Citi GPS

FUTURE OF MONEY

Crypto, CBDCs and 21st Century Cash

Citi GPS: Global Perspectives & Solutions

April 2021

Ronit Ghose, CFA
Global Head of Banks, Co-Head of Global FinTech Research

+971-4-509-9586 | ronit.ghose@citi.com

Judy Zhang
Co-Head of Pan-Asia Banks Sector

+852-2501-2798 | judy1.zhang@citi.com

Yafei Tian, CFA
Hong Kong, Taiwan, Korea Banks & Insurance Analyst

+852-2501-2743 | yafei.tian@citi.com

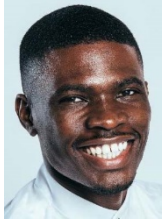
Kaiwan Master
Europe Banks Analyst

+44-20-7986-0241 | kaiwan.hoshang.master@citi.com

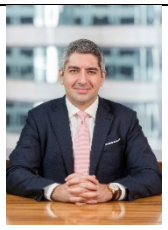
Ronak S Shah
Europe Banks Team

+44-20-7986-3960 | ronak.sharad.shah@citi.com

Expert Contributors



Temitope Alabi
CEO & Co-Founder, Afriex



Henri Arslanian
Global Crypto Leader, PWC

Tony McLaughlin
Emerging Payments & Business Development, Citi TTS

+44-20-7508-0851 | tony.mclaughlin@citi.com

Monica Singer
Decentralized Blockchain Expert

Naveed Sultan
Chairman, Institutional Clients Group, Citi

+44-20-7500-5153 | naveed.sultan@citi.com

Ajit Tripathi
Head of Institutional Businesses, Aave

Andres Wolberg-Stok
Head of Strategy, Chief Technology Office, Citi

+1-718-360-0909 | andres.wolbergstok@citi.com

With thanks to:

Shobhit Maini
Transformation, Citi MSS

Ebrahim Rahbari
Global Head of FX Analysis, Citi

Omid Malekan
Blockchain Innovation Expert, Citi Ventures

Christopher Chapman
Europe Credit Strategy, Citi

FUTURE OF MONEY

CBDCs, Crypto and 21st Century Cash

Kathleen Boyle, CFA
Managing Editor, Citi GPS

We live in a digital age. How we communicate, shop, entertain ourselves, take care of our health and order groceries, all look significantly different than how we would have done it just 20 years ago. Banking and finance is also changing. And so is money.

We already have digital money – trillions move every day, electronically. But are we on the cusp of Digital Money 2.0? Not the account-based electronic money that's been around for the past several decades, but a new type of token-based digital money. Tokenization, often via blockchain, is the basis of cryptocurrencies, stablecoins, and many proposed central bank digital currencies (CBDCs).

While much attention has focused on Bitcoin in recent months, the ongoing experiments, pilots, and policy work around CBDCs could be equally if not more significant for the world of money. Central banks around the globe are warming up to CBDCs, triggered by Big Tech, and their ambitions to build alternative payment rails to existing card and bank-based payment systems with tokenized money, as in the case of the Facebook-backed Diem project.

China is currently well ahead of major peers in developing a CBDC (which they call a Digital Currency Electronic Payment, or DCEP) and is already at the point of extensive pilot testing. Given the country's sprint to becoming a cashless society, we expect fast adoption of DCEP over the next five years relative to other CBDCs. Meanwhile, work on a digital Euro is now underway (we expect imminent announcements from the ECB) and U.S. policy makers are also now warming up to the idea of a Digital Dollar.

While stablecoins such as Diem await regulatory approval, they could benefit from the huge network effects of their Big Tech sponsors. In fact, Diem could be an effective tokenized payment format inside the Facebook universe. It is possible other Big Techs could follow into tokenized money, but for now, few have declared this ambition publicly — and Facebook's user reach is extensive (3.3 billion monthly average users) and hard to replicate.

Increased interest in cryptocurrencies like Bitcoin and Ethereum are also driving digital money. Market values have surged recently, with cryptocurrencies valued at an aggregate of approximately $2 trillion. While consumers have driven much of the adoption of crypto, the recent wave appears to be more broad-based versus 2017-18, with interest from both institutional investors and corporates as well as retail investors. Despite the popularity of crypto, it serves more as a (volatile) digital asset than a transaction currency in most parts of the world today.

All transitions have intended and unintended implications. Tokenized money could disintermediate incumbent financial institutions, increase the volatility and cost of bank deposits, and substitute existing payment form factors such as checks and cards. New payment solutions could disrupt the already crowded payment space. But crypto trading and custody could be a new source of revenue for financial institutions and CBDCs could result in more efficient and targeted monetary and fiscal policy implementation.

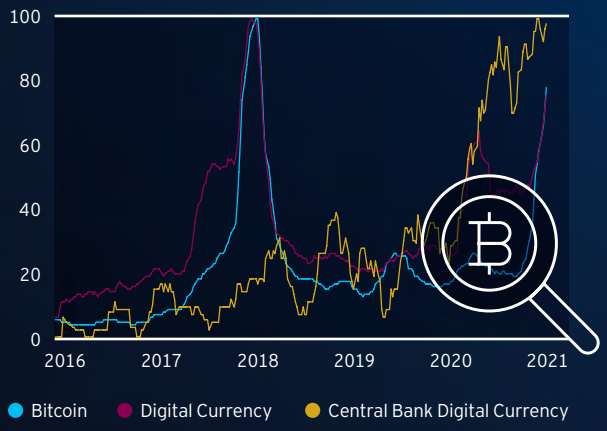
The race towards Digital Money 2.0 is on. Some have framed it as a new Space Race or Digital Currency Cold War. In our view, it doesn't have to be a zero sum game — there's a lot of room for the overall digital pie to grow.

Money at the Digital Frontier

INTEREST IN CRYPTOCURRENCIES SOAR

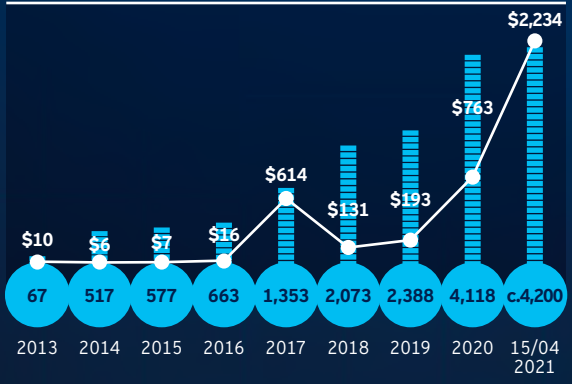
The total market value of cryptocurrencies has more than tripled from its prior 2017 peak and search interest is steadily rising. Bitcoin has led the surge, accounting for about two-thirds of the total crypto market value. Unlike 2017 when Bitcoin activity was mainly by retail investors, global institutional investors, and corporates are much more involved in the 2020-21 rally.

Google search interest over time



Source: Google Trends

Number and value of cryptocurrency over time



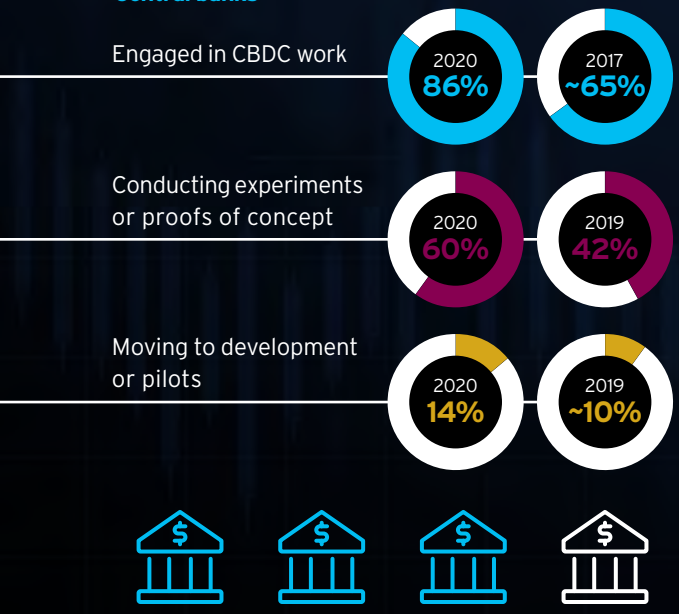
Source: coinmarketcap, Citi Research

CENTRAL BANKS ENTER THE ARENA

Source: BIS Papers No. 114

The development of Central Bank Digital Currencies (CBDCs) is still at an early stage but central banks are increasingly exploring this pathway. Plans for Diem (formerly Libra, a Big Tech-supported stablecoin) and China's progress in advancing its CBDC are driving central banks' interest in asserting ownership of the domain.

Central banks



BUT **3 IN 4** EITHER LACK THE LEGAL AUTHORITY TO ISSUE CBDCs OR ARE UNCERTAIN

China in the CBDC lead

China started developing its Digital Currency Electronic Payment (DCEP) CBDC in 2014 and tested a pilot in 2020. We expect China's sprint to a cashless society will drive DCEP adoption for retail use within five years.

RMB 314 trillion in mobile payment volume Jan-Sept 2020, up **>135x** from FY 2012.

Mobile payment penetration: **87%** in December 2020 vs. **25%** in December 2013.

Over **$300 million** in DCEP transactions in the pilot program.

KEY RISKS AND OPPORTUNITIES OF CBDCs

Along with significant opportunities offered by digital money, there are also potential implications around its adoption for banks and payment systems, currency, and policy.

Negatives:

- Disintermediation risk plus higher cost and volatility of deposit funding.
- Increased payment competition, crowding out of private sector.
- Threats to financial anonymity and privacy for citizens.
- New 'Space Race' in money between USD, RMB, EUR.

Positives:

- Improve targeting of monetary and fiscal policy.
- State-issued digital money promotes inclusion and universality.
- Reduce cost and improve efficiency in domestic payments.
- Improve management of financial crime risks.

BIG TECH, STABLECOINS AND DIEM

The story of digital money in the 2020s will be the growth of tokenized money. Central banks (via CBDCs) and Big Tech (via Diem and similar initiatives), alongside wider adoption of cryptocurrency, are building new payment formats and rails. Stablecoins such as Diem could benefit from the huge network effects of their Big Tech sponsors.

Use cases for Diem

1

Big Tech Money
Build out of payment rails via next-gen digital tokens to promote greater monetization inside social media and e-commerce platforms

2

White Label Provider
Potentially work with central banks to add their currency as a stablecoin on the Diem network

3

Cross-Border Payments
Global application could lead to reduced cross-border payment costs

Contents

Future of Money

Technologists had wanted to build digital currencies into the Internet from the beginning: "***We knew we were missing this, we just didn't know what it was***." (Marc Andreessen).

Digital is taking over the world and money is no different. A 'space race' is underway in digital money with central bank-issued digital currencies (CDBCs) on the policy agenda, Big Tech ambitions in the space (i.e., Diem), and cryptocurrencies becoming increasingly popular, albeit more as a digital asset than a transaction currency for now.

In this report we take a closer look at how money is changing. Our key points include:

- Money in the modern era is account based: "I am, therefore I own". Before the computer era, this was literally a physical ledger entry, built on double-entry bookkeeping. Twentieth-century digital money was the electronic version of this.
- Digital money in the 21st century is different — it's tokenized: "I know, therefore I own". Being programmable, its value can be fiat linked (or not) and its technology and governance can centralized (or not). The story of digital money in the 2020s is the growth of tokenized money.
- The base money of the Internet age will increasingly be tokenized, driven by central banks (via CBDCs) and Big Tech (via Diem et al.), alongside wider adoption of cryptocurrency. Popular focus is on Bitcoin (BTC) but CBDCs could be a game changer.
- Money is entering a format war, but unlike similar conflicts in video or electricity, we do not see this as a winner-take-all competition. We believe tokenized and account-based money, centralized and decentralized money, will all co-exist.
- However, tokenized money, such as CBDCs, stablecoins and cryptocurrencies such as Bitcoin are relatively new and could be disruptive to the existing monetary, banking, and payment structures.
- Tokenized money could disintermediate incumbent financial institutions, increase the volatility and cost of bank deposits, substitute for existing payment form factors such as checks and cards and, in theory, challenge U.S. dollar hegemony.
- Central bankers are developing CBDCs, triggered by Big Tech and the launch of Diem in 2019, and a space race is developing. China is ahead and is already in pilot stage, while work on a digital euro is now underway, and U.S. policy makers are warming up to the idea.
- Stablecoins such as Diem await regulatory approval. They could benefit from the huge network effects of their Big Tech sponsors. Diem could be an effective tokenized payment format inside the Facebook universe (3.3 billion monthly average users).
- Bitcoin originally was designed as peer-to-peer (P2P) digital cash. But outside some regions, such as Africa cross-border, the digital cash narrative for Bitcoin remains weak, given scalability and efficiency questions and its rising price.

- The 'digital gold' narrative for Bitcoin is in the ascendency. The current Bitcoin rally is different to the 2017 Bitcoin bounce mainly as there is more global institutional interest. But valuing Bitcoin (BTC) remains a controversial art — is it worth zero or a lot more than today's price?
- Digital money, in its tokenized form, is a mix of cryptography, economics, and politics. How it works, what its different primary form factors are, and their implications is the story of this report.

The Original Sin of the Internet

The absence of a 'buy button' from the original consumer Internet, e.g., the inability to build payments into the browser, has been described by Marc Andreessen as the original sin of the Internet. As money could not be built into the browser in 1993, the consumer Internet grew based on advertising.[1]

Mr. Andreessen has compared the timeline of the evolution of cryptocurrency and blockchain technology to the evolution of the Internet itself. Andreessen notes that in 1992 the Internet was still a fringe activity and crypto today is similar, but “it’s starting to feel really, really close to mainstream.”[2]

While technologists argue for new forms of digital currencies, the view of the financial policy establishment was well summarized in recent remarks[3] by Agustín Carstens, General Manager of the Bank for International Settlements: "***Digital money is not new and if new forms are needed it should be led by central banks"***.

Carstens’ critique of private sector digital currencies such as Bitcoin focuses around three key issues: their value stability, technical robustness, and efficiency. The critique of stablecoins — crypto which is linked to fiat currencies or other stable assets — largely relates to governance.

Society determines what is accepted as money. In the modern world, money narrowly defined (M0) is created by central banks (notes, coins, deposits at the central bank). In decentralized States, this monopoly of base money creation is weakened and sources of money creation become diverse.

This challenge to the State’s monopoly power over base money is what makes tokenized digital money so disruptive. Libra 1.0 (the precursor to Diem) attempted to create a new synthetic currency, while Bitcoin and other cryptocurrencies governed on a decentralized basis have value established independently of existing fiat currency.

Everyone Is (Once Again) Talking Digital Currencies

Digital currencies are topical and public interest is high again. Google searches for digital currency have been rising (Figure 1), the combined value of private crypto hit an all-time high in early 2021 (Figure 2), and speeches by central bankers on CBDCs are also back at all-time highs (Figure 3).

[1] Mark Andreessen: From the Internet's Past to the Future of Crypto – The a16z Podcast, August 2019.
[2] Ibid.
[3] Digital currencies and the future of the monetary system – Remarks by Agustin Carstens, General Manager, Bank for International Settlements, January 2021.

Central banks have been analyzing the topic of Central Bank Digital Currencies (CBDCs) for a while. But a tipping point was reached following the announcement of Libra (now renamed Diem) in the summer of 2019, which created a debate over whether a private actor with several billions of active users should help build a monetary format.

The idea of a private stablecoin like Libra/Diem accelerated the work being done by central bankers globally. Additionally, work on CBDCs in one part of the world (China) encouraged peers in other parts of the world to the same. (Albeit we should note that China's CBDC is not based on distributed ledger technology.)

Further, COVID-19 accelerated an ongoing change in customer behavior towards digital finance. In the U.K., ATM withdrawals during the COVID-19 lockdowns have been running at about half the pre-pandemic level (-43% versus previous 12 months).[4] Other historically cash-driven societies, such as Saudi Arabia, experienced an almost doubling of point-of-sale transactions (+75.3%) in 2020.[5]

COVID-19 had another impact: it led to significant fiat money expansion as central banks tried to support economies during lockdown and this appeared to support Bitcoin prices (Figure 4). This drove Bitcoin, which was originally a P2P payment mechanism, as per the 2008 white paper, to become viewed as 'digital gold' versus 'digital cash'.

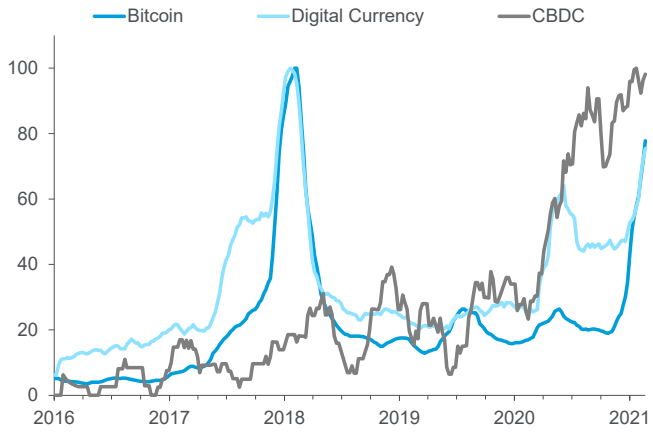
For Bitcoin supporters, monetary debasement fears justified a higher Bitcoin price — there was an increasing number of U.S. dollars in circulation but Bitcoin has a fixed supply. For others, central bank easing simply fed higher investment risk appetite, which led to increased interest in Bitcoin, cryptocurrencies, and other risk assets.

For skeptics, Bitcoin remains, according to Willem Buiter, "an asset without intrinsic value, whose market value can be anything or nothing".[6] One banker recently asked: why do you not value Bitcoin as a perpetual zero coupon bond? Translation: it should be worth zero. To which Bitcoin supporters reply: its intrinsic value comes from the network.

In the rest of the report we will discuss the pros and cons of different forms of digital money: CBDCs, stablecoins, and decentralized cryptocurrencies.

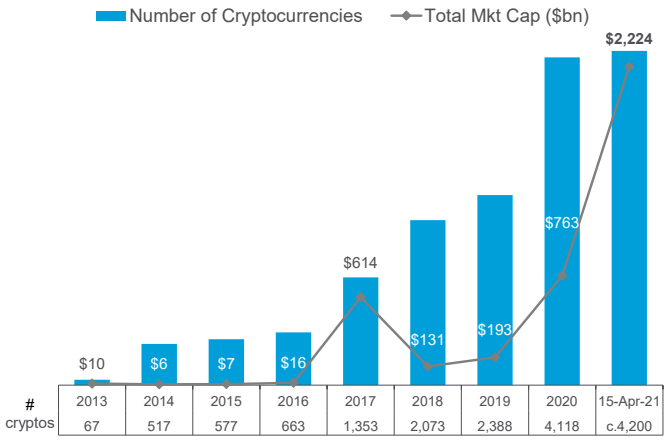
[4] Peachey, K. "ATM withdrawals drop by £37bn during year of Covid", BBC.
[5] Mubasher, "Saudi POS Sales Exceed SAR 349bn in 2020", December 30, 2020.
[6] Willem H Buiter, "Schrodinger's Bitcoin", Project Syndicate, February 12, 2021.

Figure 1. Google Search Interest Over Time



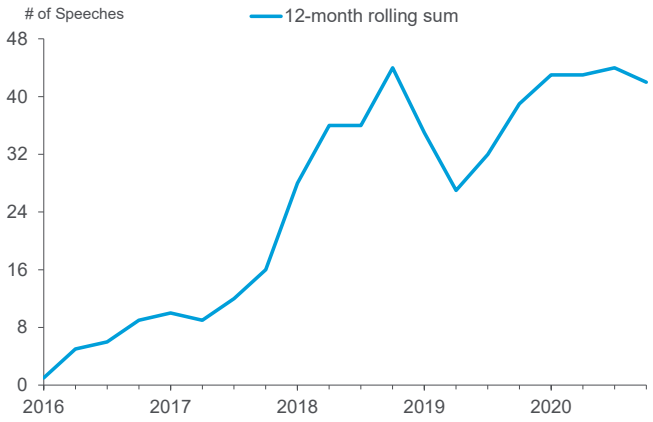
Note: 12-wk moving avg. indexed to peak of each series. Worldwide search interest on the term "Bitcoin" and "Digital Currency" and topic "Central Bank Digital Currency".
Source: Google Trends

Figure 2. Number & Value of Cryptocurrency Over Time



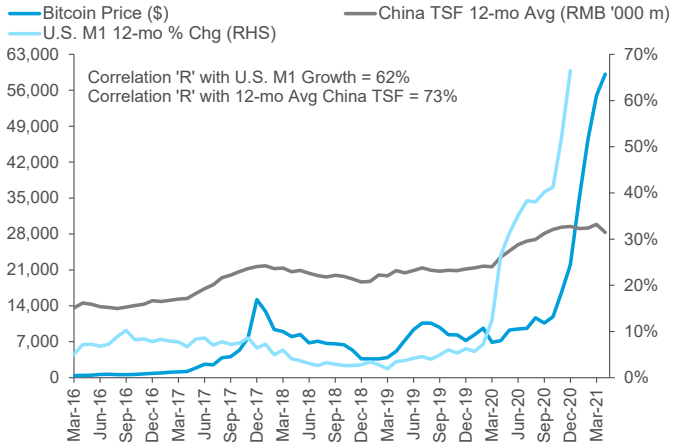
Source: coinmarketcap, Citi Research

Figure 3. Timing of Speeches and Reports on CBDC



Note: 12-month moving sum of count of central bankers' speeches resulting from a case-insensitive search for any of the following phrases: CBDC, central bank digital currency, digital currency, and digital money.
Source: BIS Working Paper No. 880.Citi Research

Figure 4. Bitcoin Price Correlation with U.S. M1 Growth and China TSF



Note: U.S. M1 Supply YoY change (%). China TSF 12-month rolling average.
Source: Datastream, Citi Research

Digital Currencies Still Early: A Look at Long-Term Implications

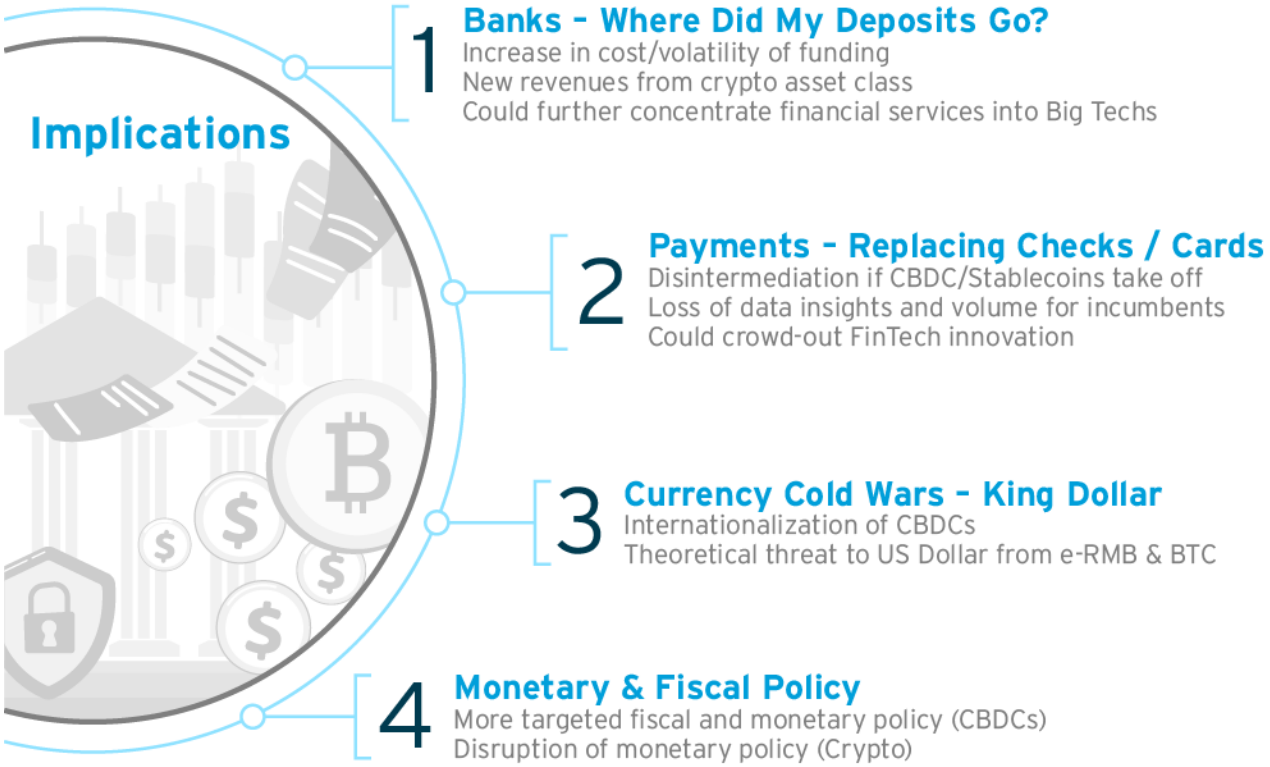
We are still early in the tokenized digital currency journey. As Marc Andreessen noted a couple of years ago, in terms of a timeline, today's digital currencies are equivalent to where the Internet was in 1992. Should digital currencies take off in the coming years the implications could be significant for the financial sector, policy makers, and society more broadly.

Digital currency tokens could disintermediate existing financial institutions, increase the volatility and cost of bank deposits, replace existing payment form factors such as checks and cards, and reduce U.S. dollar hegemony, albeit for now we see these as long-term risks given timelines for CBDCs and the small size of cryptocurrencies.

Policy positives attributed to CBDCs include more targeted monetary and fiscal policy and improved domestic payment inclusion and efficiency. They also create new revenue opportunities in trading, custody, and other services. A centralized CBDC also creates considerable privacy and anonymity questions.

Figure 5 and Figure 6 summarize the potential implications of digital money, which we discuss in more detail in the rest of the report.

Figure 5. Implications of Digital Money (in tokenized form)



Source: Citi Research

Figure 6. Summary: Impact of Digital Currencies

Risk to Commercial Banks	Risk to Existing Payment Infrastructure	New Sources of Revenue	Policy Opportunities	Role of U.S. Dollar
Potential higher funding cost and volatility including increased risk of bank runs in a crisis – this can be partly mitigated	New payment solutions could disrupt the already crowded payment space, challenging existing form factors via lower cost	Crypto trading and custody could be a new source of revenue for financial institutions – in the near term the opportunity is greater for specialist firms	More efficient and targeted monetary and fiscal policy implementation via CBDCs – greater surveillance ability also raises questions around privacy	The issuance of CBDCs and private stablecoins could, in theory, compete with the U.S. dollar (USD$) – but irrespective of token technologies, the U.S. dollar has many advantages
CBDC in a maximalist version would shift commercial bank deposits to central bank liabilities, raising bank funding costs and volatility.	Existing retail payments (e.g., credit cards) can have transaction costs. CBDC, crypto, or national A2A payment systems could lower transaction costs and income.	Crypto exchanges and custody include new specialist firms, but traditional banks have announced plans to enter this segment. But fees on crypto custody alone may not be significant, and could only provide a sizeable opportunity when merged with trading fees.	The central bank will be able to control the subject, interest rate, and timing of credit extension. For this to be successful, CBDCs have to be a material form of payment.	Some policymakers have highlighted the potential of CBDCs to build international rails that could be outside the current account-based rails subject to U.S. sanctions policy.
Risk to financial stability can be mitigated by a 'two-tiered' CBDC system, where the central bank issues CBDC to commercial banks who hold them under custody for clients (while the liability still remains with the central bank).	Crypto or stablecoins as a payment solution could gain further traction in emerging markets where the local currency is volatile, foreign exchange is hard to obtain and cross-border payment rails are costly or inefficient.	A potential area for banks to explore is offering a crypto-denominated account, without actual delivery.	Better oversight on money flows as transactions are more traceable, which reduces AML issues (provided they are not cash-like, i.e., anonymous and non-KYC'd wallets).	USD's role as Invoicing Currency: CBDCs could reinforce the currency diversification that has already happened for bilateral trade payments.
Even in a two-tier model, commercial banks could see liquid deposits, which can be used to fund loans, partly replaced by "assets under custody" (CBDCs) that cannot be re-lent. This could reduce commercial bank money creation in the economy.	CBDC could help promote digital payments or it could be a 'category killer' in digital payments and drive out private investment and development which has boomed in many countries over the past decade.	Traditional exchanges have launched Bitcoin futures and options, enabling greater institutional trading options.	Support fiscal policy implementation – easier to provide stimulus checks directly to digital wallets.	USD's role as Issuance Currency: Requires liquid capital markets and stability. CBDCs don't change the wholesale market financial and legal infrastructure.
Banks could make client deposits stickier by bundling them with additional services (e.g., payments & mortgages). For larger banks, in the U.S. and many markets, client deposit scarcity is not a current risk as many big banks have too many deposits.	Greater use of CBDCs or other tokenized digital currencies could reduce the amount of client data available to payment companies.		An alternative to private company stablecoins, to ensure money creation remains with the central bank.	USD's role as Reserve Currency: Again, needs to be liquid and stable with store of value. A very high hurdle for most other currencies to currently cross, even with tokenization and differentiated technology.
			Financial inclusion, especially for emerging markets (possibly with use of lighter / tech-driven KYC compared to traditional bank accounts), and avoid private companies controlling payments.	

