data island' of its own with the identify provider, while routine transaction data resides in separate data islands with the second tier organizations. [19].

Other countries which have announced CBDCs include Sweden (e-Krona), Turkey, Bahamas/East Caribbean Central Bank (Sand Dollar) and Iran. In some cases such as Turkey and Iran, the motivation for creating CBDC platforms is reportedly to lessen the dependence on a US Dollar-based global economy and to avoid sanctions.

6 CBDCs: the Indian scenario

The Reserve Bank of India (RBI) has consistently argued against "private digital currencies" (ie., cryptocurrencies), stating that "...currency issuance is a sovereign function and it has to be done by the sovereign" [23]. It is as yet unclear whether the forthcoming law on digital currencies will completely ban all cryptocurrency operations (including holding cryptocurrency, which is likely to seriously impact many individuals).

On the subject of CBDCs, the RBI has stated at various times that it is open to them, but has not declared a clear plan. In one of the statements made recently, the RBI Governor pointed out that "...As and when the technology evolves with adequate safeguards, I think it is an area where the Reserve Bank will certainly look at seriously at an appropriate time" [23].

7 Policy and operational considerations

While it is far from clear as to when India is likely to launch a CBDC, there can still be recommendations on policy and operational aspects that could be considered in the process of the design of the Digital Rupee. We list below some of them.

⁶ In the introductory phase, lotteries have been used to 'air drop' the Digital Yuan to end-customers.

7.1 Policy considerations

CBDCs have the potential to be a breakthrough technology that could significantly alter the current scenario for the better. We examine the most important policy considerations that should be examined during the implementation of the Digital Rupee.

1. *Financial inclusion* CBDC is a powerful tool for enabling financial inclusion. India's CBDC implementation must enable financial inclusion for the millions of India's unbanked. In particular, the design of the Digital Rupee should ensure that it is usable by all sections in society, in their own devices, in their own locations and in their own languages and not just by the technology-literate elites. In particular, an existing bank account should not be a pre-requisite to hold and use the Digital Rupee.
2. *Privacy* Privacy and protection of user data must be ensured. Given the fact that the Government has relatively low accountability *vis-à-vis* user data in the 2019 PDP Bill, extra care must be taken to ensure that personal data remains protected.
3. *Co-existence with cash and the existing ecosystem* CBDCs need to be eased in into the economy in a calibrated and phased manner, ensuring that it coexists with cash and does not result in any kind of destabilization. This may require geography-bound pilots and progressive roll-outs.
4. *Structural options: Central Bank vs Public-private partnerships* It would be useful to involve the private sector—even multiple competing entities—also in the implementation of India's CBDC, so that the system remains resilient and not dependent on a small number of points of failure.
5. *Encouraging innovation* The CBDC roll-out should provide space for start-ups and innovators (perhaps through the mechanism of RBI's regulatory sandbox) to explore innovations that could be built over CBDCs.
6. *Taking a longer-term view* Given that CBDC is "programmable money", it should be viewed as a first of a series of FinTech innovations that will, over the next several decades, completely transform India's economy, removing friction and enabling smart contracts and other innovations discussed earlier in this paper.

7.2 Operational considerations

1. *Resilience to network interruptions* India's CBDC should be resilient against network interruptions guided by the principle of 'graceful degradation'. This would mean that, for instance if the Internet

connectivity is disrupted, transactions can still take place, but perhaps with a maximum cap in place. This will ensure that the currency works in adverse environments, at least for a minimum duration.

2. *Security* Given that a large section of the CBDC users in India would be technology neo-literates, the system must be resilient against inadvertent incidents or deliberate attack.
3. *Freedom of Technology choice* The implementation should provide vendor- and platform-neutrality, leaving the users to make their own choice of technology (for instance SmartPhones and Feature phones). Where possible, the implementation must be open sourced (as is the COVID-19 tracking application, Aarogya Setu).
4. *Ease of use* The entire system should be reasonably easy to use. Users should be able to convert from the CASA (Current-account-Savings-account) funds seamlessly into Digital Rupees and back, without minimal friction (ie., without fees), transfer funds to peers even with impaired network access, and with insurance against cyber attacks or other financial losses. In addition, it is also expected that transaction will not incur fees (just like paper or coin money), and that holding/transaction caps—where they apply—should be appropriate to their tier (assuming multi-tiered wallet accounts such as personal accounts and business accounts).

8 Conclusions

There has been a considerable amount of innovation taking place in the domain of cryptocurrencies in the last decade. Some of these innovations have seen frenetic paces of development, with useful ways of generating income from cryptocurrencies, be it yield farming or NFTs. The Diem project from the consortium led by Facebook, although still undergoing regulatory scrutiny, has highlighted the significant potential of a private digital currency.

