"The genesis of digital currency can be traced to the birth of the Bitcoin network in 2009" | Puja Guha
(Pixahive)

What are digital and cryptocurrencies? Why is there so much hype about this new form of digital money? Will it threaten the hegemony of paper money? A detailed explainer in the context of recent policy explorations in India on a Central Bank Digital Currency.

Digital currency has stolen the imagination of the media, investors, central banks and governments. While the jury is still out about its nature, costs and benefits, there has been a flurry of opinion of two extremes. At one end of the spectrum, there are the netizens who see digital currency as a messiah that will unchain money from the exclusive control of central banks, and, at the other, many a policymaker sees it a threat to financial stability.

How different is digital currency (a form of digital money) from physical money?

Loosely speaking, the genesis of digital currency can be traced to the birth of the Bitcoin network in 2009, when a mysterious Satoshi Nakamoto, whose identity is yet to be firmly established, released the Bitcoin protocol as an open-source software. The cryptocurrency bitcoin (BTC) is not the only form of digital money. Over the years paper cheque-based transactions came to be replaced by digital modes of transfer like the RTGS (Real Time Gross Settlement) or NEFT (National Electronic Fund Transfer). In the process, money had already become digital as all high-value cheques effectively became digital cheques.

While BTC has become synonymous with cryptocurrency, it has had numerous competitors who have also
evolved. What has made BTC unique is that it has fascinated the millennial generation. To the uninitiated, however, a number of questions have to be answered. What are digital and cryptocurrencies? Why is there so much hype and hoopla about this new form of digital money? Does it threaten the hegemony of paper money? The present essay, in the nature of an explainer, tries to answer some of these questions.

Some basics

To begin at the beginning, let us clarify some of the technical terms associated with this form of digital money.

Centralized ledger versus distributed ledger

In today’s world, whenever two strangers exchange any asset, intermediaries whom both the strangers trust come into picture. This third party plays a pivotal role in establishing the trust chain between the two transacting parties. When a buyer Ms. A pays a seller Mr. B by cheque, their respective banks act as trusted intermediaries. The intermediaries also manage the complete process and record the exchange in a ledger for future reference. For instance, each bank maintains a ledger at its end to document all the transactions. Both parties have a great deal of trust in the presumably “unbiased” intermediaries and hope that they faithfully maintain the ledger. In the digital world, a ledger is usually implemented as a database. With the adoption of cloud technology, databases are available as a service from the cloud, whose price has come down. Even a small organization can afford a reasonably large database. If not only the banks but also transacting parties like Ms. A and Mr. B maintain ledgers, we have four copies of the same ledger with all the four parties. Every transaction is noted in all the copies. Such a situation leads to full distribution of the ledger among all the parties in a system, and the ledger is said to be distributed. This is quite different from the earlier situation where only one ledger was maintained by each of the intermediaries as a central authority. If all the parties in a system have a copy of the (distributed) ledger, is it reasonable to do away with the intermediary? The answer is “yes”, provided all parties follow a well-designed consensus mechanism. Therefore, today centralized ledgers are no longer the only viable option for exchanging assets.

The distributed ledger is a proven concept as an alternative. because the Internet, being an extremely large distributed system, has successfully exhibited how things can work seamlessly without any central supervision. From the technology perspective, the distributed ledger is implemented as a distributed database across all nodes. Multiple copies add redundancy to the system, thereby eliminating the possibility of a single point of failure, and makes the system robust (fail-safe). A summary of some of the important differences between the centralised and distributed ledgers is presented in Table 1.

| Table 1: Centralised versus Distributed Ledgers: Key Features |  |
|---|---|---|
| Key aspect | Centralized ledgers (CLs) | Distributed ledgers (DLs) |
| Middleman or central agent | Yes, relying on intermediaries. Hence burdened by the fees and inefficiencies of the middleman. | No middlemen and intermediaries. No need to pay a central agent. |
| Bottleneck in the middle | Yes, speed of transaction is limited by the efficiency of intermediary. | No, it’s directly peer to peer (P2P). Assets are directly and immediately exchanged. |
| Single point of failure | Yes – if the central ledger becomes unavailable due to some reason, the complete system fails. | No such threat exists because the ledger is distributed across the system. |
| Trust | All participants need to trust the middleman or intermediary holding the single ledger. | No participant needs to trust any other participant. The system guarantees the validity of distributed ledgers. |