Source: Citi Research

Brief Review of Definitions

Digital money and electronic money are not the same thing, albeit in everyday life they are often used interchangeably to represent non-physical forms, i.e., money that is not paper-based but intangible. Most money today in the financial system is of this intangible, electronic, or digital format.

Digital Money 2.0 is (1) tokenized and not account-based, (2) it can be based on a centralized database or blockchain, and (3) its value can be linked to fiat currency (CBDCs, stablecoins) or set by supply and demand (cryptocurrencies). By contrast, electronic money is more straightforward: linked to fiat, account-based, centralized, and permissioned.

As well as having format-based differences, money has liability-based differences. Fiat-based digital or electronic money is redeemable at par, by the e-money institution, commercial bank, or the central bank (in the case of CBDCs). However, cryptocurrencies, and potentially stablecoins, have no legal par value.

Electronic Money is narrowly defined as an electronic store of monetary value issued by a regulated e-money institution and stored on a device, typically a smartphone or equivalent. In this chapter, however, we use the term electronic money more broadly to contrast with digital money, as set out in the table below.

In our broader definition of e-money, we include existing commercial bank money as well as liabilities of e-money institutions.

Figure 7. Digital Money versus Electronic Money (e-money)

	DIGITAL MONEY 2.0	VS.	E-MONEY
Value:	Linked to Fiat, or Generated by demand/supply		Linked to Fiat
Structure:	Can be Tokenized		Account-based
Technology:	Can be Blockchain-based		Centralized Databases
Governance:	Permissioned or Permissionless		Permission-based
Examples:	CBDCs, Bitcoin, Diem		Alipay, PayPal

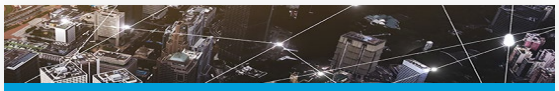
Source: Citi Research

Tokens vs. Accounts

Tokenization is fundamental to our definition of Digital Money 2.0. Benefits include:

- **24x365 Settlement:** Distributed ledger technology (DLT) networks are 'always on' while the traditional banking system is not.
- **Programmability:** 'Smart contracts' may be powerful means to embed finance in digital ecosystems.
- **Atomic Settlement:** Token exchange can remove settlement risk between counterparties.

Figure 8. Tokens vs. Accounts



Tokens

- Chains of digital signatures
- May be offered by unregulated entities
- Public or private DLT database
- May or may not represent liability of an institution
- Programmable through 'smart contracts'
- Wallets may or may not be KYC'd
- May be pseudonymous or anonymous
- Digital bearer instruments
- Synthetic and national currency units
- Atomic settlement — token transfer equals messaging & settlement
- 'Always on' infrastructure

Accounts

- Double entry bookkeeping ledgers
- Offered by regulated banks and non-banks
- Traditional database technology
- Liabilities of an institution to a depositor
- Programmable through APIs
- KYC on the account holder
- Not pseudonymous or anonymous
- Not a bearer instrument
- Denominated in national currency units
- Payment messaging and settlement are separate functions
- Batch processing and 'store and forward' messaging

Source: Citi

With account-based money, payments made across accounts held at different institutions have a special characteristic: the functions of messaging and settlement are separate. First Bank A sends a message to ask Bank B to make a payment. Then, Bank A needs to settle with Bank B through a separate channel.

When payments are made with tokens, the functions of messaging and settlement are collapsed into one. The token acts as a digital bearer instrument, so when the token moves to the recipient's wallet the transaction is complete. Tokenized value exchange removes many inefficiencies inherent to the account-based system, including errors, delays, and reconciliation issues.

Tokenized payments may provide benefits, but there are also downsides. Tokens may act as digital bearer instruments. But the general trend over past decades has been to remove bearer instruments from financial services due to the risk of financial crime. There is also a potential issue with safe management of cryptographic private keys.

Fiat money is a government or central bank-issued currency that is not backed by the value of a physical asset (like gold). As a liability of the issuing central bank, its acceptance and value as a medium of exchange (or payment) is a function of the stability and confidence in the government or central bank who also has control over the supply of the money (theoretically unlimited).

Most modern currencies, including the U.S. dollar, are fiat money. For much of recorded history, money has been based on gold or similar precious commodities and a link to that history continued into the 20th century. However, the U.S. formally abandoned the gold standard in the 1970s.

Cryptocurrencies, in their pure form, are decentralized, digital, and differ considerably to fiat money. Figure 9 below gives an overview of the differences.

Figure 9. Core Differences between Fiat Money and Cryptocurrencies

Taxonomy	Issuer	Form of Money	Value Recognition	Ledger	Supply
Fiat Money	Issued by a central bank or government	Multiple – including physical cash (coins and banknotes) and reserves held by financial institutions at the central bank	Backed by central bank credit	Centralized, issued, and controlled by the central bank	Unlimited — can be produced by the government when necessary
Cryptocurrencies	Mostly issued by the private sector (notably, there is no legal entity that issues Bitcoin)	Single form (i.e., digital token)	Facilitated by technology such as blockchain and relies on miners consensus	Decentralized, i.e., distributed ledger database is spread across several nodes/devices on a peer-to-peer network, where each replicates and saves an identical copy of the ledger and updates itself independently	Limited supply

Source: Citi Research

Cryptocurrencies, such as Bitcoin or Ethereum, are based on a peer-to-peer architecture that allows digital value to be transferred without a central authority. Cryptocurrencies rely on cryptography, the mathematical process of encoding and decoding information, to maintain security of transactions.

The value of cryptocurrencies, in fiat terms, depends on supply and demand within its network of users, which until recently have been relatively narrow. Since their beginning, with the emergence of Bitcoin in 2008, cryptocurrencies have been outside the conventional banking system, in that they are not liabilities of a central bank or commercial banks. However, crypto is increasingly joining the mainstream.

Central Bank Digital Currencies (CDBCs) are issued by governments or central banks as a digital form of fiat money and is controlled centrally, similar to fiat money. In institutional terms, CBDCs are different to e-money and commercial bank money as they are a direct liability of the central bank.

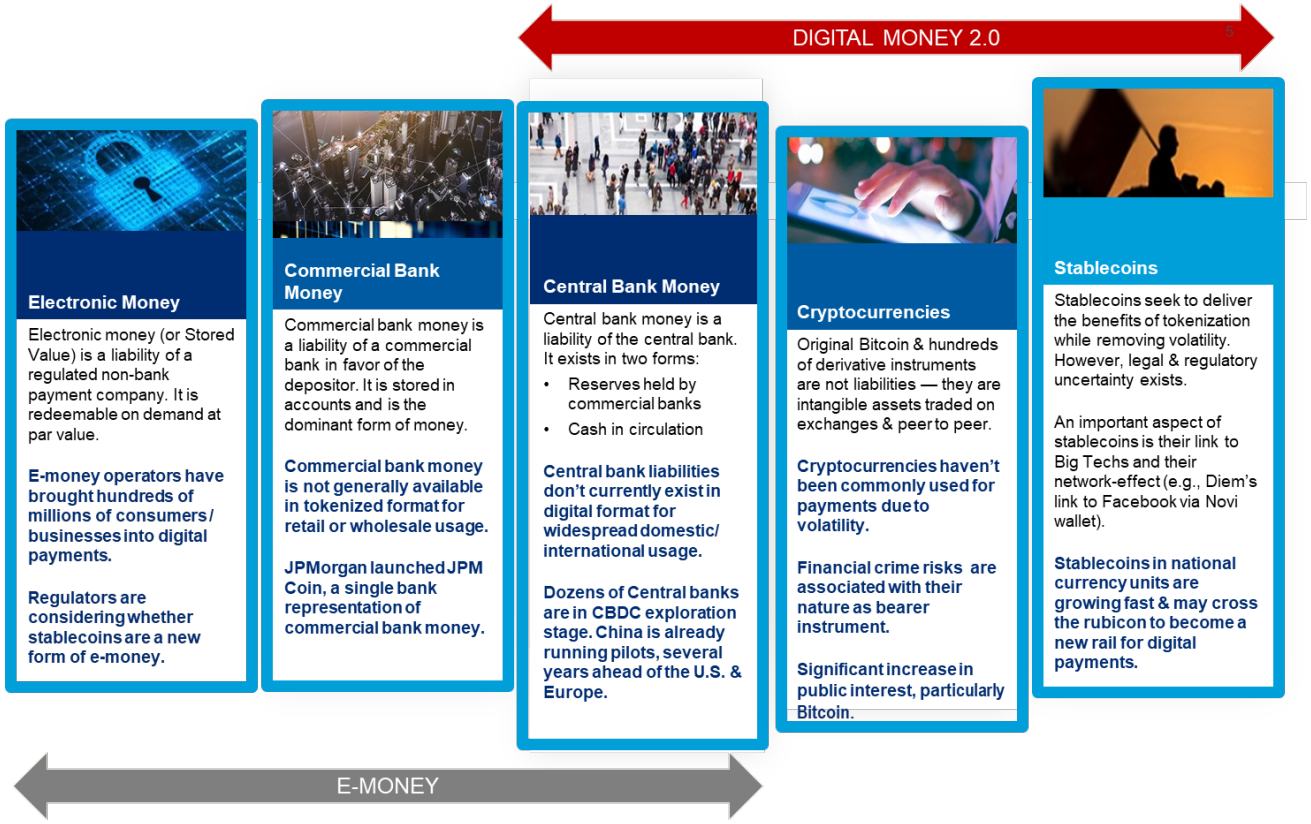
In technological terms, CBDCs can be centralized, similar to e-money, through a single proprietary system. Alternatively, they can be decentralized, using distributed ledger technology (DLT). The People's Bank of China (PBOC) is piloting its CBDC, known as Digital Currency Electronic Payment or DCEP, and we discuss this in detail starting on page 41.

Stablecoins are blockchain-based digital currencies collateralized to the value of an underlying asset (usually a claim on a reserve). Owing to their peg, stablecoins are not subject to extreme price volatility, which has otherwise prevented mainstream adoption of applications built on top of cryptocurrency protocols.

There are broadly four approaches to stablecoins: (1) fiat collateralized; (2) commodity collateralized; (3) crypto collateralized; and (4) non-collateralized. The most commonly collateralized stablecoins are linked to fiat currencies such as the U.S. dollar (USD), euro (EUR) or British pound (GBP). Prominent coins include Tether and USDC.

The biggest future stablecoin known today could be Diem (Libra). We discuss this in detail starting on page 57.

Figure 10. Digital and Electronic Money Families



Source: Citi

What is Money and Currency?

Before we discuss digital currencies in more detail, we first need to take a brief detour and define what money is. Over time, money essentially has served the following functions:

1. As a **unit of account**, which helps measure the value of a particular good or service;
2. As a **medium of exchange** for paying for goods and services; and
3. As a **store of value**, which can be saved, retrieved, and exchanged at a later time.

Social life in small pre-urban communities could function based on gift giving and reciprocity. But as civilization developed, more formal money was required. As Jacob Goldstein, in "*Money – The True Story of a Made-Up Thing*" notes: "the first known writing is not love notes or stories. It is IOUs".

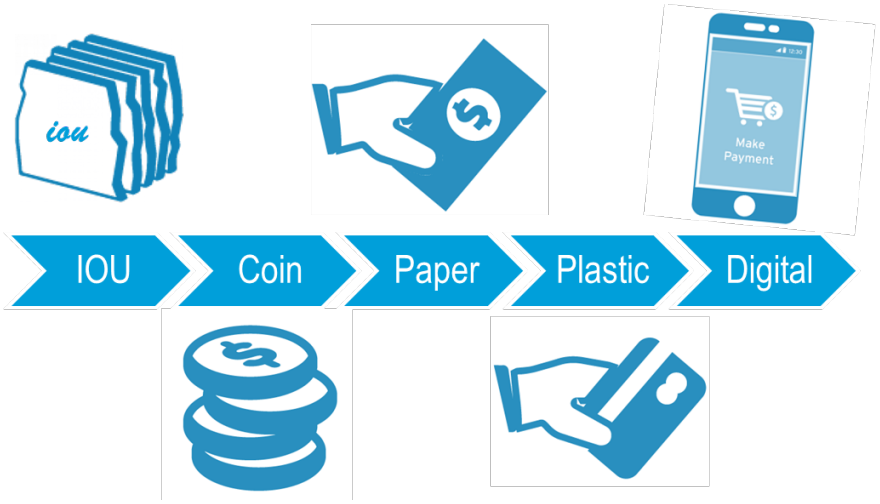
In Mesopotamia, around 3500 BC, money moved from clay tokens to clay tablets. Precious metal-based money followed, with coins circulating in Asia Minor around 550 BC. Paper money was invented by the Chinese, initially starting as promissory notes during the Tang Dynasty (618-907 AD).

China Leads: From Paper Money to Digital

By the time of Kublai Khan (1260-1294), paper money was no longer backed by precious metal, albeit this pure version of fiat money was temporary. But money was well on the road to becoming virtual. Just as China invented paper money, the digital money revolution appears to be most evident there.

Over the past decade in China, the mobile phone revolution, along with the boom in e-commerce and a growing middle class, has led to a proliferation of innovations. Digital wallets, based on e-money, now dominate payments. And it is no surprise that, among large countries, the Chinese are furthest ahead on CBDCs.

Figure 11. Evolution of Money



Source: Citi Research

A Citi View: Interview with Naveed Sultan

Naveed Sultan
Chairman, Institutional Clients Group
Citi

Naveed Sultan is a Managing Director and Chairman of Citi's Institutional Clients Group (ICG). With over 30 years of institutional banking experience, Mr. Sultan has been at Citi for over 26 years in a range of increasingly senior roles and is currently responsible for leading the digital policy, strategy, and advisory practice across all client segments. This practice advises governments in their development of policies to digitize their economies including their financial systems. It also provides guidance and thought leadership to corporates/financial institutions to transform their businesses/operating models to stay relevant in an increasingly digital world. In this role, he also engages in driving the developing markets strategy for Citi.

Q: Digital payments are driving out physical payments, so are we now entering an era of competition between different forms of digital payment?

This is the most exciting time to be in the payments business. There are some very different visions to digitize money with one of the fundamental questions moving forward being whether the future of payments will be conducted in tokens or accounts.

Q: What are the main theses you see playing out in the market?

There are four broad ways forward, each with their pros and cons:

- **Cryptocurrencies like Bitcoin:** Can they become scalable and transition from being speculative instruments to methods of payment?
- **Stablecoins:** Is it only volatility that prevents crypto from becoming a mass-market form of payment?
- **Central Bank Digital Currencies:** Is it a good idea to extend the usage of central bank money across the whole economy?
- **Development of Account-Based Systems:** Can payments be brought into the 21st century through the perfection of account-based payment?

Q: How do you evaluate the prospects of each of these options?

The big picture is that economies are rapidly digitizing and part of the vital infrastructure to enable digitization will be the removal of the remaining frictions in the payments plumbing. The question is what the best way to achieve that is.

The Bitcoin whitepaper has been around for a dozen years, but in that time the greatest digitization has been driven in account-based systems. We have seen hundreds of millions of people move into the formal system through e-money wallets in Asia and government initiatives in India.

However, there is growing discussion about the potential for tokenization to form the basis of future developments.

Q: What are the prospects for cryptocurrencies becoming dominant forms of payment?

At the moment classic Bitcoin is firmly in the realm of alternative investment. If people believe the price will go up, it is unlikely they will use the instrument as a method of payment.

Stablecoins, based on public blockchain, need to become legitimized within a regulatory perimeter. At the moment the use-cases are narrow and there is a grey zone about these instruments.

One important aspect is that the blockchain industry, primarily official exchanges, need to come up with a solution to the Financial Action Task Force (FATF) Travel rule and share data about payer/beneficiary — this information does not fit within existing blockchains.

Another point of concern is the presence of non-KYC'd wallets (non-'Know-Your-Client wallets), which can be vectors for financial crime.

Q: How about Big Tech stablecoins?

Big Techs operate vast global networks and have the potential to leverage those to embed payments and a host of financial activities. This is broadly to be welcomed. In the old days, banks built branches on the High Street or Main Street because that is where people congregated. Now people are on platforms, so that is where financial transactions will take place.

Regulation should be technologically neutral. If an e-money issuer needs to redeem balances at par value on demand, then it could be argued, so should a stablecoin issuer. If an e-money issuer cannot pay interest, then neither can a stablecoin issuer. Regulations should be neutral to the database technology employed to represent digital value. If stablecoins are considered a novel form of financial instrument by regulators, then we must avoid the danger of regulatory arbitrage against existing forms of digital value.

Q: Central bank digital currencies are much discussed…surely they are a silver bullet solution?

We should be extremely wary of silver bullets as they often have unintended consequences. Why is it that digital payments have taken over from physical? It is because there are thriving private markets in digital payments. There has been huge innovation and investment. CBDC could be a 'category killer' in digital payments and drive out private investment and development.

Having said that, a well-formed CBDC might play a role in the future of payments, but it will need to find its 'goldilocks zone'… too big and it will drive out the private sector. Too small and it will be immaterial from a policy perspective.

Q: Well, how about fixing the payments rails that we have? Is that possible or are account-based systems old hat?

Do not forget that account-based systems are based on a wonderful invention — double-entry bookkeeping. This was one of the great leaps forward of the Renaissance and I am not sure that we should roll back that advancement.

The fact is that national currencies are liabilities. In the form of central bank money, they are liabilities of the State. In the form of commercial bank money, they are liabilities of private sector entities that are heavily regulated. As long as money is a liability, then you need to record both sides of the transaction and double-entry bookkeeping is a great technology for doing that.

The development of instant domestic payments schemes, e-money wallets, digital identity, and real-time gross settlement (RTGS) systems will go a long way to delivering modern payments experiences.

Q: How about cross-border payments?

Some people claim that cryptocurrencies are perfect for cross-border payments, but they should pause. Some cryptocurrencies operate as bearer instruments on an anonymous basis. Unleashing these instruments for cross-border payments is not consistent with the fight against financial crime.

We should look into what SWIFT is doing to upgrade so-called 'correspondent banking'. This is a much maligned term, but is actually another advancement from the Renaissance. When a payment is sent from London to Jakarta, the issue is not the speed of the message between the banks. This takes place at the speed of light. The issue is whether the bank at the other side is online in the middle of the night and whether the RTGS is open for settlement in central bank money.

We are going to see banks progressively operate on a 24x365 basis and for SWIFT to interconnect them in a more interactive way. That is one way in which we can make international payments as easy as domestic payments, in a compliant way.

Q: Is there a silver bullet to fixing payments?

We need to go to the root cause and fix problems in the foundation. It is said payments equals identity plus accounting entries, and accounting entries are not the hard part. The fact is that good electronic payments is associated with good digital identity — we can see that in India and Sweden. In countries where there is an absence of good digital identity, developments are lagging.

It is not easy for a country to develop a national scheme, like India has, or a federated scheme like Itsme in Belgium or VerifiedMe in Canada. But this might be much more of a silver bullet than CBDC.

McKinsey cites countries can boost GDP by 3-13 percent going down this route, as digital ID is not just about payments, it is a foundational layer for the digital economy.

Q: What is your vision for payments in the coming 10 years?

We need to see payments in context, as part of the digital policy of governments. Governments are stretching the limits of monetary and fiscal policy, but there is a long way to go in the development of digital policy across all sectors of the economy. The development of digital payments is one arrow in the quiver of a coherent digital policy that can lead to measurable improvements in GDP.

Secondly, governments need to think of the entire 'payments stack' and optimize the whole rather than parts. Too often we see disconnected initiatives, equivalent to decorating the penthouse before central heating has been installed.

The way to get the best outcome for all economic actors will be through private/public partnership, where each plays their role. It should be the government that lays out technologically-neutral rules focused on underlying instruments rather than technology implementations while the private sector innovates and invests in new technologies to bring magical payment experiences to consumers and businesses.

This is an exciting time to be in payments, but we haven't seen anything yet. The benefits of digitizing economies lies before us like the peak of Everest, but we are barely in the foothills.

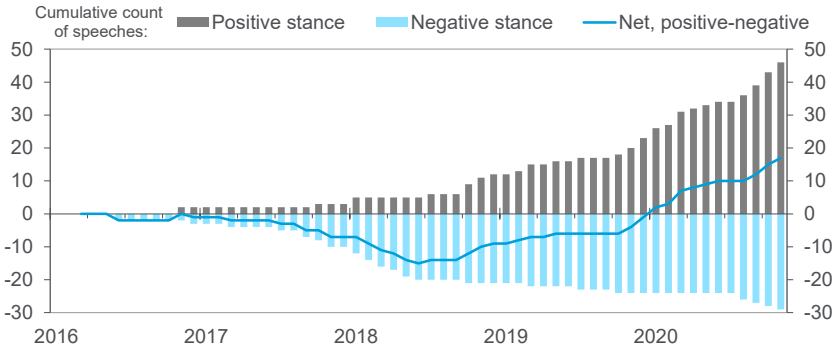
CBDCs: How They Work, Do We Need Them, and Risks.

- A 21st century digital money 'space race' is underway. The advanced work by China, the ambition of Big Tech (Diem and others), and the growth of crypto in general has accelerated work on central bank digital currencies (CBDCs).
- Central banks have moved from skepticism around CBDCs to engagement. In 2020, 86% of central banks said they did work on the topic, with 60% doing proof of concepts. However, only 14% are currently in pilot or development stage.
- Almost 60% of central banks say they may do a retail CBDC in the next one to six years, of which 30% believe they'll do one in the next three years. However, only 10% of central banks say they are "likely" to do so in the next one to three years, albeit that represents 20% of the world's population.
- Emerging market countries appear keener on CBDCs than developed markets, with China leading among the larger countries. China has been working on its CBDC since 2014-15 and has been piloting it in numerous cities during 2020-21.
- Having published its white paper in 2020, we expect the European Central Bank (ECB) to announce a Digital Euro pilot during the second quarter of 2021. U.S. policy makers, following the recent change in administration, are now much more interested in CBDCs.

Central Bankers Warming Up to (one form) of Digital Currencies

Central banks around the world have been researching the concept and design of digital currencies for years. Yet, it is only since 2019 that central banks began to warm up to CBDCs, as evidenced by the rise in number of positive mentions of retail and wholesale CBDCs in central bank speeches (Figure 12). It is more than a coincidence that the first Libra white paper was also issued in 2019.

Figure 12. Positive and Negative Stance of Central Banks on CBDCs (Number of Speeches)

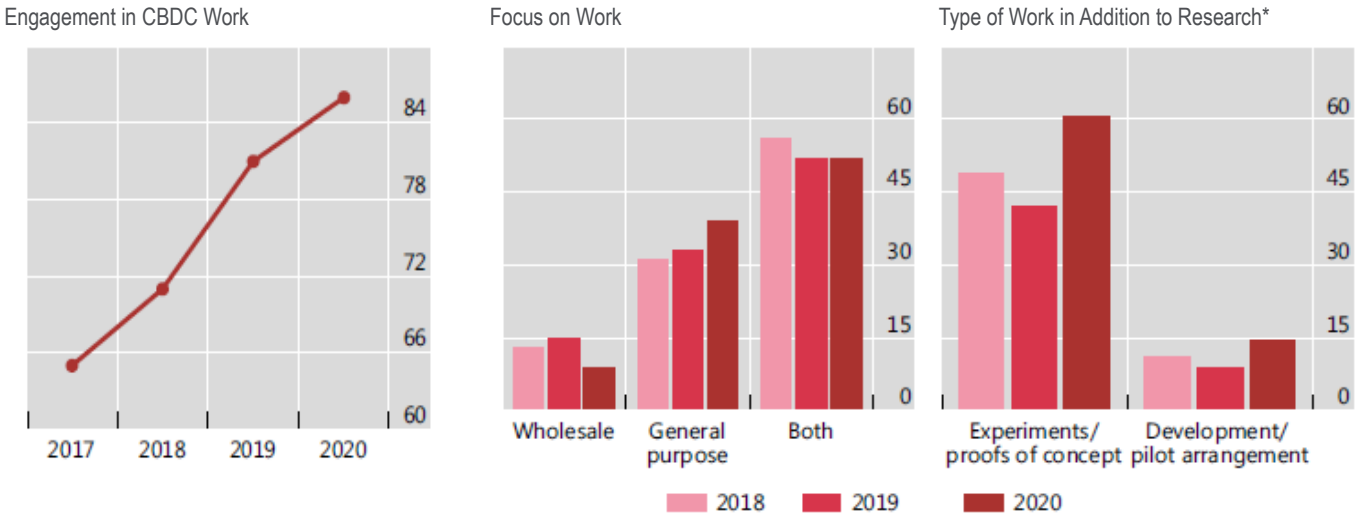


Search on keywords "CBDC", "digital currency" and "digital money". Classification based on the authors' judgment. Score takes a value of –1 if the speech stance was clearly negative or in case it was explicitly said that there was no specific plan at present to issue digital currencies. It takes a value of +1 if the speech stance was clearly positive or a project/pilot was launched or was in pipeline. Other speeches (not displayed) have been classified as neutral.

Source: BIS Working Paper "Rise of the central bank digital currencies: drivers, approaches and technologies". Material available freely at www.bis.org

Central banks across the world have advanced their engagement on CBDCs, progressing from discussion stages to experimentation. Results from the third BIS survey on CBDCs (published January 2021) shows that 86% of central banks are exploring potential benefits/shortcomings of CBDCs (versus 80% for 2019) and impressively almost 60% (versus 42% in 2019) are conducting experiments or proofs-of-concept, while 14% (versus 10% for 2019) are moving to development and pilot arrangements. Interestingly, wholesale CBDC appear to get less priority globally versus general purpose CBDC (Figure 13).

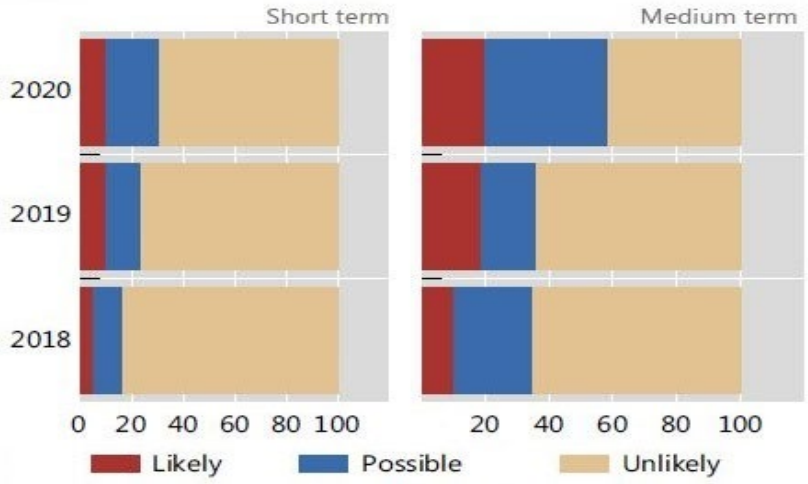
Figure 13. Increased Central Banks' Engagement on CBDC



Note: * share of respondents conducting work on CBDCs
Source: BIS Paper No. 114 titled "Ready, steady, go? Results of the third BIS survey on central bank digital currency". Material available freely at www.bis.org

The latest BIS survey shows that only 10% of central banks are “likely” to issue a general purpose CBDC in the next three years, albeit they represent 20% of the world’s population. A higher number of central banks (~60%) consider it a "possibility" over the short-to-medium term (e.g., 1-6 years).

Figure 14. Likelihood of Retail CBDC Issuance Continues to Increase (Share of Respondents)



Note: Short term: 1-3 years; Medium term: 1-6 years. "Likely" combines "very likely" and "somewhat likely". "Unlikely" combines "very unlikely" and "somewhat unlikely".
Source: BIS Paper No. 114 titled "Ready, steady, go? Results of the third BIS survey on central bank digital currency". Material available freely at www.bis.org

What Are CBDCs?

CBDCs are a digital form of central bank money that differs from balances in traditional reserve or settlement accounts. They are a digital payment instrument, denominated in the national unit of account that is a direct liability of the central bank.

The Bank of International Settlements (BIS) has provided a great taxonomy of money (Figure 15). The taxonomy distinguishes between two possible forms of CBDC — a widely available, consumer-facing payment instrument targeted at retail transactions and a restricted-access, digital settlement token for wholesale payment applications.