Central Banks have adopted mixed positions to these developments in cryptocurrency, with most developed countries either tolerating cryptocurrencies or providing legitimacy through regulatory oversight and taxation. Some Central Banks have decided upon partial or total restrictions on cryptocurrency. Prompted partly by the developments in the cryptocurrency space, Central Banks have been increasingly positive towards CBDCs in the last few years.

The COVID-19 pandemic has highlighted the need to explore new digital payment systems and to enhance the diversity and resilience of national payment systems. For a vast country like India, a technology such as CBDCs would

further enhance the resilience of its payment system, as demonstrated by several other large and small countries around the world.

CBDCs offer several advantages coupled with some risks. In general, there is guarded optimism from Central Banks—known to be a conservative community for good reason—about CBDCs after balancing the pros and cons. According to a recent survey by BIS [26], 86% of Central Banks are “actively engaging in some form of CBDC work”. About 60% of Central Banks (up from 42% in 2019) are currently conducting proof-of-concepts or similar experiments.

While the global picture is clear, the situation in India is less certain. On the one hand, RBI appears to favour CBDCs *vis-à-vis* cryptocurrencies, but on the other, it has been unwilling to share its roll-out plans so far.

Given that CBDCs would be one of the foundational technologies for a fully digital economy of the future, it is important that we put in place a robust process for achieving the Digital Rupee, given that other nations both bigger than India and smaller have successfully demonstrated. While doing so, we must ensure that the technology is appropriate for India, in terms of our population, economy, technology infrastructure, innovators & startups, and culture. If a well-designed CBDC can be implemented, it would provide abundant possibilities for further innovations towards the vision of Digital India.

References

1. Chaum D, Fiat A, Naor M (1990) Untraceable electronic cash. In: Goldwasser S. (eds) *Advances in cryptology - CRYPTO' 88*. CRYPTO 1988. Lecture notes in computer science, vol 403. Springer, New York, NY. <https://doi.org/10.1007/0-387-34799-2-25>
2. Wikipedia Contributors (2021) Strong Cryptography, https://en.wikipedia.org/w/index.php?title=Strong_cryptography&oldid=1010681671. Accessed 8 April 2021
3. Wikipedia contributors. (2021) OneCoin, <https://en.wikipedia.org/w/index.php?title=OneCoin&oldid=1017723184>. Accessed 22 April 2021
4. Browne R (2021) CNBC, Crypto is a 'speculative vehicle' and should be regulated, says boss of central bank group BIS, <https://www.cnbc.com/2021/03/24/cryptocurrencies-should-be-regulated-says-boss-of-central-bank-group.html> (Published 24 Mar 2021, Retrieved 8 Apr 2021)
5. Crawley J (2021) Finance Yahoo , Singapore's Central Bank Warns Crypto 'Certainly Not Suitable for Retail Investors', <https://finance.yahoo.com/news/singapore-central-bank-warns-crypto-114145189.html> (Published 6 Apr 2021, Retrieved 8 Apr 2021)
6. Spilotro T (2021) NEWSBTC (2021) DeFi Reaches Milestone \$50B Total Value Locked, <https://www.newsbtc.com/news/defi/defi-reaches-milestone-50b-total-value-locked/>. Accessed 09 April 2021