Source: Adapted from Saha and Ray (2021)
Birth of the Bitcoin and blockchain

The BTC is not the beginning of the story. The concept of digital cash / money can be traced to much earlier. American computer scientist and cryptographer David Chaum, hailed by many as the father of digital cash, was the first researcher to come up with the idea of “DigiCash” in his research paper published in 1983. He went on to start his own electronic cash company in Amsterdam in 1989, which unfortunately had to file for bankruptcy in 1998. Around the same time, e-gold – an Internet-based “digital currency” introduced in 1996 – became so popular in the United States and came to have several million active users that the US government had to intervene and shut it down in 2008. The first BTC was mined in January 2009 when the world was desperately trying to come out of the financial crisis of 2008. It was only around 2011 that BTC started to gain traction and garner support from investors, and subsequently the “Bitcoin Foundation” was created in 2012 as a task force dedicated to overseeing BTC’s development and propel its mass adoption.

The biggest criticism against cryptos is that they are not backed by any fiat, and they are inherently volatile being driven by speculation.

The 2009 whitepaper by the mysterious Satoshi Nakamoto showed the world what a blockchain could be, what it could achieve as a distributed ledger, and how it could enable secure low-cost payments outside conventional rails. Nakamoto also showed how a notional tokenized network asset could be used for financial transactions, and how that cryptographically-verified token could act as a decentralised digital cryptocurrency – the bitcoin or BTC. The digital currency BTC exists only in 0’s and 1’s i.e., in bits and bytes in digital format; hence the name ’bit’coin.

The first commercial transaction using the BTC happened on 22 May 2010 (now known as bitcoin Pizza day in the crypto community), when an early adopter of bitcoin named Laszlo Hanyecz purchased a pair of Papa John pizzas for 10,000 BTC. One can guess the value of one BTC at that time. Compare that with the current valuation of one BTC at about $64,000 (on 15 November 2021). It reached an all-time high of $68,521 on 5 November 2021. Following the so-called “success” of the BTC, several other popular cryptocurrencies have come into being. As of September 2021, one rough estimate is that there are about 6,500 cryptocurrencies worldwide, but most of these cryptos are obscure with hardly any backers and investors. It is still doubtful if cryptocurrencies can be a working currency. Whether they can be an alternative to government-backed fiat currency is even more difficult to answer at this point, though El Salvador adopted BTC as legal tender in June 2021. The biggest criticism of cryptos is that they are not backed by any fiat, and they are inherently volatile being driven by speculation. For example, see the BTC price during the period 2009 to 2017 (Figure 1).

As of September 2021, one rough estimate is that there are about 6,500 cryptocurrencies worldwide even though most of these cryptos are obscure.

All said and done, there is no doubt that the blockchain technology, on which most of these cryptos are based, has drawn the attention of innovators and fintechs alike. The blockchain structure as a “distributed ledger” promises to disrupt the traditional BFSI (Banking, Financial Services and Insurance) sector altogether. This will be so because blockchain as a concept is not necessarily associated with any currency, i.e., there can be blockchains which do exist even without any inherent currency. For an explanatory discussion of the blockchain (see Saha and
As a special type of distributed ledger inside the system, blockchain can be either permissioned or permissionless. The permission refers to the restriction imposed on the participating entities on validating and/or appending new entries/blocks to the ledger. If every entity has an equal right to do so, the ledger is permissionless; else it is permissioned. In the extreme case, if only one entity has the permission, then that permissioned ledger ultimately boils down to a virtually centralized ledger, though the ledgers are distributed amongst all.

Where does bitcoin stand vis-à-vis physical currency?