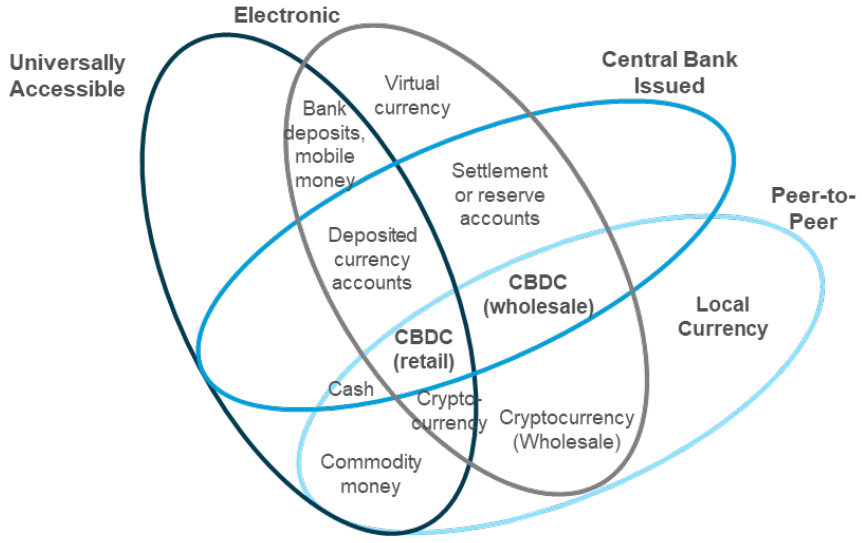
CBDCs are differentiated from other forms of central bank money such as cash and reserves as they can be exchanged in a decentralized manner, distinguishing them from other existing forms of electronic central bank money (such as reserves), which are exchanged in a centralized fashion across accounts at the central bank.

As far back as 2017, IMF Managing Director Christine Lagarde spoke at a Bank of England (BoE) event on how virtual currencies are among the top three factors that could change central banking over the next generation (the other two factors being new models of financial intermediation and Artificial Intelligence).

Ms. Lagarde saw countries with weak institutions and unstable national currencies readily adopting such virtual currencies — which she called "Dollarization 2.0". Taken to its logical conclusion, official-issued digital currencies could allow non-bank entities to hold an account directly with the central bank.

Banks could face the ultimate disintermediation, at least for client deposits. CBDCs in a maximalist form could be hugely disruptive for commercial banks' core client balances and cost of funding, and pose a threat to non-bank payment companies (i.e., FinTechs).

Figure 15. Money Flower? A Taxonomy of Money

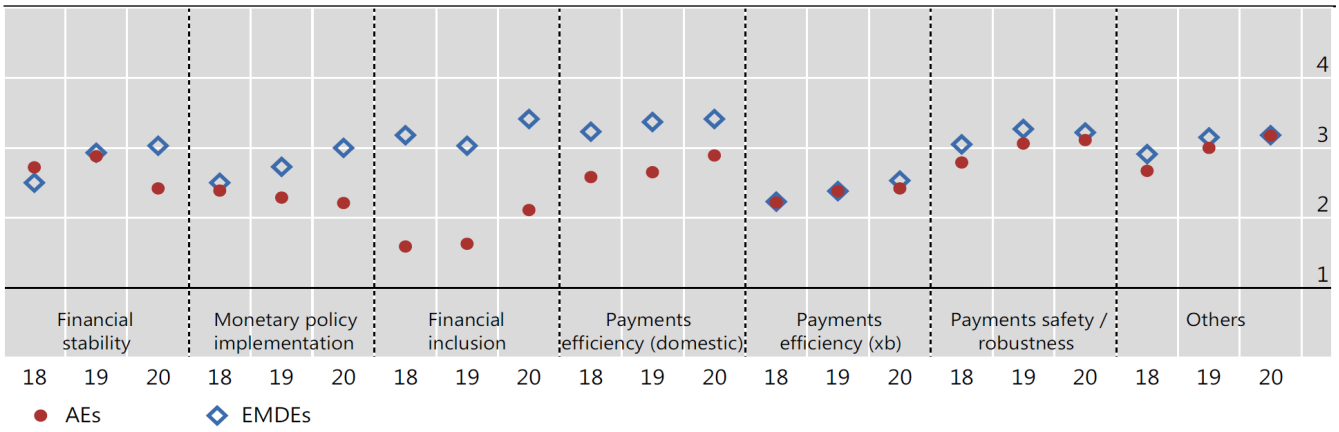


Source: BIS Quarterly Review "Central bank cryptocurrencies". Material available freely at www.bis.org

Motivation for a CBDC?

The BIS' third central banks' survey on CBDCs[7] in January 2021 suggests Emerging Markets and Developing Economies (EMDEs) report a higher motivation for issuing CBDCs versus Advanced Economies (AEs). Financial inclusion and domestic payment efficiency remain top motivators for CBDC development amongst EMDEs (Figure 16). By contrast, interim conclusions from studies in Hong Kong and Austria suggest limited need for retail CBDCs in countries with well-functioning electronic payments.

Figure 16. Motivations for Issuing a Retail CBDC

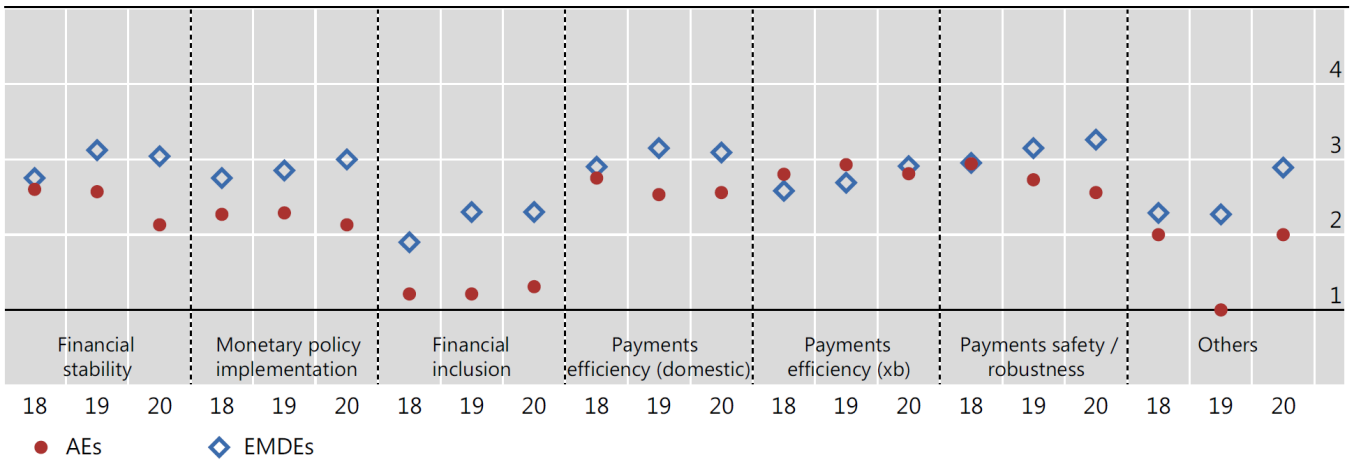


Note: (1) = Not so important; (2) = Somewhat important; (3) = Important; (4) = Very Important
AE = Advanced Economies; EMDE = Emerging Markets & Developing Economies
Source: BIS Paper No. 114 titled "Ready, steady, go? Results of the third BIS survey on central bank digital currency" Material available freely at www.bis.org

Further, the priority for wholesale CBDCs appears to be lower versus retail CBDCs globally, as reflected by the focus of ongoing central bank projects (Figure 13) as well as motivations to launch a wholesale CBDC (Figure 17). Potential motivation for wholesale CBDCs include the development of capital markets, enhancement of cyber resilience, and improvements in securities trading and settlement; albeit there could be some replication of functionality with current Real Time Gross Settlement (RTGS) systems.

[7] Codruta Boar and Andreas Wehrli, "BIS Papers No 114 Ready, steady, go? – Results of the third BIS survey on central bank digital currency", Monetary and Economic Department, BIS, January 2021.

Figure 17. Motivations for Issuing a Wholesale CBDC



Note: (1) = Not so important; (2) = Somewhat important; (3) = Important; (4) = Very Important.
AE = Advanced Economies; EMDE = Emerging Markets & Developing Economies
Source: BIS Paper No. 114 titled "Ready, steady, go? Results of the third BIS survey on central bank digital currency" Material available freely at www.bis.org

Types of Central Bank Digital Currencies

In terms of transaction purpose, CBDCs can be divided into wholesale CBDC and general-purpose CBDC. Both could improve payment safety and efficiency.

- **Wholesale CBDC:** In a domestic wholesale financial transaction, participants are limited to a central bank and mainly commercial banks — conducting interbank payments and settlements via reserve deposit balances in the central bank or setting up a segregated account and issuing a digital token for wholesale transactions.

  Global central banks think a wholesale CBDC could improve payment safety and efficiency, according to the BIS' survey. A wholesale CBDC may reduce operational costs, use of collateral, and liquidity in wholesale transactions.[8] A wholesale CBDC may eventually extend to cross-border transactions in future.

  However, a wholesale CBDC is a RTGS system built on distributed ledger technology (DLT). It remains to be seen what unique use-cases it would address versus account-based RTGS. For instance, RTGS renewal in the U.K. is proceeding on account-based infrastructure.

- **General-purpose CBDC:** This includes wider participants: commercial banks, firms, and individuals. Commercial banks may receive a certain amount of CBDC from a central bank and then distribute it to individuals' segregated accounts. General-purpose CBDCs could act as an alternative to cash or e-money.

[8] "Central bank digital currencies", Committee on Payments and Market Infrastructures & Markets Committee, BIS, March 2018.

Figure 18. Central Bank Digital Currencies Breakdown

	Wholesale CBDC	General-purpose CBDC
Token-based money (or Value-based CBDC)	**Wholesale transaction token:** e.g., Canada's Project Jasper, Singapore's Project Ubin, South Africa's Project Khokha, Thailand's Project Inthanon and Eurozone-Japan's Project Stella	**Retail transaction token:** e.g., Sweden's e-Krona (non-DLT) Uruguay's e-Peso PBOC's CBDC likely to fall into this category
Account-based money	**Institution segregated reserve account:**	**Individual segregated deposited account:** e.g., Sweden's e-Krona (non-DLT)

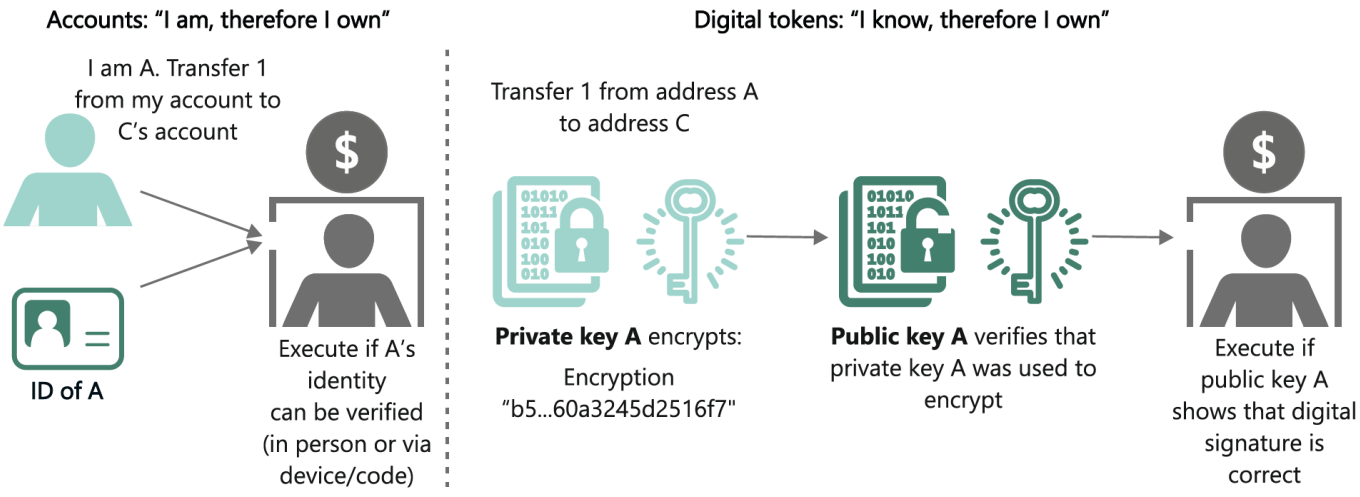
Notes: (1) This figure is based on Figure 10 and Table 2 of "Money and Central Bank Digital Currency", ADBI Working Paper Series No. 922 by Sayuri Shirai (Asian Development Bank Institute) in February 2019. (2) DLT refers to Distributed Ledger Technology.
Source: Citi Research

In terms of verification of payment, both token-based CBDC and account-based CBDC are possible (Figure 19). In payment economics, the way of verification distinguishes two kinds of payment systems: (1) store-of-value systems and (2) account-based system.[9]

Token-based CBDC: Coin, notes, and electronic stored value are examples of the store-of-value system. In a token-based CBDC, claims are honored based on demonstrated knowledge, e.g., digital signature. However, KYC'd wallets can also be used. Token-based CBDC are also called value-based CBDC.

Account-based CBDC: An intermediary verifies account holders identity for transactions, e.g., banking account and cards. In an account-based CBDC, ownership is tied to an identity, and transactions authorized via identification.

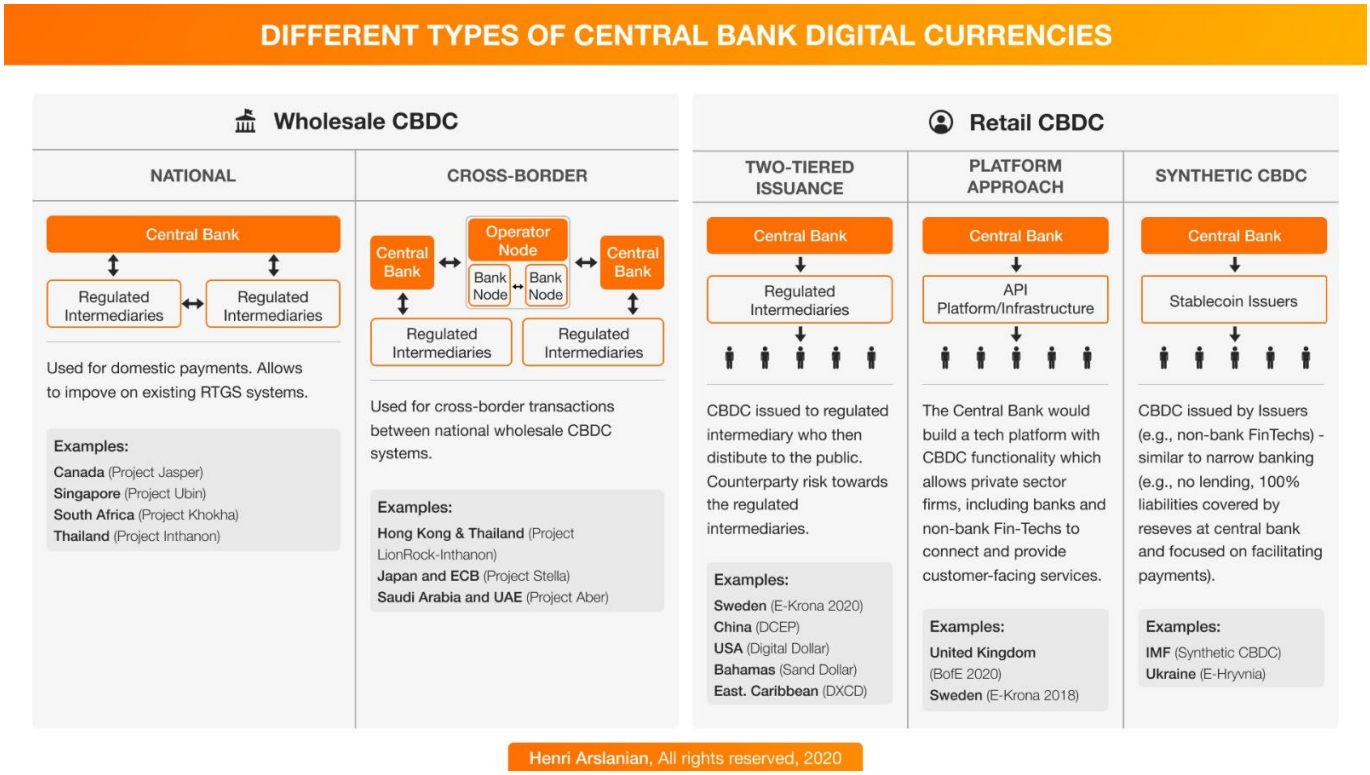
Figure 19. Account-Based Access Compared with Token-Based Access



Source: BIS speech titled "Digital currencies and the future of the monetary system" Material available freely at www.bis.org

[9] Christian Barontini and Henry Holden, "BIS Papers No 101 Proceeding with caution – a survey on central bank digital currency", Monetary and Economic Department, BIS, January 2019; Kahn, C and W Roberds (2009): "Why pay? An introduction to payments economics", Journal of Financial Intermediation, vol 18, no 3, January, pp 1–23.

Figure 20. Different Types of Central Bank Digital Currencies



Source: Henri Arslanian

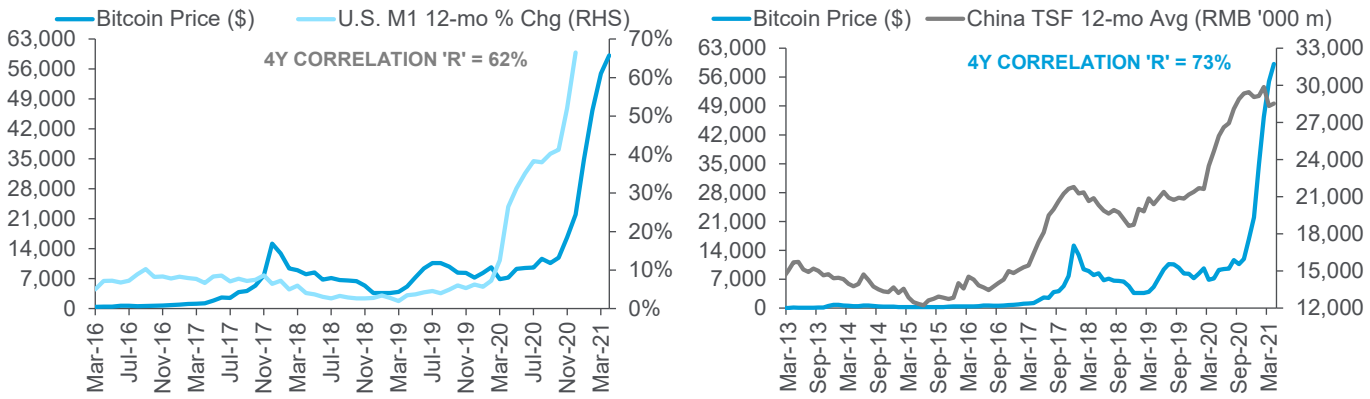
Investor Interest Rises in Private Digital Currencies

While most central bankers express skepticism around private cryptocurrencies, their prices rose rapidly during late 2020/early 2021. Bitcoin, which accounts for about 60% of total crypto value, increased nearly 3x from October 2020 to its all-time peak in March 2021.

The sharp price surge can be attributed to: (1) growth in money supply (M0 and M1); (2) people seeking to move money out of bonds into riskier assets (e.g., stocks, cryptos); and (3) debasement based on the narrative the U.S. dollar would lose value as the central bank prints more money.

Interestingly, there is also a good correlation between Bitcoin's price movements and China's 12-month average total social financing (TSF), or credit creation (Figure 21). Almost two-thirds or even more of Bitcoin mining and transactions in recent years have taken place in China.

Figure 21. Bitcoin Price (US$) versus U.S. Money Supply (M1) (12-mo % change) and China 12-mo Rolling TSF (RMB billion)



Source: coinmarektcap, DataStream, Citi Research

Bitcoins are often cited as being more commodity-like. Arguably, it is cyclical, relies on mining (process of solving a cryptographic puzzle), and has significant fixed cost. Notably, in 2015, the Commodity Futures Trading Commission (CFTC) classified Bitcoin as a commodity (link).

As with commodities, a supply/demand approach may be the best way to understand the valuation of Bitcoin and cryptocurrencies. Specific valuation approaches include: (1) mining cost, (2) stock-to-flow, and (3) comparison to gold. A more detailed analysis of valuation approaches can be found starting on page 66 of this report.

ECB White Paper on Digital Euro: Pluses and Minuses

In 2020, the European Central Bank (ECB) set up a High-Level Task Force on CBDCs, in an attempt to determine whether to launch a digital euro by mid-2021. In October 2020, the ECB published a comprehensive report on the potential issuance of a CBDC, i.e., digital euro (link). Potential drivers for issuance include:

- **Support digitalization of the economy:** Issuance of a digital form of central bank money could foster development of innovative payment solutions across the Euro-system, enhance digital efficiency while reducing costs of current payment ecosystem.
- **Reduced role of cash in payments:** The ECB paper argues that a decline in cash usage in the economy could imply increasing dependence on private forms of money and payment solutions. A digital euro, especially one with offline payments, could provide an alternative form of public money.
- **Pre-empt uptake of foreign currencies:** As several central banks and private tech firms develop payment solutions, wider acceptance of non-euro denominated alternatives, could impair transmission of monetary policy in the Euro Area and increase foreign exchange risk. The issuance of a digital euro could support European sovereignty and stability.
- **Greater monetary policy control:** A digital euro could reinforce monetary policy transmission by allowing the central bank to set the remuneration rate on the digital euro, thereby influencing the consumption/investment choices of the non-financial sector.

- **Mitigate cybersecurity/natural risks, alternate payment solution:** Financial transactions/payments are prone to cybersecurity and natural disaster risk, which could disrupt cash/traditional payments infrastructure. Co-existence of a digital euro could provide a contingency mechanism for e-payments.

Issuing CBDCs is likely to have potential effects on existing monetary and payments ecosystem that need to be carefully considered and managed. In its study on the potential issuance of a digital euro (link), the ECB highlights a few key consequences.

- **Effects on banking sector, monetary policy and financial stability:** Issuance of CBDCs could potentially exacerbate risk related to monetary policy transmission by challenging banks' intermediation capacity and affecting risk-free rates. A CBDC could induce depositors to move commercial bank deposits to central bank liabilities, rising funding costs and adversely impacting financial stability. However, to cope with this, banks could stabilize deposits by bundling them with additional services (e.g., payments services, mortgages) or replacing lost deposit funding with central bank borrowings.

- **Potential impact on safety/efficiency of retail payments:** Issuance of CBDCs would inevitably lead to the introduction of a new end-user solution in an already crowded retail payments space. Central banks need to consider efficiency and usability of such offerings and create a standard interoperable solution for users.

- **Cross-border use:** Wide circulation of digital currencies outside the primary market could have significant implications for capital flows and exchange rate of fiat currencies. For example, the rebalancing of portfolios by non-Euro Area residents towards the digital euro, could adversely increase the size of risk of the Euro-system balance sheet.

The public consultation on a digital euro by the ECB, following their white paper, ended January 12, 2021 and responses are now being processed. Christine Lagarde, ECB President said: “It is only in Spring, probably in April, that we will determine whether or not to go ahead with the work that will need to be done”.

The next step would be a pilot project. Given the positive mood music on the subject from President Lagarde, we expect work towards a pilot project for the digital euro to be launched soon. However, even if the ECB decides to launch a proof of concept, President Lagarde has warned that the roll out of a digital euro “will take a number of years”.

U.S. policy makers, who have been previously less enthusiastic on the topic, are also warming up. Treasury Secretary Janet Yellen recently noted “it makes sense for central banks to be looking at” issuing sovereign digital currencies (Bloomberg, February 22, 2021).

In the words of Secretary Yellen: “Too many Americans don’t have access to easy payments systems and banking accounts, and I think this is something that a digital dollar, a central bank digital currency, could help … it could result in faster, safer, and cheaper payments, which I think are important goals.”

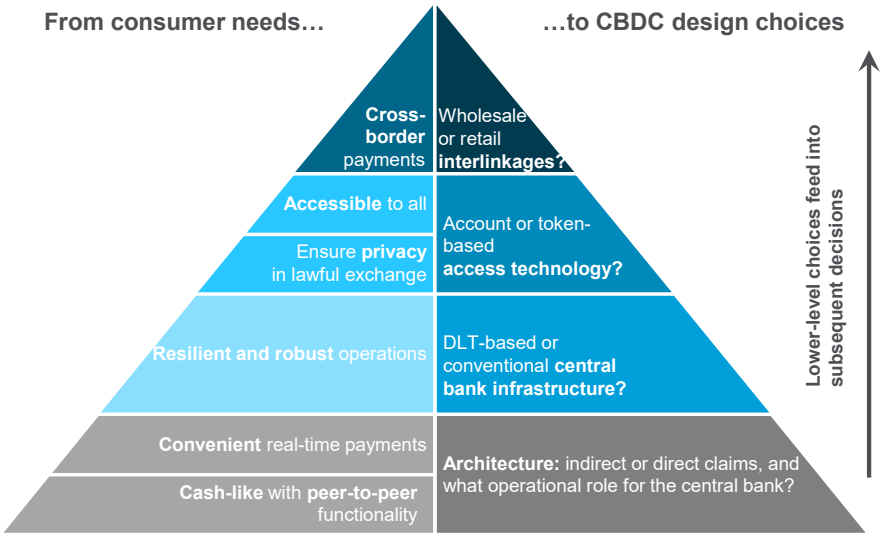
U.S. Federal Reserve Chairman Jonathan Powell has noted that work on a digital dollar is “a high priority” (Forbes, February 23, 2021). “We are looking carefully, very carefully, at the question of whether we should issue a digital dollar,” Equally, Fed Chairman Powell has cautioned it is better to get this right than be fast or first.

Approaches to CBDC Design

So what is the best way to design sovereign-issued digital currencies? According to the BIS Working Paper No. 880 "Rise of the central bank digital currencies: drivers, approaches and technologies" (August 2020), the approach to CBDC design is heterogeneous across countries.

One way to classify the design approach is using the CBDC pyramid set out in Figure 22. Under this approach, one starts by identifying the consumer needs a retail CBDC should address. It then identifies associated technical design trade-offs and derives design choices.

Figure 22. The CBDC Pyramid



The CBDC pyramid maps consumer needs onto the associated design choices for the central bank. The left-hand side of the CBDC pyramid sets out the consumer needs and associated features that would make a CBDC useful. The pyramid's right-hand side lays out the associated trade-off – forming a hierarchy in which the lower layers represent design choices that feed into subsequent, higher-level decisions.
Source: BIS Working Paper "Rise of the central bank digital currencies: drivers, approaches and technologies" Material available freely at www.bis.org

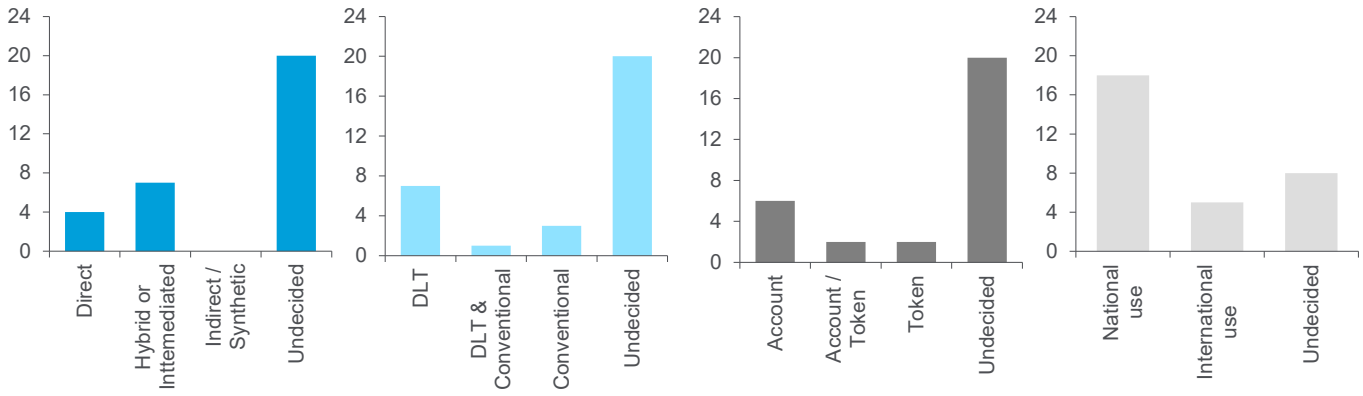
Some of the key elements of the CBDC pyramid include:

- **Architecture:** Defines the operational role taken by the central bank and private intermediaries on CBDC. Architectures could differ based on the structure of legal claims and the record kept by the central bank and can be summarized into: Direct, Hybrid, Intermediated, and Indirect CBDCs.
- **Infrastructure:** Ensures the CBDC is secure from outages at the central bank. Keeping this in mind, the CBDC infrastructure can be based on a conventional centralized database or DLT. Their key differences lie in their efficiency and degree of protection from single points of failure.
- **Access:** Determines how customers can access CBDCs. Account-based CBDCs are tied to an identity scheme and can form basis for a well-functioning payments. Meanwhile, CBDCs based on digital tokens are more appropriate for the unbanked and individuals who rely on cash.