7. Goodwin J (2021) CNN Business, What is an NFT? Non-fungible tokens explained, <https://edition.cnn.com/2021/03/17/business/what-is-nft-meaning-fe-series/index.html>, (Published March 17, 2021, Retrieved 9 April 2021)
8. Statista (2021) Most popular social networks worldwide as of January 2021, ranked by number of active users, <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users>, (Retrieved 9 April 2021)
9. Investopedia (2021) HODL, <https://www.investopedia.com/terms/h/hodl.asp>, (Retrieved 9 April 2021)
10. BIS (2021) Principles for financial market infrastructures available, <https://www.bis.org/cpmi/publ/d101a.pdf>. Accessed 8 April 2021
11. Ozsoy T, Bloomberg (2021) Turkey bans cryptocurrency payments, says risks are too big, <https://www.bloomberg.com/news/articles/2021-04-16/turkey-bans-cryptocurrency-payments-saying-risks-are-too-great>. Accessed 19 Apr 2021
12. CNBC (2021) India to reportedly propose cryptocurrency ban, penalizing miners and traders, <https://www.cnbc.com/2021/03/15/india-plans-cryptocurrency-ban-will-penalize-miners-and-traders.html>. Accessed 19 April 2021
13. Babu S (2021) Towards a progressive cryptocurrency policy for India, SFLC.in, <https://sflc.in/towards-progressive-cryptocurrency-policy-india>, (Published June 2019, Retrieved 19 Apr 2021)
14. Tiwari A, BTC Manager (2021) India: new bill seeks to introduce CBDC, Ban ‘Private’ Cryptocurrencies
15. Bank Of Canada, BIS (2021) Central bank digital currencies: foundational principles and core features, <https://www.bis.org/publ/othp33.pdf>, ISBN: 978-92-9259-427-5 (Published Dec 2020, Retrieved 19 Apr 2021)
16. Committee on Payments and Market Infrastructures, BIS (2021) Central bank digital currencies, <https://www.bis.org/cpmi/publ/d174.pdf>, ISBN 978-92-9259-143-4 (Published March 2018, Retrieved 21 Apr 2021)
17. Schilling L, Fernández-Villaverde J, Uhlig H (2021) Becker-Friedman Institute, Central Bank Digital Currency: when price and bank stability collide, <https://bf.uchicago.edu/insight/finding/central-bank-digital-currency-when-price-and-bank-stability-collide/>, (Published Dec 2020, Retrieved 21 Apr 2021)
18. Bharathan V, Forbes (2021) What made central banks rethink their CBDC strategy: evidence from Bank Of Korea, Bank Of Japan And Reserve Bank Of Australia, <https://www.forbes.com/sites/vipinbharathan/2020/11/30/what-made-central-banks-rethink-their-cbdc-strategy-evidence-from-bank-of-korea-bank-of-japan-and-reserve-bank-of-australia/?sh=67fc3e5b15cc>, (Published Nov 2020, Retrieved 21 Apr 2021)
19. Jiang J, Lucero K, SSRN, background and implications of China’s Central Bank Digital Currency: E-CNY, <https://ssrn.com/abstract=3774479> or <http://dx.doi.org/10.2139/ssrn.3774479>
20. Auer R , Böhme R (2021) VOX EU, CBDC architectures, the financial system, and the central bank of the future, <https://voxeu.org/article/cbdc-architectures-financial-system-and-central-bank-future>, (Published Oct 2020, Retrieved 21 Apr 2021)
21. CBDC Insider (2021) List of Countries Leading CBDC Adoption in 2021, <https://www.cbdcinsider.com/2021/01/12/list-of-countries-leading-cbdc-adoption-in-2021/>, (Published Jan 2021, Retrieved 21 Apr 2021)
22. BeInCrypto Staff, Yahoo Finance, China’s CBDC Trial Expands to Hainan Province, <https://finance.yahoo.com/news/china-cbdc-trial-expands-hainan-153128541.html>, (Published 8 Apr 2021, Retrieved 21 Apr 2021)
23. Helms Kelvin, Bitcoin.com, RBI Governor Discusses Crypto and Central Bank Digital Currency , <https://news.bitcoin.com/rbi-governor-discusses-crypto-and-central-bank-digital-currency/>, (Published Apr 2021, Retrieved 21 Apr 2021)
24. López Marcos A, SELF-SOVEREIGN IDENTITY—The future of identity: self-sovereignty, digital wallets, and blockchain, inter-American development bank, <https://publications.iadb.org/en/self-sovereign-identity-future-identity-self-sovereignty-digital-wallets-and-blockchain>
25. Reynolds K, Yahoo!News, Buterin, Srinivasan Donate to COVID Relief Fund for India ‘Shaken’ by Second Wave, <https://news.yahoo.com/buterin-srinivasan-donate-covid-relief-161927554.html>, (Published 25 Apr 2021, Retrieved 29 Apr 2021)
26. Boar C, Wehrli A, BIS, Ready, steady, go? Results of the third BIS survey on central bank digital currency, <https://www.bis.org/publ/bppdf/bispap114.pdf>, ISSN 1682-7651 (Published Jan 2021, Retrieved 21 Apr 2021)
27. Saha D, Ray P (2021) The Techno-Economics of Central Bank Digital Currency (CBDC): An Exploration, Indian Institute of Management Calcutta, Working Paper Series WPS No 862 / April 2021
28. Kharpal A (2021) El Salvador becomes first country to adopt bitcoin as legal tender after passing law, CNBC, <https://www.cnbc.com/2021/06/09/el-salvador-proposes-law-to-make-bitcoin-legal-tender.html>, (Published 8 Jun 2021, Retrieved 20 Jun 2021)