Contrasting the US dollar (fiat money) vis-à-vis the BTC (the most well-known cryptocurrency) may drive home the essential properties one can look for in a digital currency (Table 2).
Note that, while the BTC is not subject to inflation risk, it is prone to exchange rate risks. Interestingly, contrary to popular belief, bitcoins are not costless. If one accounts for electricity consumption behind their proof-of-work (PoW) computation, they are quite costly. Bitcoins may also be prone to huge risks of hyper-deflation. Yet, the key feature of the BTC is the existence of a distributed ledger/registry (Table 1). BTC is just one type of digital currency; there can be several kinds of digital currency.

### Types of digital currencies

What is money broadly? Amongst the plethora of definitions of money that economists have published over the years, Scitovsky (1969) captured it rightly when he said "Money is a difficult concept to define, partly because it fulfils not one but three functions, each of them providing a criterion of moneyness . . . those of a unit of account, a medium of exchange, and a store of value". Historically, several physical objects have served as tokens to represent money—such as, Yap stones, gold coins, cigarettes in war times, or high value paper bills. Thus, fundamentally, "Money is a convention, whereby one party accepts it as payment in the expectation that others will also do so" (Carstens, 2018). Note that the origin of the money presupposes various powers. First, it is an economic construct. Second, social acceptability plays a key role in recognition of money. Third, money needs to be backed by state power. Fourth, the creators of money need to have a technology that is not freely available so that counterfeit money cannot be produced easily. Thus, at the end of the day money is a social-economic-political-technological construct.

---

The bottom-line remains though that what we call money is nothing
but “a trusted token”. For currency, it is a physical token, for deposits it is a digital entry.

Note the importance of the concept of tokenization in this context. Fiat money in its current form is basically a paper/metal/plastic token issued by the state. We may call it the central bank physical currency (CBPC) if it is issued by the central bank of the state. Since it is backed by the state, it carries the notion of trust. Explicitly speaking, this trust comes from the backing of central banks (and government) in the case of paper currency and from the backing of commercial banks (and consequently clearing house) in the case of cheques. The bottom-line remains though that what we call money is nothing but “a trusted token”. For currency, it is a physical token, for deposits it is a digital entry.

Just think about what moves from your account to my account when you pay me Rs. 1000 via a UPI app, say BHIM. Is anything physical coming from my account and going to your account? No. Apart from a couple of ledger entries, nothing else happens. Thus, irrespective of the definitions, an important feature of money is that it reflects an accounting entity in a ledger/registry, which has hitherto been centralised. Illustratively, the role of the centralised registry is taken care of by the central banks in the case of CBPC or clearing house in the case of deposits. Apart from seeing it in our bank accounts, ideally we should also be able to keep digital currency in our digital wallets just as we keep CBPC inside our leather wallets. There is a plethora of digital wallets in India: Paytm leads the pack that also comprises PhonePe, Amazon Pay, Mobikwik, Jio money wallet, Airtel money wallet, and others. Just as CBPC is taken out of one leather wallet during cash payment and put into another in the physical world, the movement of digital currency from one digital wallet to another should ideally happen over the Internet.

What are the differences between the virtual, digital and crypto currencies?

A virtual currency is used only by virtual communities. As the European Central Bank noted, “virtual currency is a digital representation of value, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community; … it is not issued by a central bank or credit institution or e-money institution, … in some circumstances, [it] can be used as an alternative to money”.

Digital currency, on the other hand, “is an asset represented in digital form and have some monetary characteristics. … Digital currency can be denominated to a sovereign currency provided it is issued by the issuer responsible to redeem digital money for cash. In that case digital currency represents electronic money (e-money)” (BIS, 2015).

Cryptocurrency is a subset of digital currency. It is called crypto because it is based on some cryptographic algorithms. The BTC uses hashing and public-private key algorithms. It is therefore a cryptocurrency and hence a digital currency too. It started originally as a virtual currency used primarily within the bitcoin community. But now, with the wider acceptance of BTC by retailers, it is showing promise of being successful in the physical domain too. Regulation of virtual/digital currency is of great concern for every government. Towards this end, in 2014 the New York State Department of Financial Services proposed a regulatory framework for virtual currencies; it is commonly known as BitLicense.