- **Retail and Wholesale Interlinkages:** Relates to the use of CBDCs for cross-border payments and its accessibility for residents versus non-residents.

Figure 23 below classifies the attributes of ongoing retail CBDC projects across the four elements of the CBDC pyramid.

Figure 23. Number of Retail CBDC Projects Investigating Each Design Option



Source: BIS Working Paper "Rise of the central bank digital currencies: drivers, approaches and technologies", Citi Research Material available freely at www.bis.org

Risks and Concerns

Legal Bottlenecks

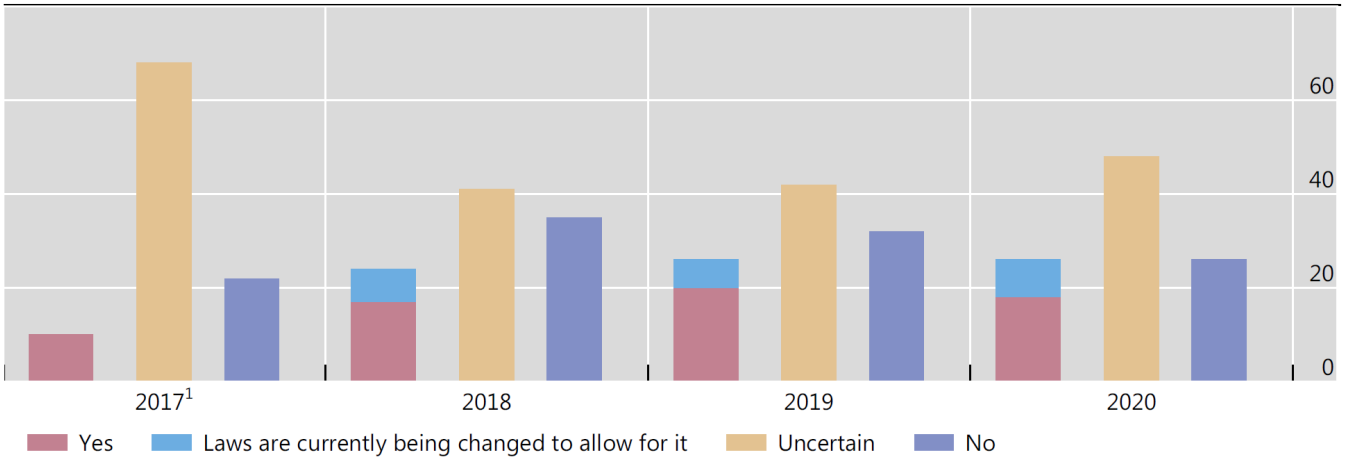
According to an IMF study[10] highlighting legal aspects of CBDCs, in order for CBDCs to be launched, there needs to be: (1) robust legal foundations that ensure smooth integration to financial systems; (2) credibility; and (3) broad acceptance by people and economic agents.

After all, any money issuance is a form of debt for central banks, and it must have a solid basis to avoid legal, financial, and reputational risks for institutions. However, according to the IMF, under existing central bank laws nearly 80% of the world's central banks are either not allowed to issue a digital currency or the legal framework is not clear. **Only about 40 central banks are legally allowed to issue digital currencies.**

According to a BIS central bank survey on CBDCs in January 2021, there has been a rise in central banks having legal authority to issue CBDCs, albeit with nearly 74% of the respondents still either not having legal authority or unsure, it suggests most central banks have not advanced much beyond pilot stages (see Figure 24).

[10] IMF Working Paper, Legal Aspects of Central Bank Digital Currency: Central Bank and Monetary Law Considerations, November 2020.

Figure 24. Legal Authority of Central Banks to Issue a CBDC (Share of Respondents)



[1] The 2017 central bank survey did not have an option for "laws are currently being changed to allow for it"
Source: BIS Paper No. 114 titled "Ready, steady, go? – Results on the third BIS survey on central bank digital currency"
Material available freely at www.bis.org

Status of Legal Tender

A currency typically enjoys legal tender status and is usually only given to means of payment that can be easily received and used by the majority of the population. That is why banknotes and coins are the most common form of currency. To legally qualify as currency, a means of payment must be considered widely usable.

Account vs. Token Based

Digital currencies can take different forms. They could be 'account-based' or 'token-based'. From a legal perspective, the difference is between centuries-old traditions and uncharted waters. The first model is as old as central banking itself. Account-based CBDC is digitalizing balances held on accounts in central bank books.

Token-based CBDC is akin to designing a new digital token not connected to existing accounts held by commercial banks with the central bank. Some central banks are allowed to issue any type of currency (including digital forms), **while 61% central banks are limited to banknotes and coins.**

Wholesale vs. Retail CBDCs

Commercial banks hold accounts with their central bank. Allowing private citizens' accounts would be a tectonic shift to how central banks are organized and would require significant legal changes. **Only 10 central banks in IMF's sample study would currently be allowed to do so.**

CBDCs and the Question of Anonymity

Digitalization of the payments ecosystem requires balance between a certain degree of privacy in electronic payments and ensuring compliance with Anti-Money Laundering/Combatting the Financing of Terrorism (AML/CFT) regulations. If a user can hold CBDCs in its wallet only after KYC, this means there is a loss of anonymity. Currently, tech-builders choose the level and degree of anonymity in the ecosystem whereas it is society who should draw the line with the technology being built in accordance.

The ECB and ESCB (European System of Central Banks) in coordination, as part of their study on CBDCs, have published a proof of concept for anonymity in CBDCs[11] suggesting a construct that allows users privacy for lower value transactions, whilst subjecting higher value transactions to mandatory AML/CFT checks.

The paper highlights introduction of new 'anonymity vouchers' issued by the AML authority, offering time-limited states to CBDC users for anonymous transfers. A user desirous of transferring CBDCs, without revealing his/her personal information to the AML authority, can simply avail the use of such vouchers. Additionally, privacy could also be further enhanced by the use of rotating public keys, zero-knowledge proof, and enclave computing.

While the ECB paper highlights the possibility of anonymous CBDC transfers, it also highlights areas where there is room for improvement. These include: (1) reducing the amount of information visible to parties not involved in the transaction; (2) users' ability to access or spend CBDC balance when the intermediary is unavailable; and (3) interoperability with an RTGS system.

CBDCs, Deposits, and Disintermediation

Sovereign-issued digital currencies would be an attractive asset for end clients as it would be a direct liability of the central bank and hence have lower counterparty risk relative to commercial banks. CBDC in a maximalist version would shift commercial bank deposits to central bank liabilities, raising bank funding costs and volatility.

Risk to financial stability can be mitigated by a 'two-tiered' CBDC system, where the central bank issues CBDCs to commercial banks who hold them under custody for clients (albeit the liability still remains with the central bank). We assume most large countries will use a two-tier model.

However, even in a two-tier model, commercial banks could see liquid deposits that can be used to fund loans, partly replaced by 'assets under custody' (CBDCs) that cannot be re-lent. This could reduce commercial bank money creation and the growth of credit in the economy.

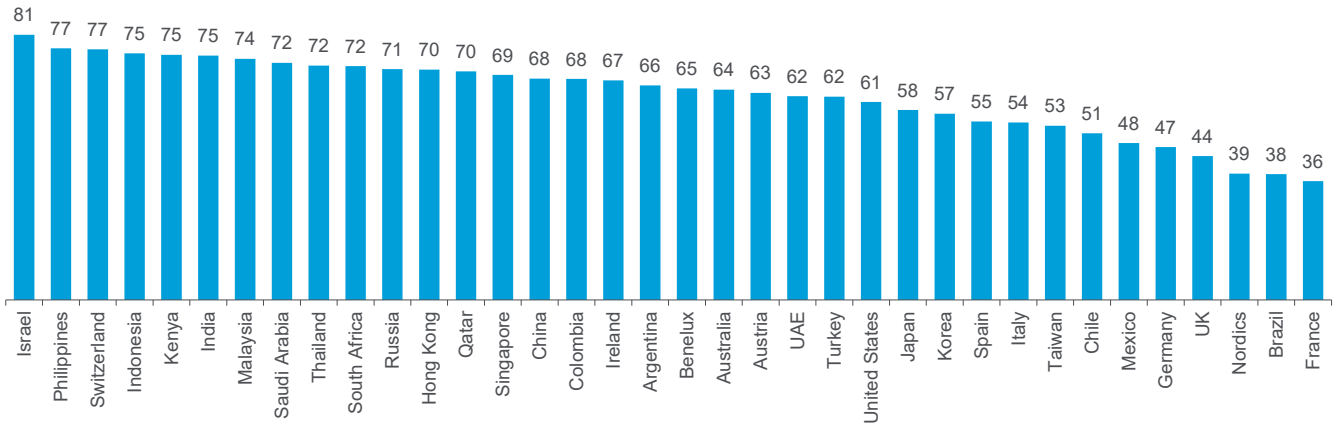
Banks could make client deposits stickier by bundling them with additional services (e.g., payments, mortgages). For larger banks, in the U.S. and many markets, client deposit scarcity is not really an issue. Low/negative interest rates and quantitative easing has left commercial banks with too many deposits.

Figure 25 and Figure 26 compare size of banking sector deposits across key markets. Those with higher banking deposits could be at higher risk should there be an outflow of bank deposits into central banks' digital money. For example, the U.S. and Japanese banks rely much more on deposits to fund loans versus the Nordic banks.

Emerging market banks, especially in Asia, Middle East and Africa, have a large part of their assets funded by client deposits (asset bases are more loan based in these countries). And with weak or non-existent deposit insurance schemes in some of these country, the credit preference for central bank direct deposits will be high.

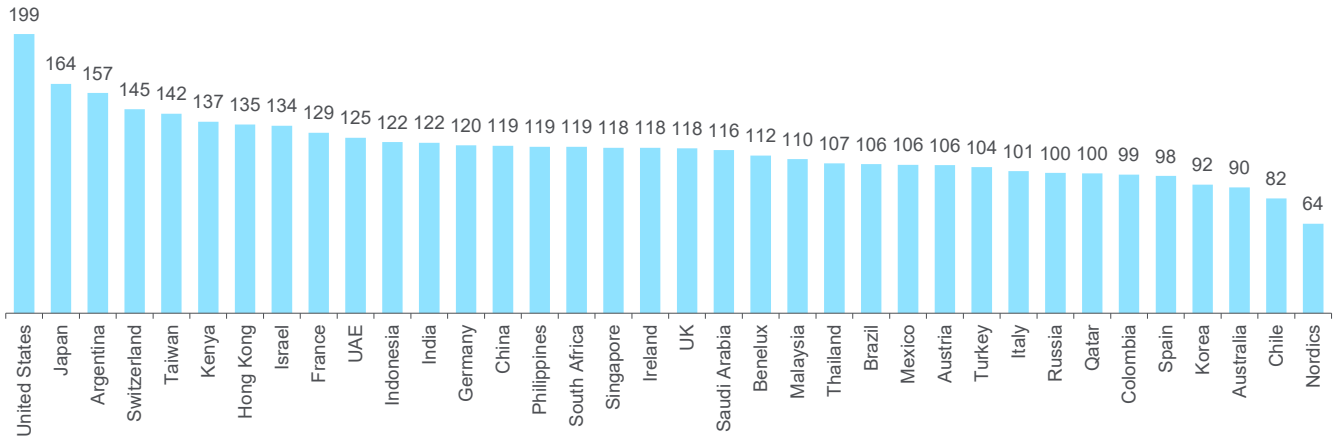
[11] European Central Bank, Issue no. 4, "Exploring anonymity in central bank digital currencies", December 2019.

Figure 25. Key Banking Sectors: Deposit/Assets, 2020



Note: Calculated bottom-up for a variety of banks under Citi Research coverage
Source: Citi Research

Figure 26. Key Banking Sectors: Deposits/Loans, 2020



Note: Calculated bottom-up for a variety of banks under Citi Research coverage
Source: Citi Research

Citi View on CBDCs: Andres Wolberg-Stok

Andres Wolberg-Stok
Head of Strategy, Chief Technology Office
Citi

Andres Wolberg-Stok is the Head of Strategy in Citi's Chief Technology Office. He leverages his experience on the front lines of digital innovation to focus on the path ahead for the firm, and to interface with regulators and policy makers around the world on digital assets, AI/ML, Open Banking, and other forward domains.

At a Glance

1. Digital currency in general should be broadly accessible, transferrable in real-time and 'always on'.

2. CBDCs present opportunities and risks. Direct access to central bank money by non-banks and individuals could affect the deposits banks need to extend credit, thus hurting growth and jobs.

3. CBDCs require many design choices, such as tokens versus accounts, wholesale versus general purpose, or single-tier versus two-tier. We highlight a number of those fundamental options in this position paper.

4. Officials should also balance public and private implementations, central bank money versus commercial bank money, and privacy versus transparency. Interoperability cannot be an afterthought.

5. Precisely how CBDCs are designed will have major consequences.

Introduction

The further digitization of currency and payments is inevitable and central banks will play an important role in driving innovation.

Digital currency in general should be broadly accessible, transferrable in real-time and 'always on'. It should accommodate the needs of emerging forms of commerce like Internet of Things (IoT), support micropayments, enhance wholesale securities settlement, and integrate with other digital platforms for the benefit of consumers and corporates. There should be a thriving private market in digital payments with high levels of innovation, competition, and investment. There are multiple routes to reaching these objectives.

CBDCs may help achieve these goals — or detract from them — depending on how they are designed and implemented. Policy makers and all other stakeholders should consider the potential development of CBDCs alongside other means to augment payment systems, such as the development of 24x7 Real Time Gross Settlement (RTGS) systems.

Opportunities and Risks

The development of CBDCs presents a range of potential opportunities and risks. Policy makers are rightly weighing up the potential for technological innovation in the issuance of national currency versus the impacts on private financial markets.

CBDCs may lead to direct access to central bank money by non-banks and individuals, reducing the deposits on which banks rely to extend credit, and crowding out private investment and innovation in payment systems. Private credit creation is fundamental to economic growth, job creation, and social mobility. Private payment systems foster innovation and ensure greater resilience through diversification of platforms.

There are many design considerations for creating a CBDC, both technological and structural. Due to the centrality of currency and payments in the economy, unintended consequences are a risk. In order to be effective, CBDCs must strike a balance between:

- Public infrastructure and private sector solutions;
- The roles of central bank money and of commercial bank money; and
- Expanded access to digital money and the risk of financial crime.

CBDCs Design Choices

Citi is keen to actively engage with central banks in the design of CBDCs, given that choices made in the formative stages could have significant ramifications:

- CBDCs could be issued using KYC'd accounts powered by existing technology, tokenized bearer instruments enabled by DLT, or a combination.
- Account-based solutions are familiar, mature, and well suited for the prevention of illicit activity.
- Tokenized solutions that are available to the general public may expand access and may offer enhanced privacy, depending on their design, but at the cost of greater illicit use. Digital bearer assets are more programmable, but come with greater risk of loss/theft, which could defeat the benefits of financial inclusion. Such assets require additional infrastructure, such as wallets, for usability and consumer protection, but that will add a new layer of intermediation.
- Account-based solutions are proven at scale and have built resilience through experience. They are already integrated into existing financial markets.
- Tokenized solutions offer easier integration into other DLT-based platforms and markets, but the technology is still emerging.

Given how many major jurisdictions are exploring potential CBDCs in parallel, it is critical that they take into account the need for global interoperability. Digitization of any kind has the potential to expand access beyond borders, and interoperability cannot be an afterthought.

Citi puts its extensive practical experience in global payments at the disposal of regulators as they ponder the broad range of design choices facing them in the formative stages of CBDCs.

Systemic Implications

Money has historically existed in both public and private forms, and most of the fiat currency in circulation today is commercial bank money. If the introduction of CBDCs increases the proportion of central bank money, there could be an incipient nationalization of credit, hampering economic growth and impeding innovation. In a currency crisis, universal access to central bank money from other jurisdictions could fuel domestic bank runs and cross-border capital flight.

Payment systems work best as public-private partnerships, and payments with CBDCs should not be an exception. Crowding out the private sector would stifle innovation and put central banks in the undesirable and onerous position of providing customer support, conducting Know-Your-Customer (KYC) procedures, and enforcing Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) regulations.

A wholesale CBDC does not need to be universally versatile. It could be engineered solely for use in domains where it would add clear value, such as tokenized capital markets, where the alternative would be private stablecoins with greater credit risk and market risk.

Expansion of access to digital payments cannot be achieved with CBDCs alone, regardless of their design. Laws and regulations need to be updated, and doing so should be done in a technologically neutral way.

External Expert View: Henri Arslanian on CBDC

Henri Arslanian
Global Crypto Leader
PwC

Henri Arslanian is the PwC Global Crypto Leader, the former Chairman of the FinTech Association of Hong Kong, and an Adjunct Professor at the University of Hong Kong. Henri advises many of the world's leading crypto exchanges, investors, financial institutions, and tech firms on their FinTech and crypto initiatives as well numerous governments, regulators and central banks on FinTech and crypto regulatory and policy matters.

Q: Central bank digital currency has become prime-time in policy discussions recently, why?

I am very fortunate to have the opportunity to advise not only several regulators, governments, and central banks, but also many large financial institutions.

I remember three to four years ago, when I would discuss the topic of CBDCs, I used to get laughed at in many cases. The biggest short-term impact of Libra/Diem was definitely that it catalyzed the conversations around CBDCs.

When we talk about CBDCs, it is really important we take a step back and try to understand the landscape. If we look at CBDCs, there are two types of central bank digital currencies — wholesale CBDCs and retail CBDCs.

Wholesale CBDCs are issued by the central bank, but operate between the central bank and member banks. The public does not touch wholesale CBDC. By contrast, retail CBDC is a digital currency accessed by the public, like a digital banknote. Retail CBDCs can have a significant impact on the financial services ecosystem.

We can segregate wholesale CBDC into two — the first is national wholesale CBDC, which is the use of wholesale CBDC within a country. Although there are pilots, their impact is likely to be limited as many countries already have well operating national payment systems like Real Time Gross Settlement (RTGS) networks. Although they may not be perfect, they work fine. So there is not much urgency there.

The second category of wholesale CBDC are cross-border CBDCs, which although more complicated, are interesting as the system today has a lot of flaws, with a clunky network of correspondent banks and legacy systems. This is one area a lot of central banks have been trying to explore if they can improve with CBDCs.

However, CBDCs are likely to have a bigger impact at the second type — retail CBDC. Within retail CBDCs, we have three main categories.

First is a two-tiered retail CBDC. In such a case, the central bank issues a retail CBDC, but it is issued via regulated intermediaries, e.g., banks. As a result, it does not disintermediate banks. It is similar to how things operate today, with the exception that the public has access to a digital form of central bank money (same way banks distribute physical banknotes via an ATM). China, the Bahamas, and some pilots in Sweden are good examples of a two-tier retail CBDC.

The second model is synthetic CBDCs, where the central bank allows tech firms and others access to a central bank account. These firms can issue stablecoins backed by central bank reserves. Unlike a bank and a fractional banking model, these stablecoins are backed 100% with reserves at the central bank.

This idea was advanced by the IMF two years ago and is not too dissimilar to the debate that took place in the U.S. around narrow banking a couple of years back.

The third form of retail CBDC is when the central bank works to create a tech platform allowing banks and non-bank FinTechs to participate. The Bank of England and even Sweden's Riksbank were leaning towards such a model.

I would argue from all the experiments we are seeing today, the one we may see in practice is probably the first model, i.e., two-tiered issuance where banks still play a role in the ecosystem, and are not completely disintermediated. This approach provides access to central bank money to the public, while causing the least risk of financial instability, which is something every central bank cares about.

Q: Is retail CBDC direct issuance unlikely to happen simply because of its potentially huge disruptive effect?

Issuance of a retail CBDC has some risks, for example, in the event of financial instability it would be potentially easier for people to withdraw all their digital assets (i.e., retail CBDC) from a bank and hold them seamlessly on their digital wallet. This is not possible today as there are physical limits to how much money you can withdraw from an ATM and how you can secure it.

From a commercial perspective, the risk is that people prefer to keep retail CBDC in their personal wallets instead of a bank (e.g., low interest environment or during times of financial instability). In such a case, banks may need to get funding elsewhere, as it does not have access to regular pools of cheap customer deposits and this could impact revenues.

However, there are easy safeguards against these risks. Central banks may limit the maximum amount someone can hold in retail CBDC in a digital wallet — this was an idea put forward by the Dutch Central Bank in 2020. Or they can offer an interest rate on CBDC that is lower than that for traditional bank account deposits.

Reality is, central banks know they have an obligation to provide public access to central bank money. In a world where less cash is being used for payments, CBDCs may be a way forward and central banks are right to explore this topic actively.

Q: What is the use-case for CBDCs?

I believe if you are central banker today and you love Bitcoin, you are crazy. It is a bit like the taxi driver being excited to see Uber come in their market.

That being said, many central banks have realized the benefits of CBDCs. One of them is that it allows us to move value almost instantaneously, 24x7, for nearly free. A good use-case is cross-border payments. Today, the average fee for cross-border payments is around 7%. We have nearly 250 million people across the world sending over $500 billion in cross-border remittances annually, and the fees are extremely high. It is embarrassing that we have not solved this issue so far.

Another benefit is traceability and transparency. Unlike cash, digital currency transactions are public. While there is a potential debate on privacy in payments (that we should have), reality is that CBDCs give us a fighting chance against money laundering and illicit activities. There is a lot of money laundered through existing system and, despite our best efforts, we are able to capture less than 1-2% of laundered transactions. Retail CBDCs may not eliminate the problem, but give us a fighting chance against corruption/money laundering. Same applies to combatting the black economy and tax avoidance, which becomes difficult in a CBDC economy.

There are benefits for policy-making as well. If we were in a CBDC-based economy, I could measure the impact of my policies in a more scientific way than today, as I could see in almost real-time the economic activity in my country. It enables many possibilities. For example, a potential feature of retail CBDC is programmable money, whereby you can embed positive/negative interest rates within the digital currency. This opens up new opportunities that policy makers simply cannot today.

Q: Can we talk about the Chinese plans for their CBDC?

I always tell my clients that if they want to see the future of finance, they should head to Shanghai or Shenzhen, not New York or Silicon Valley. When it comes to blockchain technology, I would argue China is extremely advanced, way more than many in the West believe. China, right now, has the second greatest number of patents globally on blockchain technology.

When it comes to the future of money, China is also years ahead of any other major economy. Whilst many countries are starting to explore the topic now, the Chinese central bank (PBOC), has been working on this since 2014. They accelerated the process after the announcement of Libra (Diem) and of course, COVID-19.

The digital yuan, often referred to as DCEP, e-RMB or e-CNY, is going to be quite scalable. They have announced plans of over 300,000 transactions per second. They plan to distribute this via commercial banks and tech firms, i.e., intermediaries, such as in a two-tier retail CBDC system. A pilot was launched in 2020 in four cities (Shenzhen, Chengdu, Suzhou and Xiong'an), which has been extended since. Over RMB2 billion (~$300m) have been transacted so far in over 12,000 use-cases.

The country you need to watch over the coming months, in context of retail CBDC and the future of money more broadly, is definitely China.

Q: COVID-19 is often referred to as the great accelerator. Did COVID-19 help accelerate CBDC efforts in practice, internationally?

I believe COVID-19 is a big accelerator for the future of money. While declining cash usage has been an ongoing trend, recent data suggest an acceleration in decline of cash for payments. For instance, several merchants have been refusing to accept cash lately, due to safety reasons and fears it may transmit COVID-19.

According to the Riksbank, only about 1% of Sweden's GDP is transacted in cash. Based on a survey conducted before the COVID-19 outbreak, several retailers opined that in less than 60 months they would refuse accepting cash altogether. I would argue that the pace is likely to be much more accelerated.

CBDCs could also help solve some of the inherent problems faced by us today. For instance, the U.S. is finding it very difficult to send stimuli checks to its citizens in these unprecedented times. Frankly, it is a bit laughable that in 2020, with all the technological tools available to us, we are still reliant on mailing checks.

Across developed markets too, we have a sizeable portion of unbanked. In the U.S. alone, about 7% are unbanked and the number potentially rises to as much as 20% in select cities. Can you imagine benefits of having a digital wallet/dollar?

Ironically, while there is a decline in the usage of cash for payments, there is a record level of banknotes in circulation today, as people in many countries are hoarding cash. This happens often in times of crisis. This reinforces the need for the central bank to find ways to give the public access to central bank money. A digital form of central bank money is probably the way forward.

China: Deep Dive into DCEP

- China's PBOC is a global leader in CBDCs with the development of their Digital Currency Electronic Payment (DCEP) which started in 2014 and is progressing to retail pilot testing in 2020-21.
- Retail usage of DCEP has now been trialed in half a dozen cities and we expect this to widen further to new cities and also rural areas during 2021. In addition, trials are expanding from smartphone to hardware-based e-wallets.
- DCEP is slowly permeating into the monetary base in China. Pilots that have taken place are moving material amounts of money: the latest data shows $300 billion cumulatively through November 2020.
- We expect fast adoption of DCEP over the next five years relative to other CBDCs, supported by China's sprint to a cashless society — mobile payment volumes reached RMB314 trillion in the first nine months of 2020 (135x above 2012 levels), or 10.7% of non-cash volume (versus 0.2% in 2012), according to the PBOC.
- Financial inclusion is a primary use cases for DCEP. It will be mandatory to accept DCEP, unlike private e-money and it will support double offline payments and controlled anonymity (with provisions for AML etc.)
- Wider DCEP adoption has implications on regulatory efficiency and monetary policy, especially as it helps lower currency issuance costs, assists in targeted monetary policy implementation and RMB internationalization.
- This chapter details DCEP's history, key milestones in development, technical aspects and implementation details, domestic implications on monetary policy, banking ecosystem etc. and wider/global ramifications.

A Look at China's DCEP

The People's Bank of China (PBOC) first unveiled a plan to launch its own CBDC, known as Digital Currency Electronic Payment (DCEP), in early 2018, but its research work on DCEP started in 2014. It established an internal research organization, the Institute of Digital Money, in September 2016.

In December 2016, the PBOC and commercial banks experimented with trading of digital commercial paper with CBDC. It was reportedly one of the first attempts amongst global central banks in the world.[12]

An overview of the key DCEP milestones is set out in Figure 27 below, including retail pilot testing in 2020-21.

[12] "China's Central Bank Has Begun Cautiously Testing a Digital Currency", June 2017, MIT Technology Review.

Figure 27. Key Milestones in the Development of China's Central Bank Digital Currency

Time	Institution(s)/ Involved	Event
2014	PBOC	Set up a dedicated team to explore launching a Central Bank Digital Currency.
2015	PBOC	Published a series report on CBDC; Completed two rounds of revisions on the initial design of CBDC.
Jan. 2016	PBOC	Confirmed to launch CBDC and clarified the strategic goals for CBDC launch.
Sep. 2016	PBOC	Established an internal research organization, the Digital Currency Research Institute.
Nov. 2016	PBOC	Selected electronic commercial bill ('e-bill') market as a pilot closed-application scenario for CBDC and started development work of the trading platform.
Nov. 2016	PBOC	Announced plan to hire six blockchain experts to work in the Digital Currency Research Institute of PBOC.
Dec. 2016	PBOC, Commercial bank	Experimented with trading of digital commercial paper with CBDC.
Feb. 2017	Digital Currency Research Institute of PBOC (DCRI)	DCRI successfully tested blockchain-based e-bill trading platform; DCRI joined Shanghai Commercial Paper exchange to lead the e-bill trading platform development project, joined by China banknote and credit card development co (中钞信用卡产业发展有限公司), ICBC, BOC, SPDB and Bank of Hangzhou; In February 2018, the e-bill trading platform completed its first successful trial run.
Jun. 2017	PBOC, DCRI of PBOC	PBOC officially founded DCRI in Beijing, concentrating its research efforts on the legal framework of digital currency, blockchain technology, and IC design etc.
Mar. 2018	PBOC	Former PBOC Chief Zhou Xiaochuan said during the 2018 National Currency, Gold, and Silver work conference that research & development of CBDC is one of PBOC's priorities in 2018.
Jun. 2018	PBOC	Filed 81 domestic patents for CBDC as of June 2018.
Jun. 2018	DCRI of PBOC	Launched a fully-owned subsidiary in Shenzhen, namely Shenzhen Fintech Limited, with its business scope defined as FinTech development, technology consulting/transfer/servicing, and operation & maintenance of FinTech related systems etc.
Sep. 2018	PBOC, DCRI of PBOC, Nanjing government, Bank of Jiangsu, Nanjing University	Jointly launched a FinTech center in Nanjing, which will serve as a base to develop and test CBDC pilot programs.
Sep. 2018	DCRI of PBOC	DCRI's research paper 'Considerations on the design and architecture of Central Bank Digital Currency' (法定数字货币模型与参考架构设计) won the 1st place of China banking tech development award.
Aug. 2019	PBOC	Revealed its intention to "accelerate the pace of R&D of China's legal digital currency (DCEP), track and study the development trend of virtual currencies at home and abroad, and continue to strengthen Internet financial risk remediation" during the video conference discussing it 2H 2019 work plan. Mu Changchun, deputy director of the PBOC's payments department, officially mentioned that the PBOC is almost ready to launch its CBDC.
Dec. 2019	PBOC	China's local news (Caijing) reported the PBOC is planning to initially test circulation of CBDC in two cities (Shenzhen and Suzhou) on the back of support from the four major commercial banks and three telecom operators.
Apr. 2020	PBOC	Internal pilot tests for CBDC were conducted in the Xiongan New Area of North China's Hebei Province, Suzhou of East China's Jiangsu Province, Chengdu of Southwest China's Sichuan Province, and Guangdong's Shenzhen.
Oct. 2020	PBOC	Shenzhen, along with PBOC, distributed RMB10mn to its residents in the form of CBDC, marking the first time that the test of CBDC went public from a closed internal test.
Dec. 2020	PBOC	Beijing started CBDC trial program on the Metro Daxing Airport Express.
Jan. 2021	PBOC	Pilot testing of CBDC conducted in Shanghai's Tong Ren Hospital, offering staff a convenient way to pay for their meals in the canteen.
Jan. 2021	Agricultural Bank of China	Agricultural Bank of China pioneered the launch of CBDC-enabled ATMs, which allow customers to deposit and withdraw CBDC, as part of the trial run.
Feb. 2021	PBOC	Distribution of e-CNY red packet to residents in Beijing, Suzhou, Shenzhen, and Chengdu. Expanded the use cases of e-CNY for online (e.g., JD.com) and offline (e.g., supermarkets, restaurants, gas stations etc.) consumption.
Feb. 2021	Various Banks	Rolling out e-CNY enabled card and various other wearable devices (e.g., gloves, watches, badges etc.), which are embedded with 'e-CNY' electronics chips, enabling convenient digital payments by contact.
Feb. 2021	PBOC & other Central Banks	PBOC, HKMA, Central Bank of Thailand, Central Bank of UAE announced the development proof of concept prototype to facilitate real-time cross-border foreign exchange payments on distributed ledger technology.

Source: PBOC, News Reports, Citi Research

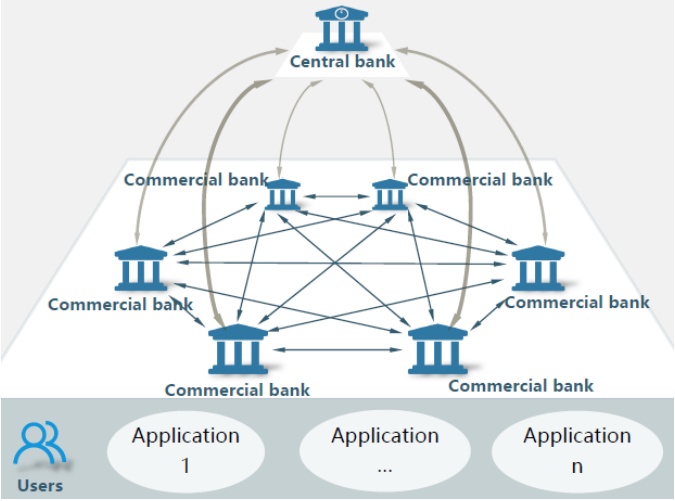
DCEP as a Two-Tier System

PBOC adopted a two-tier system for three reasons: (1) utilization of existing commercial banks' branch networks for easier public access of the DCEP; (2) mitigation of excessive concentration of risk; and (3) prevention of financial disintermediation risk. If a commercial bank is under financial stress, individuals would withdraw their deposits and the commercial bank may run out of cash — resulting in a bank-run. Individuals may prefer to save money in a central bank deposit account to protect savings. These could contract the existing money supply process through commercial banks.

- **In the First Tier**, the central bank may provide DCEP to a commercial banks' digital wallet in exchange for existing reserves. Commercial banks could exchange DCEP with each other through the digital wallet. These processes may be similar to those of the existing central bank reserve. The DCEP could be close to a token-based money in the first-tier.

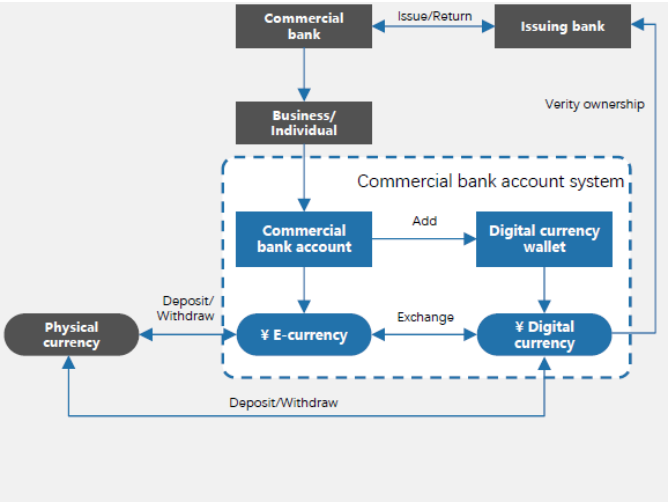
- **In the Second Tier,** individuals may open a digital currency wallet in their commercial bank accounts to exchange DCEP for existing deposit or physical cash. Individuals may utilize smartphone applications for retail transactions.

Figure 28. DCEP – Two-tiered System to be Adopted



Source: PBOC; Note: Yao Qian, "Technical Aspects of CBDC in a Two-Tiered System", Institute of Digital Money, People's Bank of China, July 2018

Figure 29. DCEP – Implementation Model Based on Commercial Bank Account



Source: PBOC; Note: Yao Qian, "Technical Aspects of CBDC in a Two-Tiered System", Institute of Digital Money, People's Bank of China, July 2018

Figure 30. Key Attributes of China's DCEP

Attribute	Digital Currency Electronic Payment (DCEP)
Definition	It is a digital form of currency designed to substitute M0 (i.e., banknotes and coins), the value of which will be pegged 1:1 to RMB
Characteristics	1. DCEP is a type of fiat currency and bears an indemnity clause. No institutions legally registered in China or Chinese citizens should decline the use of DCEP; 2. DCEP is essentially a digital form of cash and shares the identical nature of cash; 3. DCEP supports 'dual offline payment' i.e., DCEP does not require an Internet/mobile connection to pay.
Necessity	1. DCEP helps to protect China's monetary sovereignty and legal currency status; 2. Banknotes/coins have relatively high issuance and circulation costs; 3. People's demand for physical cash is declining fast; 4. DCEP satisfies the general public's demand for anonymous payment.
Operating mechanism	Two-tier operating structure; i.e., PBOC first issues DCEP to commercial banks/other commercial operating agencies, and then asks these agencies to distribute the DCEP to the public.
Technical route	DCEP would keep an open/integrated infrastructure and does not necessarily rely on one fixed technological path: 1. Between PBOC-Commercial banks/other commercial agencies: PBOC does not preset technical route, while accepts any tech solutions fulfilling its requirements of high scalability/ concurrency, quality retail customer experience & strict technical compliance; 2. Between commercial agencies and the general public: DCEP's architecture can accommodate various ledger systems (i.e., distributed and centralized) and payment methods (i.e., Internet, mobile, offline).
Deployment method	Similar to physical cash (banknotes, coins), i.e., commercial banks pay 100% reserves to the central bank; general public open digital wallets at commercial institutions (e.g., commercial banks)
Currency indemnity	DCEP is unlimited fiat currency guaranteed by central bank credit.
How can the general public use DCEP?	Similar to traditional e-payment methods, i.e., retail customers just need to download an app to access their digital wallets and settle transactions with existing DCEP balance; They can also easily convert bank deposits into DCEP in the app/ on the Internet.
Are there any transaction/balance limits for DCEP payment?	Yes, given the need to combat illegal activities such as money laundering, terrorist financing etc. In general, there are three or more levels of transaction/balance limits applicable to the same account holder depending on the identification number used during wallet set-up. Higher limits would be given to more recognizable wallets. For example, a digital wallet registered with a mobile number will be capped at lowest limits, and is likely to be restricted for use in daily small retail payments; while wallets registered with ID card number or linked to bank card will entitle higher limits, and the limits could be all lifted if the customer opens the wallet at a physical bank counter.
How does DCEP identify money laundering/terrorist financing activities?	Leveraging big data analytics; Despite a normal transaction is anonymous, the system is expected to identify the account holder by analyzing the behavior (historical activities) of the payer.

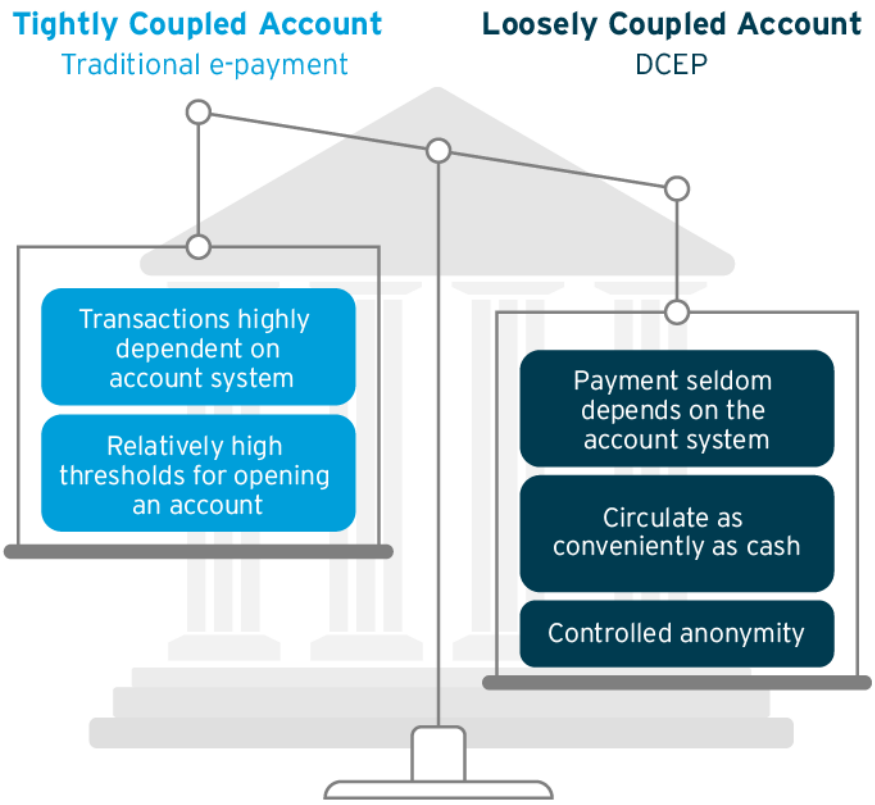
Source: PBOC, Digital Currency Research Institute of PBOC, Citi Research

Is DCEP a Better Payment Form versus Cash/Electronic?

- **Digitalized Bookkeeping and High Transaction Traceability:** DCEP will be a tokenized model and take the form of an encrypted numeric string containing basic information such as serial number, amount, owner, issuing bank signatures etc. At the core of DCEP is its registration center, managed by the PBOC in a centralized approach without the need for a blockchain consensus mechanism, hence it can be more efficient. The registration center will record all DCEPs, corresponding owner identities, as well as all DCEP transactions, including whole life-cycle of issuance, circulation, and redemption. This allows the PBOC better transaction traceability and allows better risk control (e.g., money laundering).

- **Loose Account Coupling and Controlled Anonymity:** Traditional electronic payment tools, e.g., bank cards and third-party payments, are based on tight coupling of existing base accounts (i.e., account model) and are not anonymous. DCEP, on the contrary, follows the loose account coupling model (i.e., token model) and can achieve 'controlled anonymity', i.e., the DCEP transaction data is only visible to the PBOC (upon crossing the firewall). All other parties in a transaction — banks and merchants — can only see the digital wallet address of the DCEP users (like a nickname), but will not be able to trace the true identify of DCEP users or their transaction history without the permission of the user. This allows DCEP to have better anonymity than electronic payment but has better regulatory transparency than cash.

Figure 31. Comparison Between a Tightly Coupled Account vs. a Loosely Coupled Account



Source: Digital Currency Research Institute of PBOC, Citi Research

- **Support 'Double Offline' Payment:** DCEP transactions can be done with both parties being offline, potentially achieved by a near-field communication (NFC) based payment method. This will make DCEP a direct replacement of banknotes and allow broader usage scenarios of DCEP even with no or poor Internet coverage, thus resolving one key restrictions of the electronic payment methods today. In addition, DCEP does not require the mobile device to be bound to a bank account, which means the unbanked population will also have access to the digital currency.

- **Better User Experience:** Compared with cash, DCEP is: (1) more convenient given users would only need to carry with them a card or mobile phone; (2) safer as even if the card/phone is stolen, the criminal wouldn't be able to spend the money without the PIN and the owner can always cancel the card/freeze their DCEP account immediately; and (3) more flexible in terms of reversing a mistaken/unauthorized transaction.

  Compared to e-payment, DCEP is expected to have: (1) wider acceptability given it's essentially a type of central bank money, which all institutions should accept in light of government enforcement versus not all merchants accept traditional card/mobile payments where commercial banks provide the credit; and (2) protect user privacy given the information exchange only occurs at data depositories of PBOC/commercial banks, versus the third-party payment institutions' access to account holder's information in a traditional e-payment.

Figure 32. Making Payments Using DCEP versus Cash versus Traditional e-Payments

		DCEP	Traditional e-payment		Cash
			Card-based	Network-based	
Basic infrastructure	**Physical form**	App/Chip card	Chip card	App	Banknotes, coins
	Underlying account	Bank account/digital (virtual) wallet	Bank account	Digital (virtual) wallet	n/a
	Interest on balance	Customizable	Debit card: interest-earnings (from balance in savings account); Credit card: negative interest	Zero interest; Negative interest considering the transaction fee	Zero interest; Negative interest considering the transaction fee
	Clearing system	PBOC payment and clearing system; PBOC DCEP system	PBOC payment and clearing system	PBOC payment and clearing system	n/a
Transaction characteristics	**Convenience in making remote payments**	Convenient	Convenient	Convenient	Not convenient
	Traceability	Traceable	Traceable	Traceable	Not traceable
	Anonymity	Manageable anonymity	Recognizable	Recognizable	Completely anonymous
	Transaction reversibility	Reversible under certain conditions	Reversible under certain conditions	Reversible under certain conditions	Very difficult to reverse
	Transaction limit	Customizable	Subject to (1) limits set by banks; (2) limits set by account holders	Subject to (1) limits set by FIs; (2) limits set by wallet owners	Cash withdrawal limits apply
	Network connection requirements	Potentially no requirements for transactions between individuals/businesses	Requiring access to network	Requiring access to network	No requirements
	Processing time	Real time	Only at specific times (e.g., during merchants opening hours)	24x7 servicing time	Real time
Currency nature	**Credit backed by**	PBOC	Commercial banks	Commercial banks	PBOC
	Transfer method	Point-to-point, via third-party	Via third-party	Via third-party	Point-to-point
	Money supply classification	M0	M1	M1	M0
Regulatory oversight	**Transparency**	Relatively high	Relatively low	Relatively low	Low

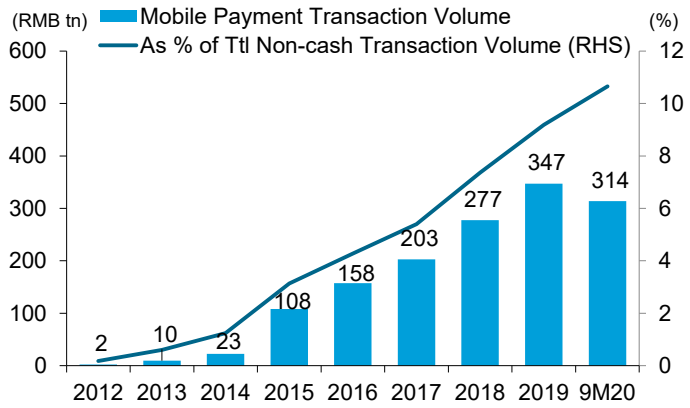
Source: PBOC, Citi Research

Is China Set for Wide Adoption of DCEP?

We see DCEP as mainly designed for retail use in its initial rollout, and we expect fast adoption of DCEP in retail transaction scenarios given China has been sprinting to a cashless society. Use of mobile payment has skyrocketed over the past eight years, with the total mobile payment-based transaction volume in China reaching RMB 314 trillion (~$48bn) in first nine months of 2020 (equivalent to over 135x of that in 2012), accounting for 10.7% of total non-cash transaction volume (up from 0.2% in 2012), according to the PBOC. The high penetration of electronic payments in China, in our view, serves as a solid foundation for the adoption of DCEP.

On top, DCEP has several advantages compared to third-party payment channels, including: (1) being more secure in nature as it enjoys the credit endorsement by the PBOC; (2) allowing both sides to be offline to conduct transaction; (3) any merchant that accepts digital payment is mandated to accept DCEP, according to the PBOC, versus the current system where certain merchants will accept only certain third-party payment vendors and there is a lack of generally-accepted digital wallets.

Figure 33. Skyrocketing Mobile Payment-based Payment Volume in China, with Rising Share of Total Non-Cash Transaction Volume



Source: PBOC, WIND, Citi Research

Implications for RMB Internationalization

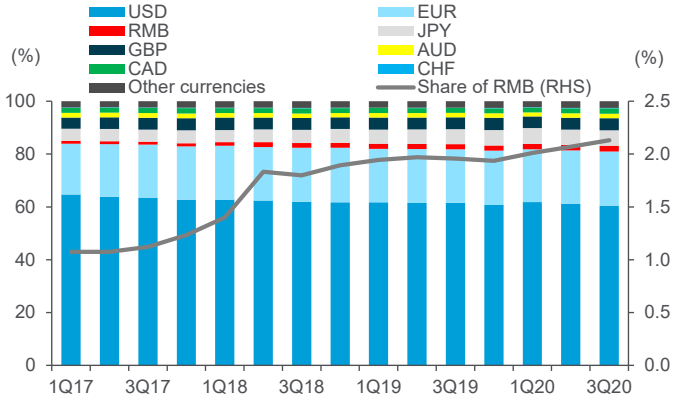
There has been no quick easy solution for renminbi (RMB) internationalization. RMB as a share of global foreign exchange (FX) reserves are a mere 2% versus the U.S. dollar (USD) at 60%. Share of goods trade settlement in RMB by China remained at around 15% in the second quarter of 2020, similar to the past few years, but well below the 2015 peak at 2x.

However, China may have a strong incentive to accelerate RMB internationalization to mitigate the potential risk of financial sanctions by the U.S., by encouraging trade financing/invoicing/settlement to be carried out more in RMB. DCEP has a domestic focus first but the second stage will be international expansion.

Currently, RMB cross-border payments are mainly facilitated by two international interbank payment systems, i.e., the Belgium-based Society of Worldwide Interbank Financial Telecommunications (SWIFT), and the China-based Cross-border Interbank Payment System (CIPS). Both of these are account-based systems.

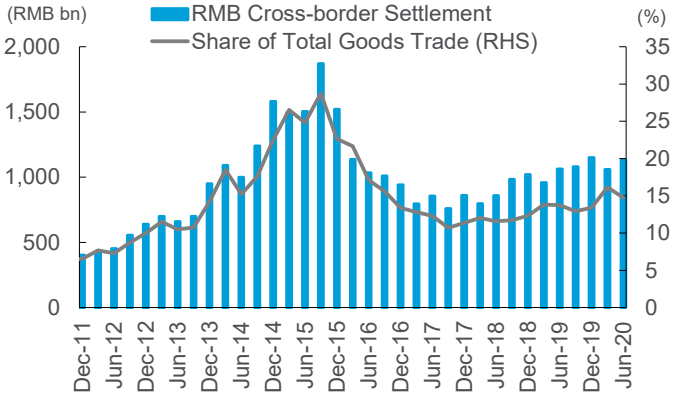
The use of DCEP in cross-border payment will mean a regime shift from an account model to token model, and may give rise to an alternative payment solution for bypassing SWIFT in international settlement in the long run, which appears to be attractive for some Chinese policy makers.

Figure 34. Composition of Allocated Foreign Exchange Reserves; Rising Share of RMB



Source: International Monetary Fund, Citi Research

Figure 35. China: Share of Goods Trade Settlement in RMB Recorded at Around 15% in 2Q 2020



Source: CEIC, Citi Research

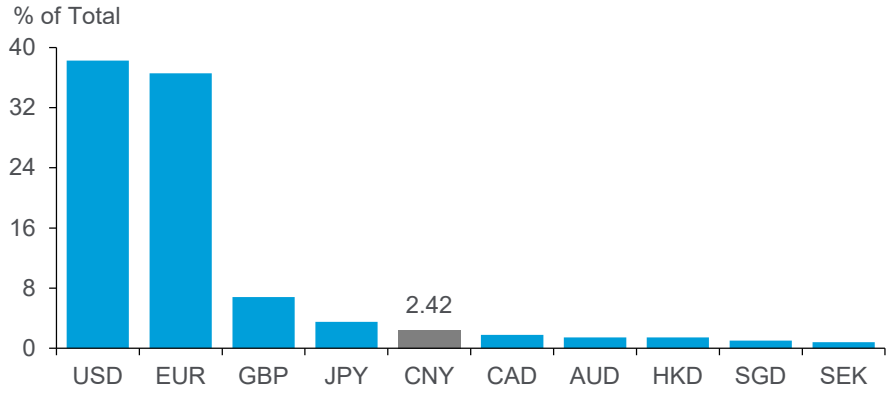
We believe DCEP holdings will lower hurdles for circulation of RMB in cross-border payments as: (1) it only requires one to have a DCEP wallet, which is not bound to bank accounts and is likely easier to have than to open RMB deposit accounts, and (2) digital flow will allow for speedy and low-cost cross-border payments.

However, application of DCEP in cross-border transactions will likely take longer to become a reality. CBDC is still at the very early stages in terms of acceptance even for domestic usage. Even a domestic CBDC in China may need several years to evaluate its technical and economic achievement.

Second, technical assessment could take a much longer time as cross-border transactions would involve many international counterparties. More technical assessments are needed to prove a clear economic incentive in utilization of CBDC for such transactions.

At the onset of DCEP adoption, it would make more sense to hold more RMBs, but that seems to be a long road ahead. RMB's share in international payments is low at 2.4% relative to its share in global trade. While this is likely to rise over time as China's economic weight grows, the disparity between USD/EUR and RMB is huge.

Figure 36. RMB's Share as an International Payments Currency at 2.42% in January 2021



Source: Swift Watch/ RMB Tracker, Citi Research

On February 23, 2021, the People's Bank of China, the Central Bank of the UAE, and BIS Innovation Hub joined the m-CBDC bridge with the Bank of Thailand and the Hong Kong Monetary Authority (HKMA) to develop a proof of concept prototype to facilitate real-time cross-border foreign exchange payments on the distributed ledger technology (link).

The m-CBDC Bridge project aims to propose solutions and concepts to resolve the current pain points in making cross-border fund transfers such as operational inefficiencies, high cost and complex regulatory compliance.

Internationalizing central bank issued currency would mean enabling wider usage/acceptance of e-RMB outside of Chinese soil and this may be a potential long term threat to U.S. dollar's dominance in the global currency market and could possibly lead to a digital currency cold war.[13]

CBDC as a Monetary Policy Tool

A new form of money allowing users to directly make electronic payments is likely to offer greater end-user convenience, but also impact the structure of traditional banking systems. Some of the potential impacts include:

1. Effective transmission of monetary policy as any changes in policy rates would be passed on faster and fully to households and corporates.

2. Help reduce systemic risk by providing an alternative payment service, not reliant on legacy banking systems.

3. On the flip side, CBDCs could also increase the risk of disintermediation, as users could switch some of their funds from banknotes/commercial bank deposits to CBDCs.

4. Lastly, CBDCs could also introduce risks for financial stability, as the shrinkage of banks' balance sheet could affect the availability of credit in the economy.

[13] David Birch – The Currency Cold War: Cash and Cryptography, Hash Rates and Hegemony (2020).

PBOC to Substitute M0 with DCEP

According to the PBOC, DCEP will not just be a digital currency, but it is also designed to substitute M0 (i.e., banknotes and coins), but not M1 or M2, as those have already been electronic and digitalized. The DCEP will be pegged 1:1 to the RMB, and similar to the existing M0, DCEP will be a central bank liability to the public.

However, DCEP is expected to resolve some of the pain points of physical cash, such as high issuance and storage costs, ease of anonymously forging it, and risks of being used for money laundering and terrorist financing.

Figure 37. DCEP and PBOC's Monetary Supply

	Dec 2019	
	RMB tn	as % M2
Money and quasi-money (M2)	198.6	100.0%
Non deposit	2.1	1.1%
Total deposits	188.8	95.0%
Deposits of households	81.3	40.9%
Deposits of non-financial enterprises	59.5	30.0%
Deposits of gov't and NBFIs	48.0	24.1%
Currency in circulation (M0)	7.7	3.9%
Banknotes and coins in circulation	7.7	3.9%

Post official use of DC/EP
Money and quasi-money (M2)
Non deposit
Total deposits
Deposits of households
Deposits of non-financial enterprises
Deposits of gov't and NBFIs
Currency in circulation (M0)
Banknotes and coins in circulation
DC/EP in circulation

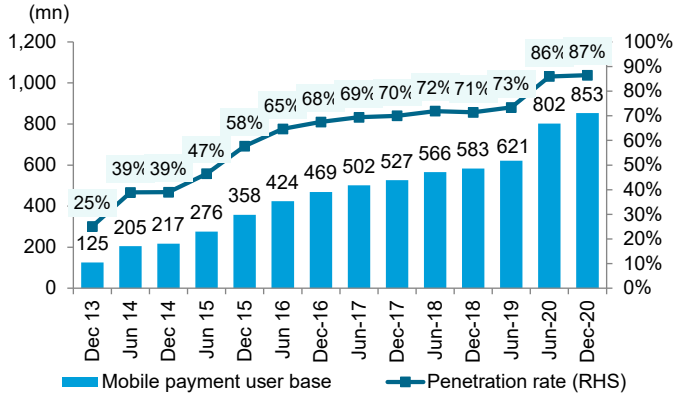
Note: We assume DCEP to serve as a complement of cash, rather than to replace cash completely.
Source: PBOC, Citi Research

A general-purpose CBDC as an alternative to improve stability of the whole payment system: China's currency in circulation (percent of GDP) has declined from 11% in the fourth quarter of 2011 to 7% in the third quarter of 2019 amid rising popularity of third-party mobile payments. The penetration rate of Chinese mobile payment users surged to 87% in December 2020 from 25% in December 2013.

Two platforms have continued to dominate the third-party mobile payment market with around 90% market share since 2014. The average Chinese citizen owned 0.53 credit and debit-integrated cards on average at the end of 2019, much lower than an average of 4 credit cards per American in the U.S., as estimated in the 2019 Experian Consumer Credit Review.

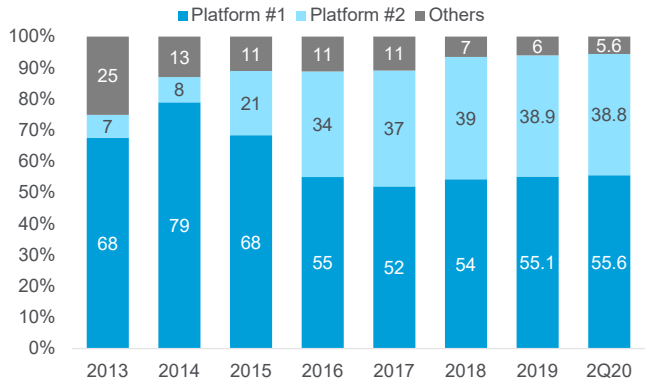
Given less usage of cash, China is increasingly dependent on just two private payment systems. If these two major payment platforms have problems for any reason, individuals and firms would experience difficulties in retail transactions. This could create systemic issues for the central bank and developing the DCEP provides an extra layer of payments resilience.

Figure 38. Penetration of China Mobile Payment Users Jumped to 87% in December 2020 from 25% in December 2013



Source: CNNC, Citi Research

Figure 39. Two Platforms Continue to Dominate the Third-Party Mobile Payment Market (Market Share by Transaction Volume)



Source: iResearch, Analysys, Citi Research

Implications for Regulatory Efficiency & Monetary Policy

If DCEP gets more widely adopted and expands to wholesale transactions over time, we believe it will help improve PBOC's regulatory efficiency and achieve more effective monetary policy transmission. We highlight below the key potential benefits of DCEP versus the existing monetary policy mechanism.

1. **Lower Currency Issuance Cost:** Unlike banknotes and coins, issuing DCEP does not incur any production cost (i.e., raw materials used), nor any warehousing or transportation costs, given it is fully digitalized and can be issued and 'delivered' to commercial banks by simply updating the ownership information.