Typically, there are two forms of money: account-based (claim) and token-based (object). The key difference between the two types of money lies in the verification process for payments. In an account-based system, what must be verified is the payer’s identity. In a token system, the authenticity of the item (object) to be exchanged instead needs to be verified.

Digital currency may be either token-based or account-based or a
Cash and coins are types of token money that have existed for centuries. In a cash transaction, the payee will accept payment only if she believes the cash is genuine, meaning the payee effectively assumes liability if the cash turns out to be counterfeit. Cryptocurrencies and money in digital wallets are token-based money (object). For example, to transact currency on Alipay’s network, all that is needed is a password linked to a particular digital “wallet.” No one is required to verify that the person who presented the password is the wallet’s true owner. Similarly, to transact cryptocurrency, the payer must sign transactions with her “private key” and the payee needs to unlock the transaction with her “private key”, and the transaction is valid regardless of who presents that key.

Cryptocurrencies and money in digital wallets are token-based money...

Importantly, token-based money is typically unrelated to the provision of credit, whereas account-based money tends to be inside money linked to the creation of credit. Digital currency may be either token-based or account-based or a combination of both, depending upon the uses—much like CBPC (object) co-exists now with deposits (claim) in the current system. If digital currency is token-based, it will add to the supply of token-based money alongside CBPC. On the other hand, if digital currency is account-based, it will add to the supply of account-based money alongside deposits. While the former will be a significant transition from the physical to the digital domain, the latter will be an easy extension in the already digital domain. However, an expansion in the supply of account-based money will surely have quite different socio-economic implications from an expansion in the supply of token-based money (Table 3).

<table>
<thead>
<tr>
<th>Table 3: Forms of Currency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
</tr>
<tr>
<td>--------</td>
</tr>
<tr>
<td>Regulated</td>
</tr>
<tr>
<td>Unregulated</td>
</tr>
</tbody>
</table>

Source: European Central Bank (2012)

Mainstreaming digital currencies: Central Bank Digital Currency

Where does one locate the Central Bank Digital Currency (CBDC) in the technological scheme of digital currencies? Its utility lies in providing a frictionless way for people to transfer and use funds. Governments need to offer CBDC in order to retain monetary independence. In the digital economy, as cash disappears and payments revolve around social and economic platforms rather than banks’ credit provision, the traditional transmission channels of monetary policy weaken significantly.

Conceptually, the CBDCs can be located in the taxonomy of money based on four key properties (Bech and Garratt, 2017): issuer (central bank or other); form (digital or physical); accessibility (widely or restricted); and technology (token- or account-based). Like CBPC and deposits, CBDC should also be regulated so that CBDCs “do no harm” to monetary and financial stability. Initially, it should coexist with CBPC and other types of money in a flexible and less-cash payment ecosystem. CBDC in your digital wallet should indeed be reasonably similar to the CBPC in your leather wallet. CBDC should differ from the digital deposit you have in your bank account in the
same way a banknote differs from money in your account. However, there will be a difference between CBDC deposits and current bank deposits. The deposit you have with the bank now is typically not legal tender. But CBDC would have legal tender status, though it would not be your bank’s liability. Since CBDC is backed by a central bank, through that it will have legal tender status.

**Cross country experiences**

Across the globe, central banks are experimenting with some form or the other of CBDC and building the capability to issue a cash-like CBDC. The motivations for working on issuing CBDCs tends to differ across countries. A survey of central banks in the BIS Committee on Payments and Market Infrastructures (CPMI) in late 2019 revealed six motivations: (1) payments safety/robustness; (2) domestic payment efficiency; (3) financial stability; (4) monetary policy implementation; (5) payments efficiency; and (6) financial inclusion (Boar, et al., 2020). Interestingly, in summarizing the survey on possible motivations for introducing CBDC, it was noted:

…Our overview has also shown some key common features. In particular, none of the designs we survey is intended to replace cash; all are intended to complement it. Most still involve a strong role for intermediaries—although potentially in parallel to direct provision of some services by central banks. None of the designs is pursuing the Indirect model, where a CBDC is a claim on intermediaries rather than on central banks. (Boar et al, 2020).