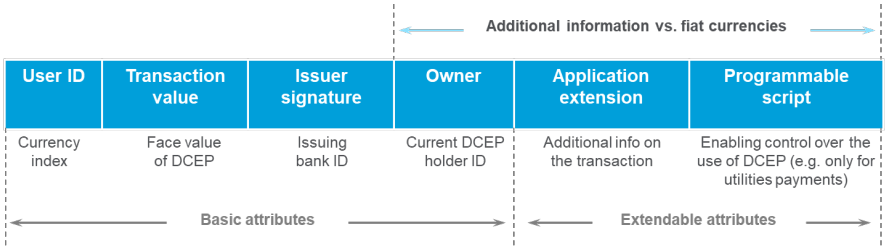
2. **Better Oversight on Money Flows:** Traditional e-payments adopt account-based bookkeeping methods, where the amount is deducted from the payer's account balance after each transaction, and the same amount is added to payee's account balance.

   To trace one transaction, regulators would need to dig through numerous historical transactions in both the payer's and payee's accounts, which is time consuming, costly, and raises concerns over data privacy abuses.

   Each DCEP token has a standardized structure which entails information on user ID, transaction value, issuer, owner etc. Information gets updated with each transaction and is stored in a centralized registration center managed by the PBOC. As such, the PBOC would only need to extract information on one DCEP token to trace all underlying transactions.

   DCEP will also resolve difficulty in tracking transactions involving cash, as the PBOC could easily extract transaction details of every DCEP payment from the central data depository and authorization center (to find out the real identity of payer/payee), lowering regulatory cost against tax evasion, money laundering, illegal transactions, and limiting illicit activity with cash payments.

Figure 40. Proposed DCEP Design Attributes



Source: Digital Currency Research Institute of PBOC, Citi Research

3. **More Targeted and Effective Implementation of Monetary Policies:** PBOC's current monetary policy framework is more inclined to broad-based management, instead of structural adjustment, mainly restricted by weakness in overseeing money flows.

   In times of monetary easing, the effectiveness largely hinges on commercial banks intermediating flow of funds. Should there be any deficiency in banks' loan pricing mechanism, the credit structure could be sub-optimal ultimately, which would undermine effectiveness of monetary measures.

   By loading DCEP with smart contracts, it will allow the PBOC to achieve more efficient and targeted monetary policies implementation. Based on the patent information released by the PBOC, it will be able to control the subject, interest rate, and timing of commercial banks' credit extension.

   The PBOC can also alter the DCEP redemption interest rate based on economic condition to implement counter-cyclical policy adjustment.

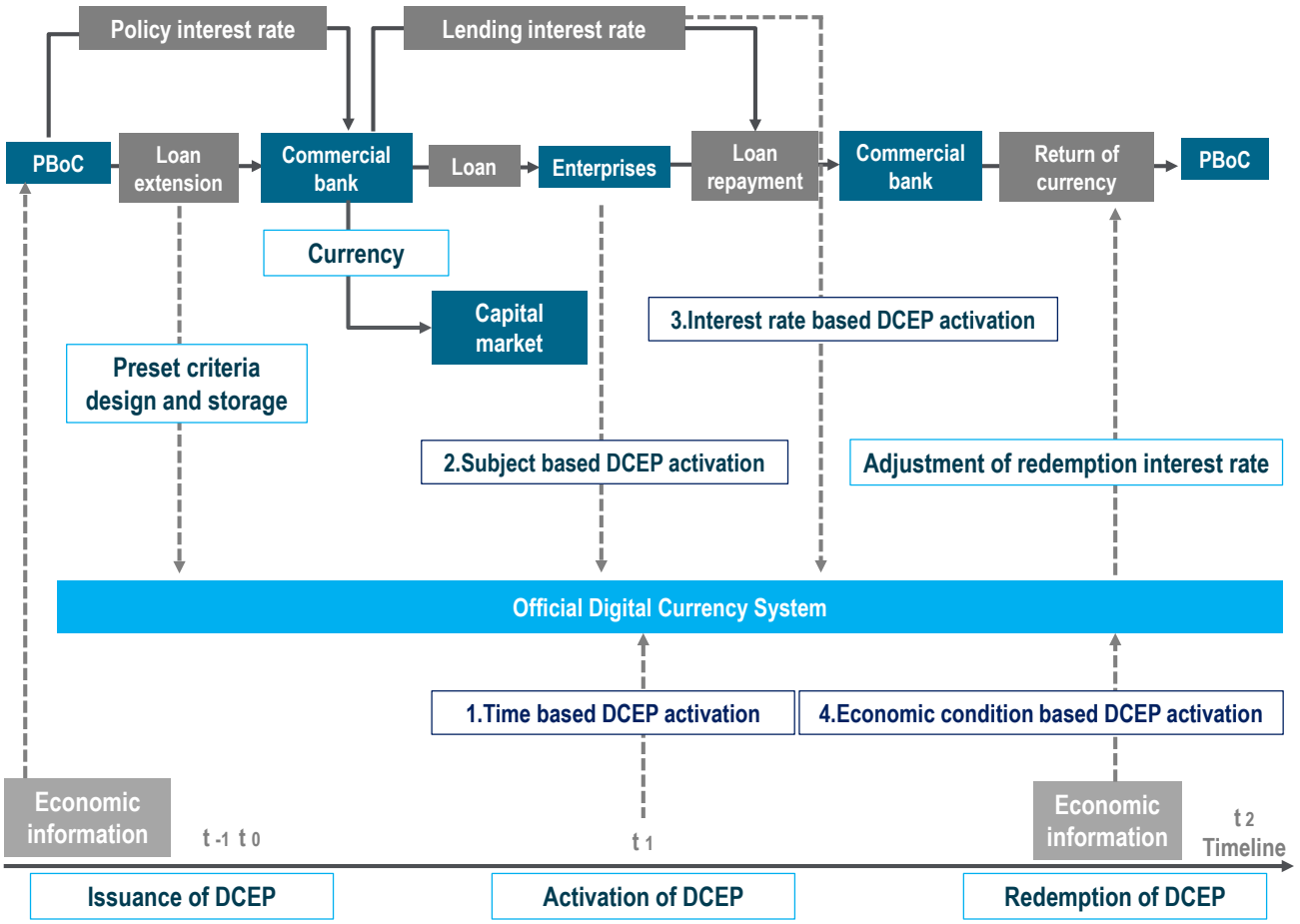
- **Time-based DCEP management:** The DCEP will be preset as 'invalid' upon issuance, and when financial institutions make request to activate it, the system will validate the time that the request is sent, and will only make the DCEP valid when the time information match with the preset criteria. This will resolve the timeliness issue of the current monetary policy transmission mechanism, so that the time the currency becomes effective will not necessarily be the time when currency is issued, but can be delayed to a certain future time that fits the policy goal, so as to avoid currency idling.

- **Interest rate-based DCEP management:** The DCEP will be preset as 'invalid' upon issuance, and when financial institutions want to extend loans using DCEP, they will make a request to active it. The system will then validate the corresponding loan interest rate, and only make the DCEP valid when the loan interest rates match with the preset criteria. This will allow more effective transmission of policy rates to real lending rates.

- **Subject-based DCEP management:** DCEP will be preset as 'invalid' upon issuance, and when financial institutions want to extend loans using DCEP, they will make a request to active it. The system will then validate the loan extension subject, and only make the DCEP valid when the subject matches with the preset criteria. This will allow more targeted credit extension (e.g., to SMEs) and allow the financial system better serve the real economy.

- **Economic condition-based DCEP management:** The above three mechanisms target the credit extension process after DCEP is issued, while this mechanism targets the redemption of DCEP and determines the interest rate upon redemption. When banks return the DCEP to PBOC, the economic information (e.g., GDP, CPI, industrial production) at the time of return will determine whether and how the DCEP redemption interest rate will be adjusted (i.e., different set of condition will point to different preset interest rate). This will allow the PBOC to implement counter-cyclical adjustments, i.e., lifting redemption interest rate in economic upcycles and lowering redemption interest rate in economic down-cycles, so as to reduce the pro-cyclicality of financial institutions' lending behavior (i.e., increase new loan quota/loosen credit standards during economic booms; or shrink new loan quota/lift credit standards during economic downturns) and avoid the risk of a 'liquidity trap'.

Figure 41. Implementation Process of DCEP-based Targeted Monetary Policy



Source: Citi Research

However, we note the PBOC remains prudent on the use of smart contracts in DCEP. As warned by Mr. Mu Changchun, Head of the PBOC's Digital Currency Research Institute, if DCEP is loaded with too many smart contracts or smart contracts beyond its monetary function, the currency will be torn, may degenerate into a value instrument degraded, and its usability will be reduced. He also indicated that the PBOC will only load smart contracts that are beneficial to the monetary function, but remain more cautious towards additional smart contracts beyond the monetary function. Hence, we expect immediate impact from the launch of DCEP on monetary policy to be limited.

4. **Provide Conditions for Implementing Negative Interest Rates:** Following the Global Financial Crisis, several central banks have implemented negative policy interest rates to boost growth, but most of these policies only target the interest rate of banks' deposit reserves at the central bank as a means to stimulate banks to lend, and are not transmitted to the personal deposit rate. Personal deposit rates do not go below zero in practice, as if they do, depositors will withdraw interest bearing deposits and hold cash instead (with zero nominal interest rate), reducing effectiveness of the negative interest policy.

   The introduction of DCEP to fully replace cash can resolve this problem. By charging households or businesses negative interest rates on DCEP they hold, they will be forced to spend and invest and hence stimulate growth.

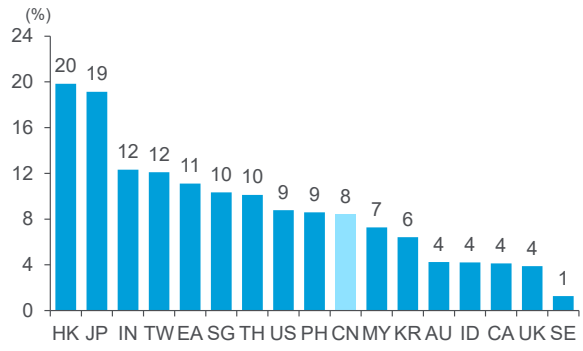
5. **Improve Efficiency of Open Market Operations and Interbank Market Transactions:** Currently Open Market Operations (OMO) and interbank payments can only be settled through financial institution reserves placed at the PBOC, and are subject to various limitations of the interbank payment system (e.g., specific trading hours).

   While DCEP is mainly designed for retail use, we see potential for it to be extended to wholesale (interbank payment) as well as serve as a supplement to excess reserves, helping improve the efficiency of OMOs/interbank payments; given shorter settlement time, better traceability, and longer operating hours DCEP is expected to enjoy versus traditional e-payment systems.

6. **Reduce Banks' Liquidity Risk During Stress Times:** In times of financial stress, faster/easier conversion from bank deposits to DCEP (versus cash) and its more secure nature means bank runs could happen in a faster/larger scale, increasing banks' liquidity pressure. But in practice, the PBOC could avoid this by (1) setting a low negative interest rate on DCEP to curb demand; (2) adding some exchange costs/frictions or set transaction limits to avoid pro-cyclical conditions in stress environment; and (3) setup temporary DCEP discount facilities to rapidly provide banks with additional DCEP needed to fulfill DCEP withdrawal demand.

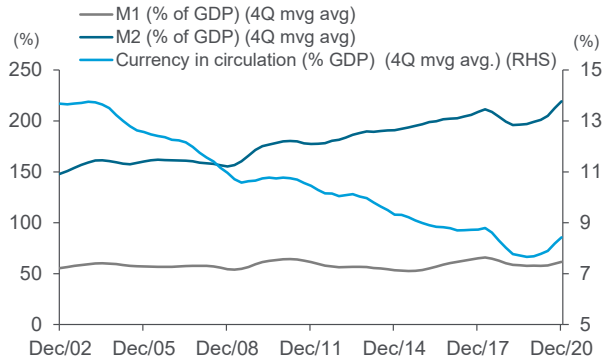
   Convenience of DCEP payment means it can replace electronic payment and the use of account-based excess reserves in interbank transactions; whilst higher efficiency in payment/settlement will help reduce interbank liquidity risk.

Figure 42. Global: Currency in Circulation (% of GDP), 4-qtr Moving Average, as of 3Q/4Q 2020



Source: Haver Analytics, Citi Research

Figure 43. China: China's Currency in Circulation (% of GDP) has Declined from 10.5% in 4Q 2011 to 8.4% in 4Q 2020



Source: Haver Analytics, Citi Research

Big Tech, Stablecoins & Diem

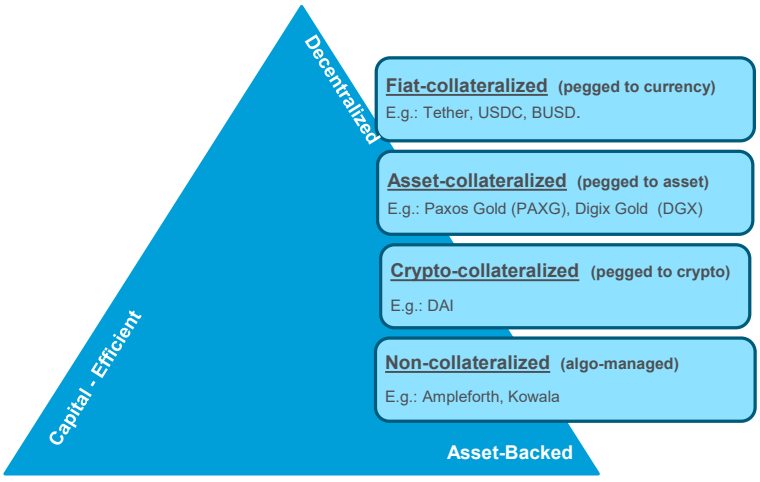
- Why Diem? Facebook is building alternative payment rails to the existing card and bank-based payment system on which its Novi wallet (and others) could be hosted. These wallets would need to be regulated in their home markets.
- Potential use-cases for Diem/stablecoins include greater integration of payments with social media, facilitating cross-border payments, and working with cryptocurrencies (as on/off ramps).
- Diem, the protocol layer, could receive FINMA regulatory approval before the end of 2021, and with it could launch a Diem Dollar, albeit many jurisdictions have publicly noted their antipathy towards the whole project previously.
- What's changed with the 2020 Diem (Libra) Whitepaper update? A move to a single currency stablecoin linked to fiat, enhanced compliance, no more transition to permission-less system, and enhanced design details of Libra reserve.
- It is possible other Big Techs could follow into tokenized money, but for now few have declared this ambition publicly — and Facebook's user reach is extensive (3.3 billion monthly average users) and hard to replicate.
- We start with an introduction to stablecoins in this chapter — What are they? How do stablecoins differ from decentralized cryptos and e-money? What are their use-cases? Different approaches to developing a stablecoin?

Stablecoins 101

Stablecoins are blockchain-based digital currencies that are linked to the value of an underlying asset. Blockchain technology enables a marketplace to operate without assigning control to any single participant. This can create good economic properties for fostering competition and innovation in the long run.

Owing to their peg, stablecoins are not subject to extreme price volatility, which has otherwise prevented mainstream adoption of applications built on top of cryptocurrency protocols. The most commonly collateralized stablecoins are the ones linked to fiat currencies such as the USD, EUR, or GBP.

Figure 44. Different Approaches to Developing a Stablecoin



Source: Citi Research

Stablecoin Use-Cases

- **Cryptocurrency Wallets/Trading:** A digital wallet that stores private/public keys and interacts with various blockchains, allowing users to send/receive digital currency. Stablecoins could be used for crypto-trading on exchanges that cannot access banking services. It is also useful compared to legacy payments as they are instant and available 24x7.
- **Fiat Proxy in Decentralized Finance (DeFi):** One can convert bank-based U.S. dollars into USDC and deposit it in a protocol like Aave to earn interest.
- **Global Currency:** A stable digital currency can become a global medium of exchange (e.g., remittances), in markets with either hyper-inflation, economic uncertainty, or capital controls.
- **Cross-border Payments:** Currently, global remittances can take days to settle and cost can be as high as double-digit percentages in some Emerging Markets. With stablecoins, remittances could be sent instantaneously around the globe at very low cost.
- **Trade Receivables Market:** MakerDao, for instance is working with supply chain management startup Tradeshift, to tokenize unpaid invoices by selling them at a discount to crypto investors, so that small businesses can receive their payment upfront.
- **Offers individuals a cold store for USD/fiat** by storing crypto in a medium that's disconnected from the internet and secured by one's own private keys.

Tether: The Elephant in the Stablecoin Room

The biggest of the current stablecoins is Tether with over $40 billion in circulation as of end-March 2021. As a large liquid U.S.-dollar denominated stablecoin, Tether's reported daily turnover is close to $100 billion, making it the most traded asset in the cryptocurrency ecosystem. However, Tether is not without controversy, most recently in the settlement with the New York Attorney General's Office[14], which prohibited its parent company from trading in New York.

While the New York Attorney General's agreement was not a positive outcome for Tether, it did at least lay to rest some of the wilder elements of speculation about the coin. Nevertheless, there remain serious questions about the lack of audit. And given the high dependence of the crypto-ecosystem on stablecoins, a loss of confidence in the most high-profile stablecoin would be a significant blow to valuations across the crypto-space, although less-liquid coins would likely be most impacted.

However, the crypto-ecosystem has shown itself to be highly resilient to shocks and damage, and should Tether stumble, we think that its place would be taken by another stablecoin. Although Tether is the largest stablecoin, there are a number of challengers in the space. As the second generation of stablecoins many of these challengers deal directly with the biggest criticism levelled against Tether and provide full audits of the assets that back them.

[14] https://ag.ny.gov/sites/default/files/2021.02.17_-_settlement_agreement_-_execution_version.b-t_signed-c2_oag_signed.pdf

While Tether undoubtedly benefits from incumbency in the space, and has grown significantly in the past year, the next generation of coins is, if anything, growing faster. But, they remain a long way behind and still lack the same network effect that Tether has. Given the wider acceptance of these coins on more highly regulated exchanges and the lower credit risk that comes with fully audited coins, it seems possible that Tether may lose its crown in the near future.

Stablecoins vs. Decentralized Cryptos

Decentralization, in essence, means no single central party has the authority or power to control the operation or outcome of the process. A decentralized network relies on host of computers to complete the process. Hence, blockchain technology needs a P2P network. On the contrary, stablecoins tend to be backed by a single base, and work more in a centralized pattern.

Decentralized cryptos do not have a central repository which could wipe out all the holdings in case of a server crash or if the user misplaces his private key. This is not the case with collateralized stablecoins which have equal or more asset base to rely on. An interesting point here is that while private keys get lost all the time and the pool of coins diminishes, coins could get over-collateralized with time.

Another difference would be the reason stablecoins were invented i.e., price volatility. It is possible for decentralized cryptos to have large price variations as opposed to stablecoins which are not very price sensitive (at least in theory). Some coins are also pegged to the U.S. dollar, which links them to the U.S. banking/financial system, and thereby rely on a centralized infrastructure.

Depending on the protocol, stablecoins can possibly transact faster than classic cryptocurrencies. The Libra protocol technical document highlights “the system is likely able to meet the demand of 1,000 transactions per second (TPS)”. By contrast, Bitcoin has a transaction capacity of 7 TPS. Visa handles around 1,700 TPS (or 150 million a day) and claims to be able to handle up to 24,000 TPS, in theory.

Stablecoins vs. e-money

Money can be broadly defined to have the following attributes: (1) a unit of account; (2) medium of exchange; and (3) store of value. While cryptocurrencies have often been compared to money, a major deterrent has been their extreme price volatility, making them an unreliable unit of account over time.

Stablecoins are cryptos designed to minimize price volatility. They achieve this by pegging their value to a stable fiat/other assets. Despite their similarities to fiat currencies, below are a few points that distinguish them from e-money:

- **Privately issued, not linked in regulatory framework:** Stablecoins are privately issued. For instance, the most popular stablecoin, USDT, is issued by Tether International Ltd, a privately-held company. They are also not automatically linked in the regulatory framework with central bank money.
- **Underlying technology:** Classic e-money tends to be limited to the purpose and infrastructure of the issuing institution/business, while operating in a closed loop system. In contrast, issuance of stablecoins on a decentralized network allows for transfer of funds between businesses and people.
- **Expensive liquidation into fiat:** Costs for liquidation of stablecoins into fiat currency can be high versus e-money which tends to be near costless.

From Libra to Diem

A white paper on Libra was released on June 18, 2019 titled "An Introduction to Libra" detailing its blockchain-based financial infrastructure project. Libra rebranded to Diem in December 2020. Diem It is expected to launch its first stablecoin, likely a "Diem dollar", which could be over the next year, assuming it is licensed by FINMA (the Swiss Financial Market Supervisory Authority).

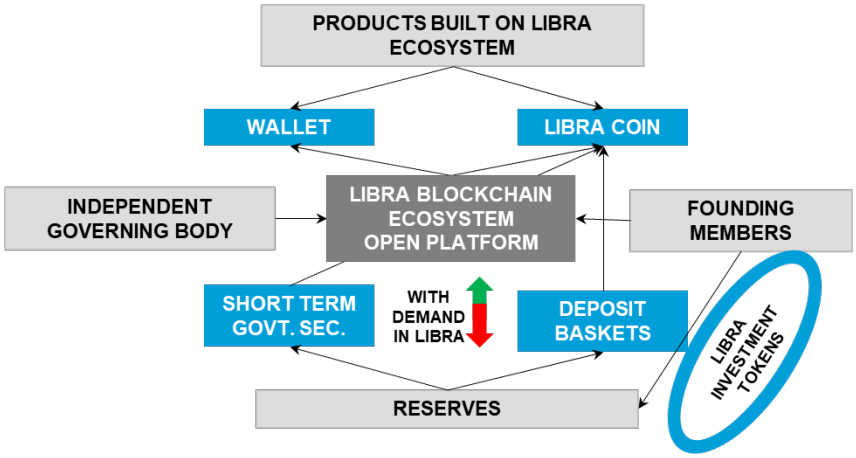
Diem is designed to develop a new type of payment network and eventually also infrastructure for not only payments, but also financial services. It is built on blockchain technology, which is believed to result in reduced transaction costs, especially when it comes to cross-border payments.

Diem is also designed to enable a very high degree of interoperability between different participants, whether these are banks, financial institutions, service providers, like wallet providers to consumers, payment service providers, etc. And can build an infrastructure layer on top of future national CBDCs.

Libra White Paper v1.0:

- **Two Tokens:** The white paper unveils two tokens (1) the stablecoin token called Libra, which is meant strictly to be used as a medium of exchange; and (2) equity in the project called Libra Investment Token.
- **Fiat Peg:** Every Libra created and in circulation, will be tied to a basket of major fiat currencies and backed by bank deposits and short-term government securities "in currencies from stable and reputable central banks".

Figure 45. The Libra Ecosystem



Source: Libra White Paper v1.0, 2019, Citi Research

- **Economics:** Interest on the reserve assets will be used to cover the costs of the system, ensure low transaction fees, and pay dividends to investors.
- **AML/KYC:** AML/KYC (Anti Money Laundering/Know Your Customer) will likely be done at the application layer and not the protocol layer. This means, users will have the option to interact with the network directly and pseudonymously without disclosing any personally identifiable information.
- **Open-Source:** Libra Blockchain will be open to everyone in order to build their own wallet, custody solutions, and add value through their services.

Libra White Paper v2.0: What's Changed?

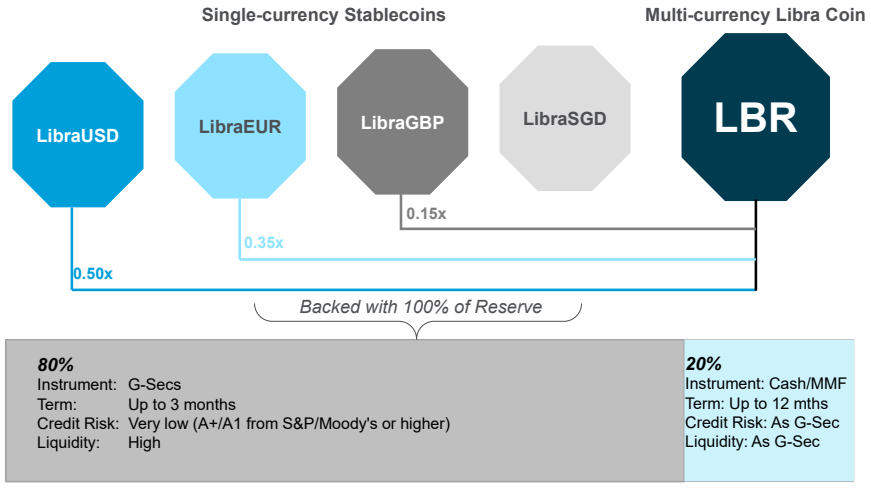
The Libra Association in 2020 published an update to its initial white paper from June 2019 (link), following feedback from regulators, central banks, and stakeholders. Key changes include: (1) introducing single currency stablecoins; linked to local fiat; (2) enhancing the compliance framework; (3) abandoning the transition to permission-less system; and (4) designing of Libra reserve. The association has also submitted its application to the Swiss FINMA for a payment system license.

- **Scaling Back Global Currency Ambitions:** White Paper v2.0 highlighted plans to create single-currency stablecoins (e.g., LibraUSD, LibraEUR, LibraGBP and LibraSGD) in order to complement fiat currencies and not allow multi-currency Libra Coin (LBR) to interfere with monetary sovereignty and monetary policy (if the network reaches significant scale).

  Aimed at mitigating concerns raised by regulators, Libra network announced that LBR will not be a separate digital asset, but a composite of single-currency stablecoins available on the Libra network. Diem Dollar will be the first coin available on the network and hoping to expand to new jurisdictions thereafter.

  The association has also provided details on composition of the Libra reserve — 80% comprising Government securities with up to 3-month maturity and very low credit risk (A+/A1 from S&P/Moody's or higher). The remaining 20% is to be held in cash, with overnight sweeps into Money Market Funds (MMF) investing in up to 12-month Government securities or similar credit risk/liquidity profiles. Diem will also have additional capital requirements and buffers to account for potential losses from credit market liquidity and operational risk. The reserve holding and related data would be published daily and regularly audited.

Figure 46. Libra Single-Currency Framework and Reserve Constituents



Source: Libra White Paper v1.0, 2019, Citi Research

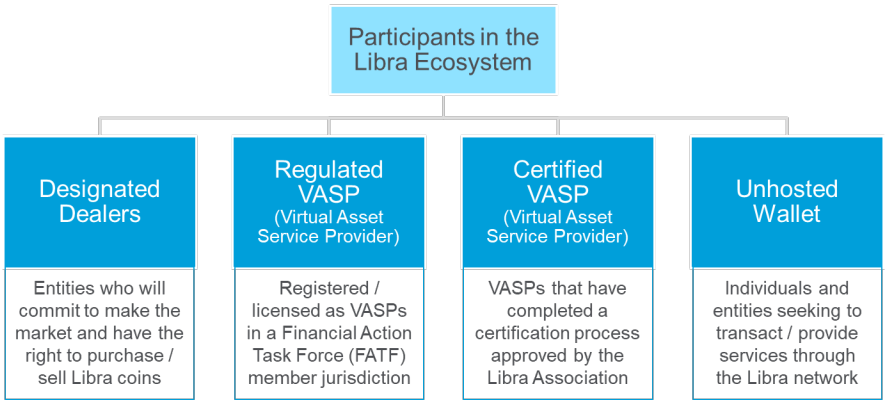
To further strengthen the payments system, the Libra Association is developing a regulatory framework to maintain capital buffers, in order to protect against potential losses from credit, market, and operational risks. Furthermore, in order to avoid or slow the speed of runs on the reserve under severe stress scenario, the Association is considering implementation of Redemption Stays and Early Redemption Haircuts.

This new approach is likely to seamlessly integrate CBDCs into the Diem network as they launch, thus eliminating the need to maintain the Reserve, reducing credit and custody risk.

- **Enhanced Compliance Framework:** The White Paper v2.0 identifies the need to develop a comprehensive framework for financial compliance to meet stringent norms on AML, CFT, and sanctions. For this, a new robust framework has been developed, breaking down the hierarchy of involved entities into four categories:
  - **Designated Dealers:** Entities that have the right to purchase/sell Diem Coins to Diem Networks. New coins will be created by Diem Networks and distributed only via designated dealers.
  - **Regulated VASP (Virtual Asset Service Provider)** including exchanges and custodial wallets, registered to perform VASP activities per 2019 FATF guidance. VASPs will be regulated in their home jurisdictions.
  - **Certified VASPs:** those have completed a certification process approved by the Association.
  - **Unhosted Wallets:** individuals or entities seeking to transact/provide services in the Libra network.

  The association aims to have the network initially accessible only to Designated Dealers and Regulated VASPs. Subsequently as necessary compliance processes are developed, other VASPs and unhosted wallets can be added. Membership of the Association consists of geographically distributed and diverse businesses and non-profit organizations.

Figure 47. Hierarchy of Entities Involved in the Libra Network



Source: Libra White Paper v2.0, Citi Research

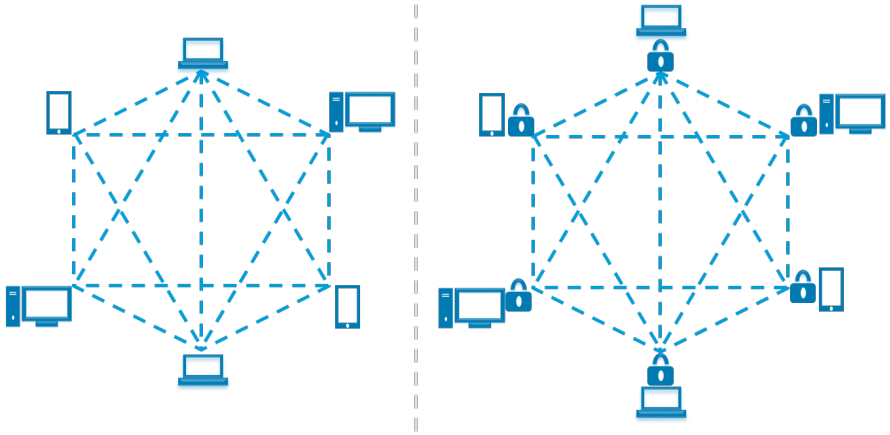
- **Abandons Plan to Transition to Permission-less Network:** A key regulatory concern in relation to Libra Associations' original white paper from June 2019, was the risk posed by a permission-less network and need to guard against unknown participants taking control of the system.

  Notably, according to the original white paper, the Libra Association planned to operate on a public, permissioned blockchain initially, but gradually shift towards a permission-less network over 5 years.

A permission-less blockchain would allow anyone to transact and join as a validator, i.e., no single entity was in control of it, making the system decentralized. Popular blockchains like Bitcoin, Ethereum and Litecoin are permission-less blockchains.

Libra 2.0/Diem acknowledged potential concerns on compliance and revised plans for a hybrid approach importing good economic properties of permission-less systems (i.e., the ability for anyone to compete), with a permissioned/ controlled perimeter.

Figure 48. Permission-Less versus Permissioned Blockchain



Public Blockchain: Permission-less
An open network system where all the devices can freely access without any kind of permission. The ledger is shared and transparent.

Private Blockchain: Permissioned
A user has to be permitted by the blockchain authority before he/she could access the network. The user might join only if he/she gets an invitation.

Source: 101 Blockchains, Citi Research

- **Design of the Libra Reserve:** The Association will establish custody agreements with a geographically distributed and regulated group of global institutional custodians. It will also establish operational procedures and will work with regulators to determine the best framework for determining composition of fixed weights for single-currency stablecoins that comprise the Libra Coin.

  While the revised white paper helps clarify several areas of the Libra coin and payment system, we believe some aspects still remain unaddressed, namely — economics of the association itself (i.e., investment from members) and impact of zero/negative rates on the operation of a reserve.

Use Cases for Diem

1. **Local Payment Systems:** Each country has their ecosystem. In smaller countries where the central banks need help on technology to build the payment infrastructure, Diem may be able to help. In countries which are building their own CBDC and have strong domestic technology players and ecosystem, Diem is likely to have less domestic success.

   It can also help in bringing a different experience to commerce. If Facebook is able to link the domestic payment systems that they are developing, they could power Instagram commerce and Facebook commerce via Diem (and the Novi wallet they are building on top of it).

2. **Become a White Label CBDC Provider:** The overall design is one that can support a transition and an evolution towards CBDCs. If a CBDC becomes available in any of the jurisdictions where Diem is operating, the network could integrate directly with the public sector effort and provide additional functionality and features when it comes to payments on top of the public sector rails.

   Diem network can provide an infrastructure layer, with greater programmability, on top of whatever the public sector provides via CBDCs. In the Diem white paper, it was clear that they are open to having a discussion with any Central Bank who would be interested in adding their currency as a stablecoin on their network. Diem has the potential to become a white label CBDC provider.

3. **Cross-Border Payments:** Global average cost for sending money is around 6.5% and even with smart remittances, it is around 4.2%, so there is massive room for improvement. Diem has the potential to reduce the cost of cross-border payments. If Diem can be applied to a global level, it will allow people to send money to each other in a cost-efficient way. Presently, cross-border payment fees can go up to double digits for emerging markets.

   Some of the traditional custodians will benefit because every Libra asset will be backed one-to-one with Reserve, listed in the Libra white paper. These will be held with traditional institutional grade custodians. On the other hand, remittance companies who are charging pretty high fees will be the losers.

   Diem could also bring cross-border interconnectivity between domestic payment wallets, including those operated by the same Big Techs operating globally.

Diem Members

Figure 49 lists the members of Diem Association. Most members will be running validator nodes on the network and kind of protecting its stability and operations on a daily basis. The network is designed to really foster interoperability and competition. The idea is to let consumers and especially merchants experience low switching costs, allowing them to move between different service providers without friction.

There will be many companies working on the application layer above the Diem protocol layer. Application layer companies, providing wallet services for example, will need to be regulated in their local markets.

Figure 49. Members of the Diem Association

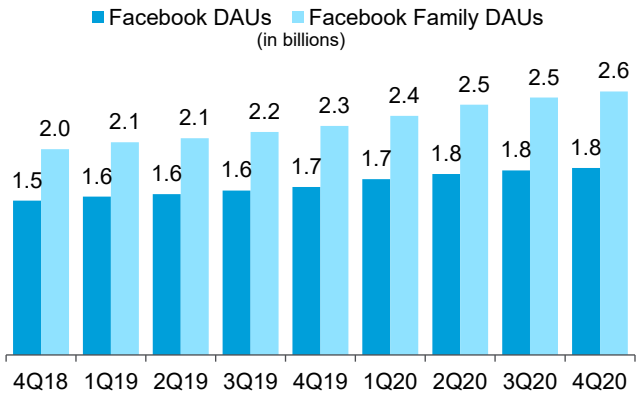
Company	*Industry*	Company	*Industry*
Anchorage	*Blockchain, Cryptocurrency*	**Mercy Corps**	*Non-Profit Organization*
Andreessen Horowitz	*Venture Capital Firm*	**Paradigm Fund**	*Crypto-focused Investment Firm*
Blockchain Capital	*Venture Capital Firm*	**PayU**	*Payments Company*
Breakthrough Initiatives	*Venture Capital Firm*	**Ribbit Capital**	*Venture Capital Firm*
Checkout.com	*Payments Company*	**Shopify**	*E-Commerce*
Coinbase	*Blockchain, Cryptocurrency*	**Slow Ventures**	*Venture Capital Firm*
Creative Destruction Lab	*Non-Profit Organization*	**Spotify**	*Audio Streaming Company*
Novi Financial (Facebook)	*Payments FinTech*	**Temasek**	*Investment Management*
Farfetch	*E-Commerce*	**Thrive Capital**	*Venture Capital Firm*
Heifer International	*Non-Profit Organization*	**Uber**	*Ride Hailing/Transportation*
iliad	*Telecommunications*	**Union Square Ventures**	*Venture Capital Firm*
Kiva	*Non-Profit Organization*	**Women's World Banking**	*Non-Profit Organization*
Lyft	*Ride Hailing/Transportation*	**Xapo Holdings Limited**	*Blockchain*

Source: Citi Research

A significant aspect of Diem is its link to Facebook via its Novi wallet. As of end 2020, Facebook has nearly 1.8 billion daily active users (2.8 billion monthly active users) and the numbers are even higher if we look at the number of users in the Facebook family of products (Facebook, Instagram, Messenger, and/or WhatsApp).

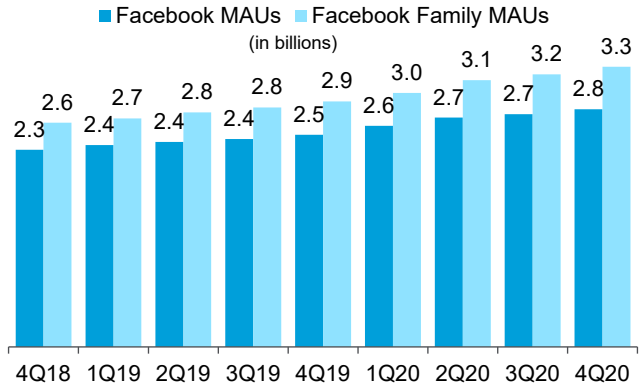
This should help Diem gain critical mass, especially in the early adoption phase, driven by the network effect of use within the Facebook family. In that case, it could indeed be a new day ("Novi Diem") for payments.

Figure 50. Facebook Only and Facebook Family (DAUs)



Facebook family of products include Facebook, Instagram, Messenger, WhatsApp
Source: Company Reports, Citi Research

Figure 51. Facebook Only and Facebook Family (MAUs)



Facebook family of products include Facebook, Instagram, Messenger, WhatsApp
Source: Company Reports, Citi Research

External Expert View: Henri Arslanian on Libra/Diem

Henri Arslanian
Global Crypto Leader
PWC

Henri Arslanian is the PwC Global Crypto Leader, the former Chairman of the FinTech Association of Hong Kong and an Adjunct Professor at the University of Hong Kong. Henri advises many of the world's leading crypto exchanges, investors, financial institutions and tech firms on their FinTech and crypto initiatives as well numerous governments, regulators and central banks on FinTech and crypto regulatory and policy matters.

Q: How important will be Diem be?

The announcement of Libra (now renamed Diem) was probably one of the most important developments we have seen in the crypto ecosystem since the launch of Bitcoin in October 2008. I truly believe when we will look back at the history of money in 20 to 40 years, Diem (Libra) will be a defining moment.

What was interesting with Diem (Libra), obviously, from the day it was announced, was that it catalyzed two big waves.

The first initial wave was it forced many people in financial institutions and industry players to start focusing on this topic. Libra literally brought digital assets on the agenda for any executive of a financial institution. They may not like it, but they had to at least understand its potential impact.

The second wave was a deluge of research papers from policy makers. A good example is the ECB. Since Libra 1.0 was announced, we have seen a number of academic papers come out from economists at the ECB. I would say some of these are the best that have been published so far.

Other policy makers started to focus on the topic as well, including the World Economic Forum, which released a toolkit for central banks on CBDCs.

Without any doubt, the one institution Diem (Libra) has impacted the most is the Bank for International Settlements (BIS). For the first time, the BIS hired a Head of Innovation that sits on the Executive Board. They have undertaken industry-wide consultations and published numerous policy papers analyzing the impact of not only Diem, but also stablecoins, CBDCs, and digital currencies more broadly.

Diem has many good use-cases including cross-border payments. Diem wants to make sending money globally as easy, fast, and cheap as sending a WhatsApp message or an email.

But realistically, at a national level, Diem's use-case argument is not as strong. If you look at most countries, payment systems for domestic payment and transfers generally work — maybe not perfectly, but they work. However, that is far from being the case in cross-border payments, especially in emerging markets. The average fee for sending money cross border is around 7% and can rise to double digits in emerging markets. This is something that Diem can fix.

Think about a domestic helper from Hong Kong, who is sending payments back to Indonesia or a construction worker in Saudi Arabia sending money back home to the Philippines. In my opinion, these are the corridors Diem is trying to tackle, and that is where we are likely to see the most activity initially.

Q: How does Diem fits into WhatsApp Pay?

I believe this is an interesting question. Notably, the Diem (Libra) white papers have made it very clear that they will focus on being regulated/compliant with various regulations including the Travel Rule (a recent FATF requirement) as well as other anti-money laundering (AML) requirements globally. As a result of being regulated, people will be able to use the wallet easily, but in a compliant way.

But Diem is also open source. Which means anybody can build any application on top of the Diem blockchain. This is different from some of the other platforms available today that are centralized. Also, Diem is based on blockchain technology, which enables several features like smart contract settlements or finality of payment, which are not possible with other centralized payments systems.

Surely Know-Your Client (KYC) and AML will be essential. However, one development I am watching is whether there will be an exemption for small payments, similar to what we have today with gift cards or micro payments.

Central banks are looking at this as well. For instance, the Bank of England recently stated that any CBDC they issue, should be capable of use for small value transactions without the need for KYC. This also allows for small transactions to be made offline.

Q: How might Diem interact with established crypto like Bitcoin and Ethereum?

The way I often ask this is if somebody goes on the Diem ecosystem, why would that person need to leave, if they can conduct their basic transfer and payment activities using the Diem ecosystem?

User convenience and experience are important, therefore if there are some serious frictions in the on-ramp and off-ramp processes, then that would be a challenge.

Generally speaking, Diem can be an on-ramp for people to conduct more activities using digital assets, including using cryptocurrencies like Bitcoin and Ethereum. We will have to see over the next few months how the interaction will happen. But I think the benefit of the ecosystem, when it's very convenient, could be very powerful.

Imagine if someone enters the Diem ecosystem, can make cross-border payments seamlessly, access cryptocurrencies, and even conduct basic financial services like borrowing or lending directly in that ecosystem.

If we look again at how we got to the first billion Internet users in the U.S., it was partly due to the work of AOL, Hotmail, and Yahoo free e-mails. But afterwards, a lot of new players and offerings came in and the ecosystem got stronger.

Same could happen here. One of the great things with Diem is that it is going to be open source. Literally, anybody can come and build on top of it. I think the one thing we may see is the rise of new FinTech offerings built on top of this open source infrastructure, which could even solve some of the problems we have been trying to tackle for a long time (e.g., financial inclusion).

Q: In the medium term, if we see a pick-up in the usage of Diem, what does this mean for other players in the ecosystem? What is the impact on other financial institutions that already exist in the payment space?

It is a question we have seen many financial service executives ask themselves. It will have an impact for sure. I really hope the era of an average 7% fee to send money cross borders comes to an end.

The questions will be: What is your strategy? How are you going to potentially deal with this new reality moving forward? You may love Diem/Bitcoin, you may hate it; but you need to have a point of view and a strategy to be ready.

The period we are going through is an historic one, not only for cryptocurrencies, but in the evolution of money. There will be winners and there will be losers. It all depends on how certain financial service providers react/adapt over the coming months and years.

Bitcoin and Cryptocurrencies

- The market value of cryptocurrencies (especially Bitcoin) has surged recently, driven by the digital gold/fiat currency debasement narrative. A big difference in 2020-21, relative to 2017, is the interest from institutional investors and corporates.
- Bitcoin has huge brand value in the cryptocurrency market due to its first mover advantage, a 12-year track record of not being hacked, and high profile backers, including Elon Musk and the who's who of the tech world.
- Valuing Bitcoin is an art and high risk. As with commodities, supply/demand analysis is key. Valuation approaches used include the stock-to-flow model and relative valuation (which is also used for gold).
- The challenges for cryptocurrencies, especially as a payment option, include price volatility, scalability, and energy consumption inefficiency. New cryptos/ stablecoins may help address some of these questions.
- We start with the 2008 Satoshi Nakamoto white paper that outlined how, using blockchain technology, you can have a peer-to-peer permission-less network to transfer value instead of a centralized authority as in traditional finance.

The Original Member of Crypto – Bitcoin

The Origin of Bitcoin

Bitcoin was first presented in a 2008 white paper, by its pseudonymous creator(s) Satoshi Nakamoto, titled "Bitcoin: A Peer to Peer Electronic Cash System" (link).

The October 2008 timing, amidst global markets melting down and the Occupy Wall Street movement, did aid the 'building a better financial system' narrative around Bitcoin, But in reality Bitcoin was a synthesis of decades of previous experiments and innovations by cryptographers to create Internet-based digital money that was not controlled by banks or governments and could be exchanged on a peer-to-peer basis.

Bitcoin was not created to fix a crisis or challenge any sovereign or state. Instead, it offered the option to address the diminishing trust by some in institutional solvency and gave them a new online payment system based on cryptographic proof-of-work. Bitcoin is a technological evolution of a process that started decades ago to diversify risk in processes established centuries ago.

This evolution of peer-to-peer digital money and finance continues today with Ethereum and various other blockchain-based protocols optimized for different classes of applications, which we discuss in passing in this chapter, albeit a more detailed discussion of decentralized finance (DeFi) is probably for another report.

How Blockchain/Cryptography Works?

Bitcoin miners are computers running the Bitcoin core software client. Each instance of the software maintains a copy of the Bitcoin ledger or database. The Bitcoin ledger is maintained in the form of a chain of blocks in which each block stores the cryptographic hash of the previous block (hence blockchain).

An owner of a Bitcoin, sends it to a receiver by signing a transaction and transmitting to the Bitcoin chain through a node. The transaction signature is created based on the (1) sender's private key; (2) receiver's public key; (3) transaction timestamp; and (4) transaction amount. The nodes verify the authenticity of the transaction.

All valid transactions are then put in a queue called 'Mempool' from where miners pull out the transactions and start bundling them in a block, the hash of which takes in individual transaction signatures, hash of the previous block and timestamp, and a random nonce to create hash of the current block.

The hash of the new block must meet some conditions set by the Bitcoin protocol — this is the cryptographic puzzle that miners solve. Each block requires solving a different mathematical puzzle chosen from a very large set of similar puzzles. Each block's problem is equally hard to solve. In order to solve this mathematical problem, a lot of computational power is used (and thus a lot of electricity).

The 'proof-of-work' is the computational power expended to create a hash of the new block that meets the conditions set by the protocol and it is achieved through brute force by trying out different values of nonce as the input for hash function.

Once the cryptographic puzzle is solved (Bitcoin protocol conditions are met), the miner then transmits the block to the network and other miners will verify it by looking for a random number that, once inserted into the hash function, yields the right number of leading zeroes in the output.

Once verified, the block can be added to the blockchain, and is distributed to all other nodes on the network. All the nodes in the network will update their copy of the Bitcoin ledger with this new block. The miner that mined the block will then be rewarded with a 'block reward' aka 'mined Bitcoins'.

After the block is added to the chain, every block added on top of it counts as 'confirmation' for the block. If the current blockchain is 625 blocks long and my transaction is in the 620th block — that means my transaction has 'five' confirmations.

It is referred to as a confirmation because every time another block is added on top of it, the blockchain reaches consensus again on the complete transaction history, including your transaction and your block. In other words, your transaction has been confirmed 5 times by the blockchain at that point.

The more confirmations your transaction has, the deeper the block is embedded in the chain and harder it is for attackers to alter it.

How Does a Bitcoin Transaction Work?

When an individual makes a bank transfer, the bank records and maintains that transaction and subsequent balance in an electronic ledger, which acts as a proof of transfer in case any party claims otherwise.

Bitcoin performs the same function of storing a record of all transactions and account balances on a distributed database. It requires each of the computers running on the Bitcoin network to validate and save these transactions onto the Bitcoin ledger, a copy of which is maintained on each Bitcoin node. This transaction data on the Bitcoin 'shared ledger' is maintained in the form of a chain of blocks secured by cryptography, hence the term blockchain.

Abstract from the 2008 White Paper:

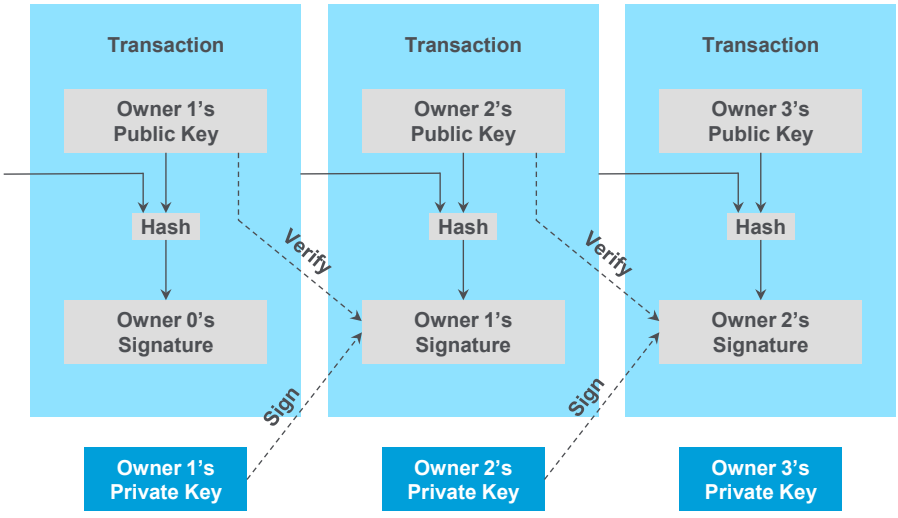
"A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending."

"We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work."

"The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers".

According to Satoshi Nakamoto, an electronic coin is a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of previous transaction and the public key of the next owner, adding these to the end of Unspent Transaction Outputs or coin. A payee can verify the signatures to verify the chain of ownership.

Figure 52. Illustrative Diagram of a Peer-to-Peer Electronic Cash System



Source: Bitcoin.org, Citi Research

Hashcash is a proof-of-work algorithm, invented by Adam Back in 1997 and employed in web applications as a denial-of-service counter measure tool. Bitcoin used hashcash as the foundation for its proof-of-work algorithm and at this point is most widely used as Bitcoin's mining function.

In proof-of-work, computers running blockchain software (nodes) compete to solve a very difficult cryptographic puzzle and the node that solves the puzzle becomes eligible for proposing the next block. The node that wins this contest is rewarded in the form of a block reward (newly minted cryptocurrency).

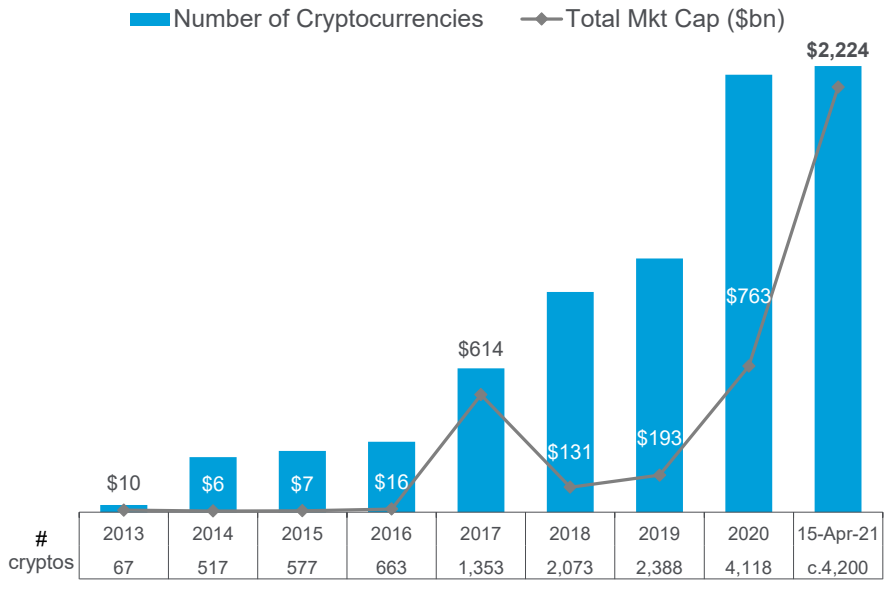
Proof-of-stake blockchains rely on the 'stake' that each blockchain node posts to become eligible for voting. The higher the stake, the higher say the node has in selecting the next block. This process is vastly more energy efficient than Proof of Work as posting a bond and voting does not require as much computing power.

Number and Market Value of Cryptocurrencies Surge

More than a decade since the creation of Bitcoin, cryptocurrencies have gained wider recognition. Currently, there are nearly 4,200 privately-issued cryptocurrencies available with some of the most recognizable names apart from Bitcoin being Ethereum and Litecoin.

Cryptocurrency prices have surged recently. The total market value of cryptos has more than tripled from its prior 2017 peak. Bitcoin remains the brand name coin, accounting for about 60% of the total cryptocurrencies' market value. Bitcoin prices surged to a record close in April 2021 (over 3.2x its 2017 peak).

Figure 53. Number and Value of Cryptocurrencies Over Time

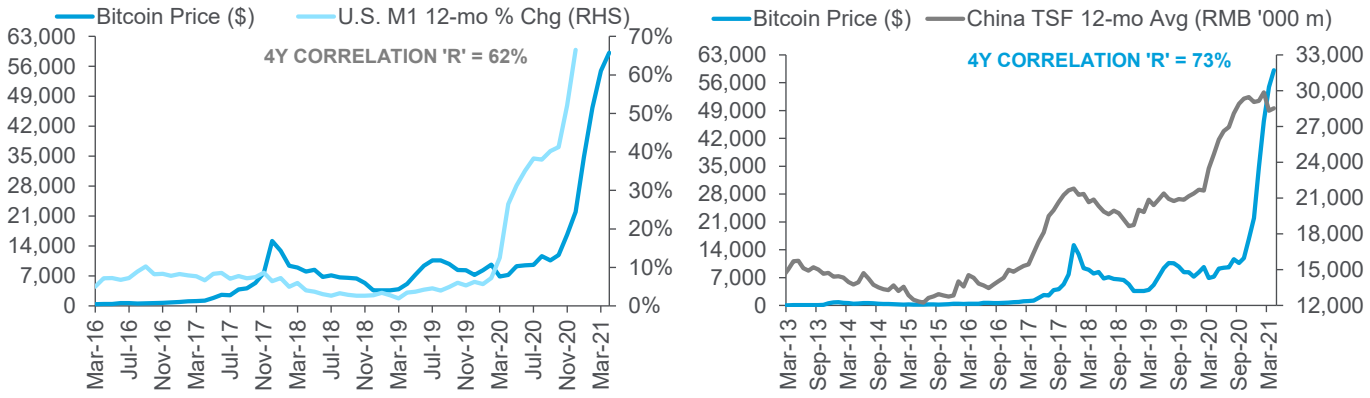


Source: coinmarketcap, Citi Research

The recent increase in Bitcoin price can be attributed to several factors, including:

- **Growth in money supply (M0, M1) and fiat debasement fears:** As we noted earlier in the introductory chapter of this report, there is a good correlation between Bitcoin's price movements and China's 12-month average total social financing (TSF), or credit creation, and change in U.S. M1 money supply. While central bankers are generally crypto skeptics, their actions may have supported investor interest in Bitcoin and peers. The growth in money supply has fed the 'buy BTC as a fiat currency debasement' hedge. More simply, in our view, more liquidity has pushed investors into increasingly higher risk assets.

Figure 54. Bitcoin Price (US$) versus U.S. Money Supply M1 12-mo % Change and China 12-month Rolling TSF



Source: coinmarketcap, Datastream, Citi Research

- **Portfolio shift towards riskier assets:** As central banks globally adopted an accommodative policy stance to support households and businesses during the pandemic, there has been a surge in financial flows into the capital markets and also into alternative investment opportunities including riskier stocks, cryptocurrencies etc. One notable difference in investor interest in crypto in 2020-21 versus 2017 is the larger number of institutional investors, based in money centers around the world, asking questions about crypto. In 2017, by contrast, interest was more retail oriented. Crypto has until recently been a retail asset versus an institutional asset.

- **Money for the social media age:** If all money is a social construct, Bitcoin and other cryptocurrencies appear well-suited to the social media age. Social media coverage, including from some leading technology entrepreneurs, celebrities, and influencers has helped raise the public awareness of Bitcoin and cryptocurrencies. West Coast venture capitalists and tech entrepreneurs were the early adopters of Bitcoin, but the scale and reach of recent social media boosterism, led by Elon Musk and others, is unprecedented.

- **Institutional and corporate demand:** Beyond factors mentioned already, Bitcoin and cryptocurrencies also received support from institutional and corporate moves into the space. A few examples include:

  – In 2021, PayPal customers (nearly 350 million worldwide) will be able to have a balance denominated in cryptocurrencies (without cryptos being actually delivered) and make payments at PayPal's 26 million merchants around the globe. Merchants will have no additional integrations/fees (link). Square had earlier enabled its customers to be have a crypto balance (link).

- Later in 2021, Visa will launch a crypto service to enable its clients to buy or spend cryptocurrencies using their Visa credentials, albeit the payment firm sees “crypto assets as more like digital gold” and “there’s less demand to spend bitcoin”.[15]

- Significant investments in creating institutional-worthy pre/post crypto trade market infrastructure (exchanges, custodians, cold-storage) have enabled large order execution, compliance, and asset protection. In addition, in some but not all countries, the regulatory infrastructure is also more institutional worthy.

- Tesla purchased $1.5 billion worth of Bitcoin as part of an effort to “diversify and maximize returns on (their) cash” held in corporate treasury. Tesla simultaneously announced it would start accepting payments for its products in Bitcoin, albeit this would be “subject to applicable laws and initially on a limited basis”.[16]

Valuing Bitcoin is an Art

Cryptocurrency, especially Bitcoin, derives its value from the very network it runs on — decentralized, censorship-resistant, and immutable. Bitcoin has dominated the crypto-narrative and commands a very high brand value in return for providing a censorship-resistant P2P payment network that has now been tested for a dozen years.