Interestingly, according to the BIS survey, as of mid-July 2020, at least 36 central banks have published some form of retail or wholesale CBDC work with at least three countries (namely Ecuador, Ukraine and Uruguay) having completed a retail CBDC pilot. Moreover, in some countries, viz., the Bahamas, Cambodia, China, the Eastern Caribbean Currency Union, South Korea and Sweden, retail pilots on CBDC are going on.

Interestingly, China has been working on its digital currency since 2014. After successfully building the digital yuan prototype in 2016, the People's Bank of China (PBoC), started the digital yuan research and development project at the end of 2017. The PBoC announced in October 2019 the release of the “digital renminbi” (digital RMB or e-CNY)—a cryptocurrency on the Digital Currency Electronic Payment (DCEP) system which can be decoupled from the banking system. The PBoC distributed CN¥20 million worth of digital renminbi in December 2020 to the residents of Suzhou through a lottery programme to promote the government-backed digital renminbi. Holders of digital renminbi could use it as retail CBDC to make both offline and online purchases.

To begin with, a number of countries (with the exception of China) were very cautious about the introduction of a CBDC. Apart from the fear of the unknown, losing the power to issue paper currency, the loss of seigniorage revenue on the part of the government, and threats to financial stability have all been expressed from time to time. In the Indian context, an apprehension has been expressed that introduction of a CBDC may lead to disintermediation of the banking system. In other words, a CBDC could not only have the potential to replace cash but could replace chequable bank deposits as well. A recent report of the Reserve Bank of India (RBI), has noted, “The public can convert their CASA deposits with banks into CBDC, thereby raising the cost of bank-based financial intermediation with implications for growth and financial stability. In countries with significant credit markets, commercial banks may lose their primacy as the major conduit of monetary policy transmission” (RBI, 2021; p. 154).

A knotty issue in this context is the presence of a negative interest rate that is currently prevalent in some of the advanced countries. Would such a negative interest rate be applicable on CBDCs as well? One recently proposed solution to limit disintermediation is the introduction of a two-tier remuneration system for CBDCs, as proposed by Bindseil and Pannetta (2020).
While many central banks may not have immediate plans to issue a CBDC, private players are not sitting idle. The wakeup call was given by Facebook’s announcement in June 2019 about its own digital currency, initially called Libra, later known as Diem. If 2.8 billion Facebook users spanning the globe start using Diem, what would happen to the prevalent sovereignty over money supply; what would happen to the international monetary system? The Diem project though stalled now, shook major governments and central banks and prompted them to rethink their “wait and watch” stance on CBDC.

What has been the Indian stance?

There has been quite a bit of interest in cryptocurrency in India. In fact, a recent study by the broker discovery and comparison platform BrokerChooser has placed India as the seventh-most crypto-aware country. As over 70 per cent of Indian investors in cryptocurrency did not invest more than Rs 3000, such interests seemed to be highly exaggerated.

Despite such euphoria about cryptocurrency there, has been a plurality of views about their usefulness. In one of the earlier initiatives, the central government had constituted an Inter-Ministerial Committee (IMC) in November 2017 under the chairmanship of the Secretary (Department of Economic Affairs, Ministry of Finance), to study the issues related to virtual currencies and propose specific action to be taken. In the report, the IMC highlighted the positive aspect of distributed-ledger technology (DLT) and suggested various applications, especially in financial services, for use of DLT in India. In particular, it mentioned, “The DLT-based systems can be used by banks and other financial firms for processes such as loan-issuance tracking, collateral management, fraud detection and claims management in insurance, and reconciliation systems in the securities market”. As far as private cryptocurrencies are concerned, the committee highlighted various risks and recommended a ban on cryptocurrencies in India and the need to impose fines and penalties for carrying on of any activities with cryptocurrencies. The IMC also proposed that the government keep an open mind on official digital currency.

What make digital currencies truly revolutionary are the tremendous new functionalities they offer.

The RBI too has repeatedly cautioned users, holders and traders of virtual currencies (including Bitcoins) on the various risks associated in dealing with such virtual currencies. In April 2018, the RBI imposed a virtual ban on cryptocurrencies. After the Supreme Court quashed this ban in March 2020, the RBI issued a circular on May 31, 2021 giving some forward guidance to the banks.” More recently, on November 11, 2021, RBI Governor, reportedly raised an alarm bell and pointed out that cryptocurrencies tended to pose a very serious concern from a macroeconomic and financial stability viewpoint. Meanwhile, the government has prepared a draft “Banning of Cryptocurrency & Regulation of Official Digital Currency Bill, 2019”. This draft Bill seeks to “prohibit mining, holding, selling, trade, issuance, disposal or use of cryptocurrency in the country”. On November 13 2021, Prime Minister reportedly chaired a meeting on the way forward on the issues relating to cryptocurrency. The outcome of the meeting is yet to be known.

Insofar as introduction of a BDC is concerned, the Deputy Governor of the RBI, commented recently, “RBI is currently working towards a phased implementation strategy and examining use cases which could be implemented with little or no disruption” (Rabi Sankar, 2021). Going forward, a major issue could come up if the CBDCs become interest bearing. In this context, a former RBI Governor has recently said that the intermediary function of commercial banks could come under stress if the CBDC offered by RBI becomes an interest-bearing instrument.

Thus, while the CBDC does have the potential to become a digital currency, a number of practical and implementation-related issues need to be settled in the days to come.
Going ahead

At a conceptual level, looking at the recent experience and the literature, one may perhaps differentiate between two distinct notions, (a) a digital currency and (b) a digital asset. While it seems that the digital asset is a concept whose time has come, one is not so sure about digital currencies. However, what make digital currencies truly revolutionary are the tremendous new functionalities they offer. They are the financial equivalent of the leap from postal service to email, or lending library to the Internet. But, while digital currency has many benefits, the presence of a decentralized register in the case of cryptocurrencies makes it difficult to substitute money (both cash and cheque (physical or digital)). At the risk of being speculative, one gets a sense that the authorities have realized that it is difficult to fight digital currency and have therefore decided to join the bandwagon of CBDC. While work on CBDCs is going on the world over, it is still in the process of being and becoming. To say that we do not know the future enough is perhaps not a helpful way to conclude, but given the euphoria of the market and scepticism of the regulators, as of now it seems that the future of digital currency looks somewhat hazy.

This article reflects personal views of the authors.

The India Forum welcomes your comments on this article for the Forum/Letters section.
Write to editor@theindiaforum.in

References:


IMF (2016): "Virtual Currencies and Beyond: Initial Considerations", IMF Staff Discussion Note, No. SDN / 16/ 03.


Tags: Digital Currency
       Bitcoin

Footnotes:

1. Recently Forbes Magazine reported ten major cryptocurrencies (with market capitalization in brackets): (1) Bitcoin (over $821 billion); (2) Ethereum (over $353 billion); (3) Tether (Over $68 billion); (4) Cardano (over $67 billion); (5) Binance Coin (over $64 billion); (6) XRP (over $44 billion); (7) Solana (over $41 billion); (8) USD Coin (over $31 billion); (9) Polkadot (over $28 billion); (10) Dogecoin (over $26 billion).


3. The bitcoin network runs on the most exhaustive consensus mechanism known as Proof of Work (PoW) which is compute-intensive and hence energy-hungry. Migration to more energy-efficient consensus mechanisms, such as Proof of Stake (PoS) in Cardano, Proof-of-Authority (PoA) in Binance, and Proof of History (PoH) in Solana, is however, offering viable cost-effective alternatives to PoW.

4. In the draft Bill, cryptocurrency is defined as, "any information, code, or token which has a digital representation of value and has utility in a business activity, or acts as a store of value, or a unit of account".