There are several challenges in valuing cryptocurrencies as the economic characteristics of cryptocurrencies vary widely. Bitcoin is more of a digital commodity whereas certain crypto tokens, such as those issued for raising venture capital, can have equity-like characteristics.

In our view, utility is the key to valuation. Because Bitcoin means different things to different people, establishing a valuation is difficult. Long term, Bitcoin as a digital payments mechanism has a different value, potentially larger, than Bitcoin as a form of digital gold.

Digital Gold as an Analogy

To the extent these outcomes are not mutually exclusive any Bitcoin valuation could possibly include elements of both, but even the strongest proponents of crypto have to accept there are already incumbent assets in both of these areas and it seems unlikely to us that crypto assets will fully displace them in the near future.

If we take the narrow use case of Bitcoin, or another crypto, fitting into the ‘digital gold’ position then, valuation can be estimated by comparing it to the global gold stock. Total gold value today is approximately $9 trillion, of which just under half is held as jewelry, with about 40% for investment purposes and the rest for other reasons.

[15] Bambrough, B., "Visa Reveals Bitcoin and Crypto Banking Roadmap Amid Race to Reach Network of 70 Million", Forbes, February 3, 2021.
[16] Kovach, S. "Tesla buys $1.5 billion in bitcoin, plans to accept it as payment", February 8, 2021

However, while 'digital gold' is the prevailing predominant Bitcoin narrative, it is unclear to us why from a valuation perspective this helps us determine a price. After all, what if Bitcoin doesn't stand the test of time — either because cryptocurrencies don't last or even if they do we find Bitcoin is replaced by a coin with greater utility.

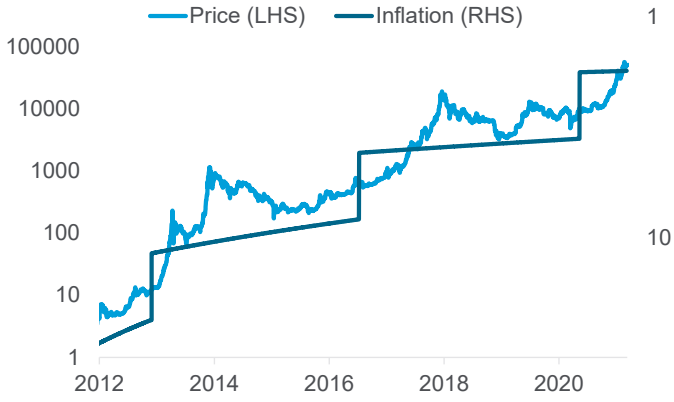
On the flip side, maybe it will in the future be possible to construct a wider use case for crypto beyond 'digital gold'. Digital payments segues naturally into some form of current/checking account and crypto bulls end up comparing the cryptocurrency world not with gold but 'money with aero maturity', a much larger segment.

Stock-to-Flow Model

In the short term, Bitcoin is still undergoing a period of price discovery. One simple and popular approach to modelling Bitcoin pricing is called the 'stock-to-flow' model. Simply put, this models the price of a Bitcoin as inversely related to the rate of Bitcoin inflation — i.e., how quickly is the stock of Bitcoin expanding.

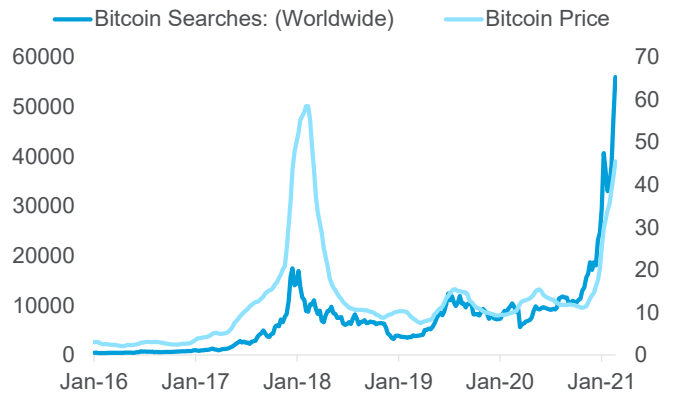
While there are various tweaks that can be made to the stock-to-flow model, and the model clearly breaks after the mining reward falls to zero, and we can debate whether scarcity drives value, as a simple model it seems to have some explanatory value (see Figure 55).

Figure 55. Simple Illustration of Stock-to-Flow. Bitcoin Price ($, RHS) Seems to be Inversely Correlated with the Rate of BTC Inflation (% LHS, Inverted)



Note: Data series is logarithmic
Source: Datastream, Citi Research

Figure 56. Google Searches for Bitcoin (RHS) Seem Correlated with Bitcoin Price ($, LHS)



Source: Google Trends, Datastream, Citi Research

How Does Demand Fit into the Equation?

Certainly, the missing part of the stock-to-flow model is demand. This is difficult to estimate and the numbers that come from exchanges are often unreliable. A simple model of demand being proportional to interest as expressed in Internet searches again seems to have some explanatory value (see Figure 56).

There are of course questions as to whether interest (and demand) is a leading or lagging variable to price. We believe there is a feedback mechanism where a higher price leads to more interest and hence a higher price. That causes a virtuous cycle on the way up until inflows are exhausted and then we see a vicious circle on the way down and with a still poorly defined end use case the peak-to-trough variation can be extreme.

Beyond Bitcoin

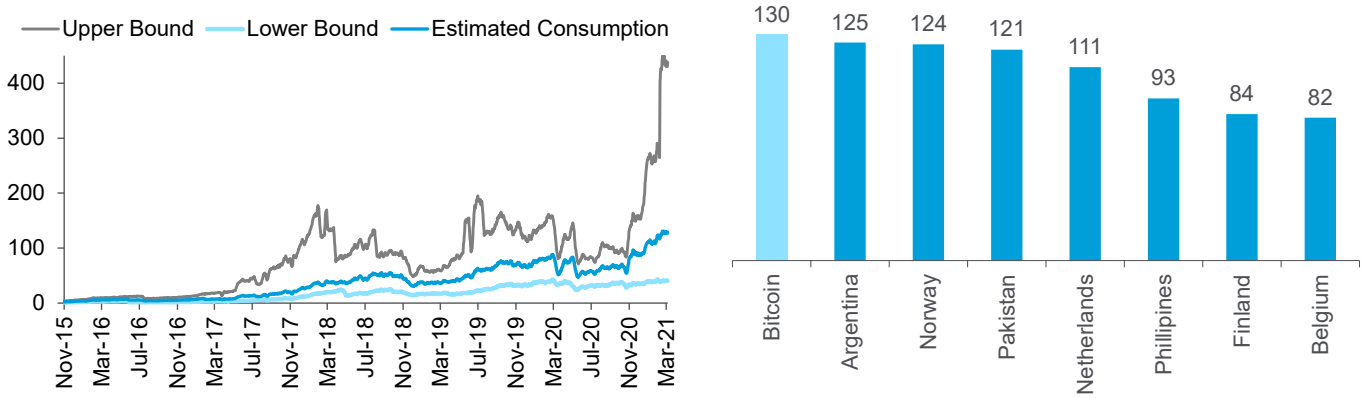
Bitcoin dominates the cryptocurrency market due to its first mover advantage in the decentralized/uncensored P2P network, a 12-year track record of not being hacked, and various popular narratives created by early adopters. These narratives create a potentially large brand value for Bitcoin, which can be attractive and even valuable for investors or consumers interested in the space.

However, it is important to look at technological advancements beyond Bitcoin in terms of applications, environmental factors and adverse regulatory actions in countries like Nigeria and India.

Moving Towards a More Sustainable Network

There is ongoing debate around Bitcoin's energy intensive proof-of-work mining method. As the price of Bitcoin has increased, so has its energy consumption and the median estimate for the Bitcoin network's annualized electricity consumption has increased to around 130 TWh, higher than many countries (Figure 57).

Figure 57. Annualized Bitcoin Electricity Consumption: Over Time (Left) and versus Select Countries (TWh) (Right)



Note: Lower/Upper bound estimate correspond to assumption of minimum/maximum total electricity consumption. Estimated consumption is 7-day moving average of annualized pervious power estimate.
|Source: CBECI, Citi Research

As mentioned previously, that's actually part of the design of Bitcoin; the network's security in part rests on the need to expend resources to contribute. However, that is a problem in a world that is increasingly aware of the impact of investment decisions on the environment.

At the very least it may deter some investors from holding Bitcoin and it could spur government intervention to ban mining, as seen in parts of China. For their part, advocates for Bitcoin point out that its energy consumption is a target for criticism because it is measurable, while energy costs in other assets are hidden.

The use of renewables may form part of the solution. According to the Cambridge Center for Alternative Finance, 76% of miners use renewable energy in some capacity and almost 40% of all mining is based on renewable energy.[17] Also, its decentralized nature may allow Bitcoin miners to optimize energy consumption.

[17] University of Cambridge, 3rd Global Cryptoasset benchmarking study, Apolline Blandin, Dr. Gina Pieters, Yue Wu, Thomas Eisermann, Anton Dek, Sean Taylor, Damaris Njoki, September 2020.

In an attempt to square the circle, and keep the benefits of a decentralized cryptocurrency with more limited energy costs, many new networks such as Polkadot use a proof-of-stake algorithm, which is less energy intensive than the proof-of-work algorithm used by Bitcoin.

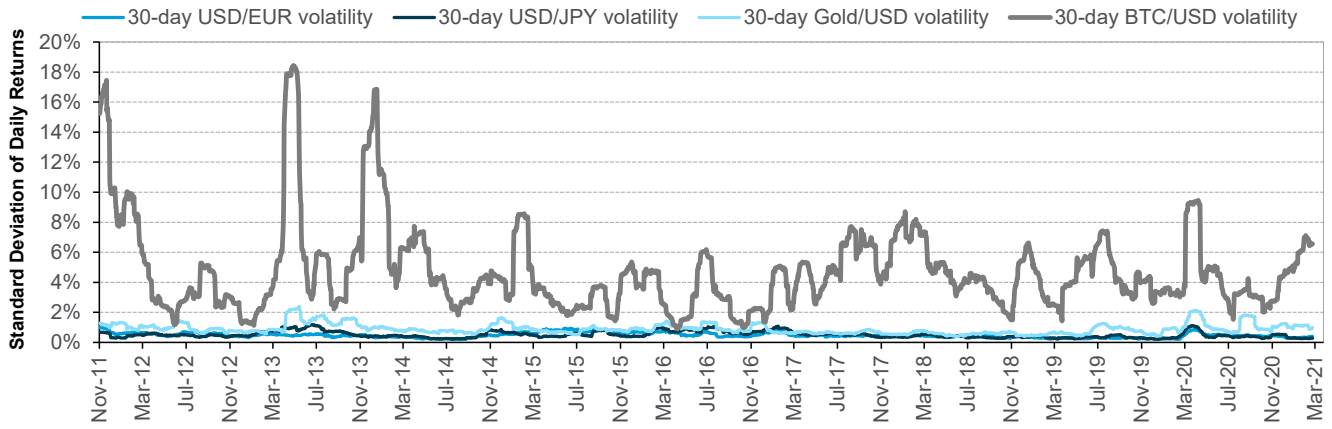
The second most popular cryptocurrency by market value, Ethereum, is also migrating from proof-of-work (PoW) to proof-of-stake (PoS). Ethereum 2.0 and the move from PoW to PoS has been ongoing for a while and the process has had many delays and is complex. Time line for completion: “next few years”.

PoS will mean no mining in a traditional crypto sense. It should lead to higher capacity, more usage, and more transaction. A more valuable network should lead to more valuable Ethereum, but the risks could be high.

On Volatility and Inequality

As with the surge in Bitcoin prices, its volatility has also witnessed a significant rise in recent months. In fact, Bitcoin price volatility continues to be nearly 10x higher than major exchange rates. For comparison, the average volatility of Bitcoin (in USD terms) is about 5%, while that for major currencies (USD/EUR, USD/JPY) averages 0.5% and gold averages about 1%. Bitcoin’s extreme volatility is one of the key criticism that adversely affects its potential role as a medium of exchange and store of value.

Figure 58. Volatility of Bitcoin versus Gold versus Fiat Currency

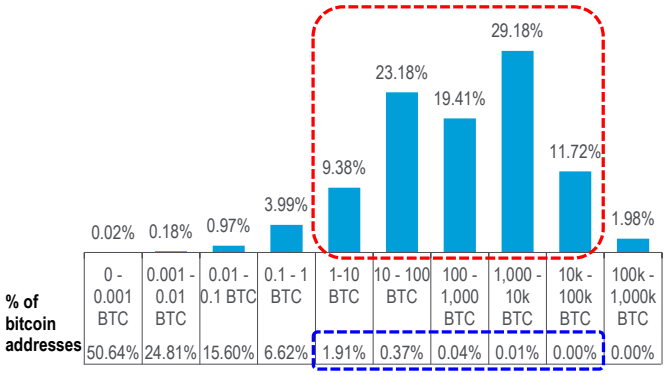


Note: We define volatility as the standard deviation of daily returns for the preceding 60 days.
Source: DataStream, Citi Research

Distribution of Bitcoins across network participant addresses suggests ownership is highly concentrated, with just over 2% of bitcoin addresses controlling nearly 93% of all Bitcoins (Figure 59). However, one Bitcoin address may not represent an account, as one user may control multiple addresses and one address may hold funds from multiple users (e.g., exchange address may hold funds from several users).

Figure 60 below takes into consideration addresses that belong to exchanges and miners. This suggests the distribution is less concentrated with entities holding over 1,000 Bitcoins together control around 31% of the Bitcoin supply, according to data from Glassnode. These are mostly institutions, funds, custodians, Over-the-Counter (OTC) desks, and other high net worth individuals. Meanwhile, entities holding up to 50 bitcoins control nearly 23% of the supply, and likely represent retail investors.

Figure 59. Bitcoin Distribution



Source: Bitinfocharts. * Data as of Feb. 2021

Figure 60. Bitcoin Supply Distribution, Jan. 2021

Source: Glassnode

Ethereum and DeFi

Decentralized Finance (DeFi) extends Bitcoin's original idea of peer-to-peer (P2P) electronic cash by enabling complex P2P, mutualized, financial instruments and applications that run on smart contracts on public permission-less blockchains

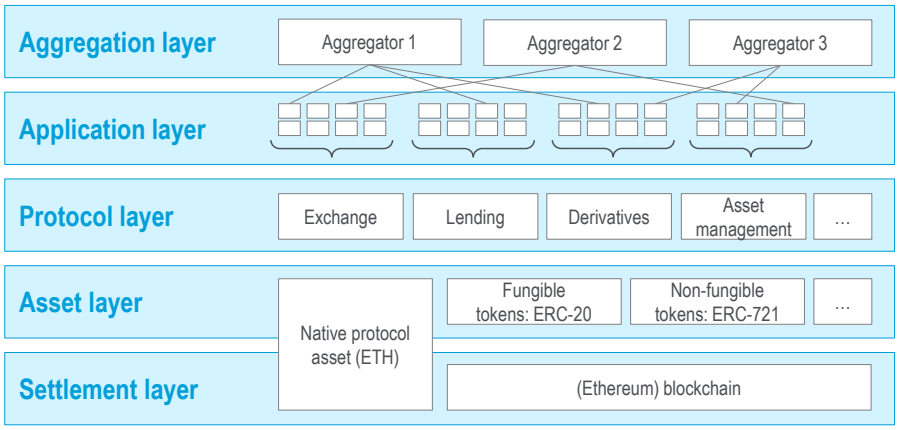
Today, most DeFi applications are built on the Ethereum blockchain. Ethereum (ETH) sets itself apart from Bitcoin by providing a software development platform for general purpose peer-to-peer applications, especially financial applications. The original Ethereum white paper envisioned such complex financial uses-cases.

DeFi leverages core principles of the Ethereum blockchain to increase: (1) programmability of financial contracts; (2) financial security and transparency; and (3) unlock liquidity and growth opportunities. Applications include Collateralized Lending (e.g., Aave) and Automated Market Marker (e.g., Uniswap).

Total amount of funds (US$ and ETH) locked in DeFi is a good proxy to ascertain its accelerated adoption. Total value locked in DeFi in November 2020 was ~$12 billion, which has increased over 4x to ~$45 billion in March 2021 with overall market capitalization of DeFi tokens rising to over $90 billion (link).

Increase in volume locked in DeFi over time represents growing confidence among consumers to place money in smart contracts to interact with new financial tools. Rapidly rising aggregate market capitalization of tokens issued by DeFi projects, indicate current investor enthusiasm for long-term potential of DeFi applications.

Figure 61. The DeFi Stack



Source: Federal Reserve Bank of St Louis, Citi Research

MakerDAO: The Decentral Bank

At the heart of the DeFi ecosystem is MakerDAO, one of the oldest and most sophisticated projects on Ethereum. Maker is a complicated system of interlocking smart contracts that enable collateralized loans paid out in a stablecoin.

For owners of crypto-assets such as ETH (the native coin of Ethereum), Maker is a means to unlock liquidity by posting their coins as collateral. For everyone else, it's the source of a blockchain token known as Dai, a U.S. dollar (USD)–pegged stablecoin.

Maker can be thought of as a digital pawn shop, where users post something that is already valuable in exchange for a cash loan. If they repay that loan with the required interest, they get their asset back. If they default, or if the collateral value falls below a predefined threshold, the collateral is automatically liquidated.

You can also think of MakerDAO as a perpetual repo market for digital assets, one that prices the collateral in dollars and gives loans in Dai. Depositors who wish to borrow money first transfer their collateral from their own wallet to one controlled by the system.

Although each borrower gets their own vault — the official term for the blockchain address where each borrower's collateral is locked up — individual loans are not backed by individual vaults. Instead, all of the outstanding debt is backed by all of the available collateral.

Unlike fiat-backed stablecoins (such as the proposed Diem) that are backed by cash held off-chain, Dai is backed by the pool collateral held by MakerDAO's smart contracts, akin to so-called commercial bank money, which is backed by deposits or cash.

Benefits of DeFi

The benefit of DeFi is the open financial platform on top of which all projects reside. Openness enables greater innovation and competition. It also allows uninterrupted interoperability. Any user can move capital seamlessly between Maker, Compound, Uniswap, and UMA in minutes and with minimal fees. Other benefits include the following:

- **Programmability:** Everything from a simple lending solution to a complex derivative product can be programmed into smart contracts that hold participant collateral in escrow and execute outcomes in a trustless fashion.
- **Transparency:** Smart contracts are open source and transparent. Because all deposits and collateral are handled on-chain, important numbers such as leverage ratios and margin requirements can be audited by anyone in real time.
- **Permission-less:** Any user can access DeFi solutions. Since there are no minimums, DeFi can be empowering for the poor/underbanked — constituencies often left out of the legacy financial system due to cost constraints.
- **Non-custodial:** Assets are held by either users or smart contracts. There is no centralized custodian who may be compromised.
- **Lack of intermediaries:** Eliminating middle layers results in higher yields for savers and lower cost for borrowers.

Challenges and Limitations of DeFi

The biggest challenge to the DeFi ecosystem is regulatory. Pseudonymous usage means that important laws such as the Bank Secrecy Act cannot be enforced. The decentralized nature of many DeFi projects also means there is nobody to hold accountable (or punish) for misdeeds. Other challenges and limitations include:

- **Complexity:** Protocols such as Ethereum are hard to comprehend, and DeFi solutions multiply the complexity, requiring understanding of complex technical and financial models. This also increases risk of unforeseen “black swan” events.
- **User Interface, Experience:** Most DeFi projects are relatively new and have not had time to develop the friendly user interfaces common in traditional financial services.
- **Liquidity:** Although growing, the amount of liquidity available is insignificant compared to traditional solutions.
- **Technical Risk:** If smart contracts are not coded properly, they could make mistakes or be hacked. The immutable nature of the Ethereum blockchain makes it impossible to undo faulty transactions. This challenge is compounded by the relative lack of maturity of the underlying technology, leaving room for potential glitches.
- **On-ramps and Off-ramps:** Limited interoperability with the existing financial system impedes adoption.

It is worth noting that traditional financial service providers offer more than just trust. They have spent years (if not decades) building reputations for understanding complex market dynamics and knowing how to adjust under pressure.

DeFi projects have yet to build up this sort of institutional experience. They are not only vulnerable to unforeseen technical issues such as a bug in smart contract code, but also unforeseen market developments.

External Expert View: Ajit Tripathi

Ajit Tripathi
Head of Institutional Business
Aave

Ajit Tripathi is the Head of Institutional Business at Aave, one of the world's leading decentralized finance platforms. He is also the crypto co-host of Breaking Banks Europe Podcast and a Columnist for Coindesk. In his prior roles, Ajit has consulted on Banking and Payments Partnerships for Binance and Paxful, led the FinTech practice at ConsenSys and co-founded the UK Blockchain practice for PwC. Prior to embarking on his blockchain/crypto career, he served as Head of Risk Data Technology at Barclays Capital, and Head of Risk IT in Asia for Goldman Sachs. He has an MBA from IMD and a Bachelors in Electrical Engineering from Indian Institute of Technology, Kanpur.

Q: Tell us about the history of cryptocurrencies, digital assets, and the financial industry.

It is a complex history. The history of Bitcoin starts from the Lehman crisis and the Occupy Wall Street movement. In fact, if you go back to the Bitcoin genesis block, which is the first piece of data that was ever mined in Bitcoin, it's got a coded message saying, "Chancellor on the brink of another bailout."

Bitcoin was not the first experiment of this nature. There is a long history of trying to build Internet-based money all the way from Netscape and Marc Andreessen. A lot of those experiments went on for a long time. Bitcoin's predecessor was Hashcash, which uses the same cryptographic algorithm as Bitcoin.

Bitcoin was the synthesis of quite a few technologies and experiments that had been done before, and it really took-off in a way that other experiments had not. The reason is Bitcoin was the first experiment where you could essentially get something that was incorruptible — a piece of data that could not be copied.

Since you could not copy this piece of data that was shared on a decentralized ledger, you could assign it some value. Let us say you have an email and that email can be copied 'n' number of times, then each of the copies effectively has a value of zero. Likewise, if you can copy a dollar bill, then the dollar will have a value of zero.

Bitcoin created a way of producing uniquely identifiable data that would be assigned to an address or a cryptographic key pair, and therefore to an individual. In the early days there were very few uses/users of Bitcoin, except maybe a few users in the underground economy.

The first time Bitcoin was used for a mainstream transaction was when somebody paid 25,000 Bitcoins for a pizza. I hope it was a really good pizza. I think Silicon Valley venture capitalists/technologists were early to see the value and we have come a long way since then.

There is now a variety of privately-issued digital assets. Ultimately, crypto is just a class of technologies that relies on blockchain cryptography. Different cryptographic assets have different properties, some are more like equity or debt, Bitcoin is much more of a digital commodity and it should be valued as such.

Q: How many Bitcoins are there in the world and how close are we to mining the last Bitcoin?

It depends on who you ask. We are supposed to get to 21 million Bitcoins in the world, and I do not want to be 'expelled from Bitcoin' for saying this, but a paper from Professor Arvind Narayanan at Princeton, suggests that the Bitcoin network may or may not be secure after the mining rewards run out in 2040.

I do not know how big that risk is, but there is a definite risk after the mining rewards run out and all 21 million Bitcoin have been mined. That is why some of the other networks (e.g., Ethereum), has an inflationary policy. Rewards never run out, and you secure the network irrespective of transaction volume.

Bitcoin miners are rewarded in two ways: one is block rewards: allowing them to sell Bitcoin at a profit; and the second is transaction fees. Every time I send a Bitcoin transaction, I have to send a small fee and this is supposed to be the only incentive to pay for mining after the rewards run out, but we will see how that works or if Bitcoin will see a change.

Miners today rely heavily on block rewards and the profits they make in good years. It is a boom and bust business. In bad years, you lose a lot of money. Some miners outside of China have a lot of debt from the bad years we just experienced, and they are hoping to make good on that. It is a very cyclical business.

There is a very strong belief in the Bitcoin community that there will never be more than 21 million Bitcoins. I do not have a view on this, because there is quite a bit of simulation and mathematics that goes into it and ultimately Bitcoin is software that can in theory be changed.

In practice, the value of Bitcoin is based on the 'scarcity' narrative, and changing the software to issue more Bitcoin will likely not be accepted by Bitcoin holders.

Q: In your view, what makes Bitcoin more like a digital commodity, what would make other crypto assets more like digital equity or debt?

Technology needs to be demarcated away from underlying economics. In 2017 many Initial Coin Offerings (ICOs) came online, and a lot of tokens were issued by private entities that were looking to raise capital for effectively venture investments. SEC took a stance that many of these were effectively equity securities. Subsequently, legal structures like Simple Agreement for Future Equity (SAFE/SAFT) have been used to issue such tokens.

Bitcoin's economic properties are more like commodities. Mining is the act of solving a cryptographic problem. It takes a lot of fixed capital similar to digging for oil and takes quite a bit of operating costs similar to the electricity you would have to pump into a mining rig and the labor you would have to invest.

A lot of times people who say, Bitcoin has no value, come from equities or fixed income backgrounds, whereas commodity analysts tend to understand Bitcoin quite easily, because it has exactly the same underlying mechanics and economics. The CFTC said in 2015 that Bitcoin is effectively a commodity and not a security.

Q: What about currency characteristics? Gold and silver are considered both a commodity and currency. Would you consider Bitcoin the same?

It is a philosophical debate to some extent. In my book, money is debt and currency is generally debt issued by sovereign government, which can be used to pay taxes, i.e., settle debts public or private. If you listen to old-timers, Bitcoin is supposed to replace the U.S. dollar and is supposed to be the dominant currency in the world and the main medium of exchange, but that is not quite how it has actually happened.

At the same time, Bitcoin is in fact the unit of account for the crypto community. Every time I log into Binance or any other exchange, I see my balance in Bitcoin, not in U.S. dollars. Everybody in the crypto world cares about what their net worth is in Bitcoin, not in dollars.

What are these applications? When Bitcoin started, Satoshi's vision or the white paper was about creating peer-to-peer electronic cash. It was supposed to be used for payments. It was supposed to be a censorship-resistant payment network that is independent of governments, and it is still used as such.

Whether in the early underground economy or later on in Nigeria, Lebanon, and Argentina where currencies have been rather unstable, Bitcoin has actually been used extensively as a medium of exchange or as a payment system. Absolutely customers in Nigeria, Kenya, and elsewhere definitely use Bitcoin for payments.

Over a period of time however, the crypto narrative has shifted from P2P e-cash to “the dollar is going to crash as central banks keep printing more money”. As a result in 2020, this digital gold narrative really clicked with many people, as M1 and M3 growth shot up due to the extraordinary amount of monetary stimulus and signaling by central banks that they were willing to print unlimited amount of money.

Now if that narrative is not actually held by reality — if the U.S. does not see a lot of inflation and the dollar retains its value, then maybe institutions will adjust their perspective. But even then Bitcoin is starting from such a small base that the amount of growth that is possible is actually extraordinary.

Q: How would you value Bitcoins and other crypto protocols?

It depends on the cryptocurrency in consideration. As we noted, Bitcoin is more of a commodity. Since there are no expected future cash flows, price of any commodity is determined by demand and supply, which makes valuation very difficult.

Commodities analysts generally use 80 or 90% of the cost of mining a Bitcoin as the floor price of Bitcoin which currently sets the theoretical floor at around $8-$9,000. The market price of course is another matter. Some analysts use the 'stock-to-flow' model which is also used for estimating the price of gold.

Last but not least, social media is never short of technical analysts, astrologers, and early Bitcoin adopters who have their own idiosyncratic theories and narratives about what the price of Bitcoin will be one day.

Q: Why do we always talk about Bitcoin and not other cryptocurrencies?

There is definitely a lot more trust in Bitcoin than in anything else in the crypto space today. This is partly because Bitcoin has not been hacked for 12 years now while thousands of other cryptocurrencies have come and gone. A secondary reason for this trust is the overall regulatory clarity around Bitcoin. The CFTC has stated that Bitcoin is a commodity and the SEC has not challenged it.

Now, I do not think anyone has tried to estimate the brand value of Bitcoin. There is fundamental value and then there is this brand value. What is Apple's or Tesla's brand value? Bitcoin also has an extraordinary brand value.

Even Silicon Valley pundits like Chamath Palihapitiya or Jack Dorsey are essentially Bitcoin maximalists — they cannot think beyond Bitcoin and do not acknowledge other cryptocurrency innovations. In that sense, Bitcoin has some of those religious properties; and such strong sentiments are very valuable, if you are trading.

Anyone who touches crypto, looks at Bitcoin first. It is such a word that rolls off the tongue. I am very big on Bitcoin, but I came in it for the technology, and engineers always tend to struggle with this. The simplicity and the brand value of Bitcoin are beautiful and give it extraordinary reach/adoption.

Now technology has come a long way since. Ethereum is a smart contract platform. You can actually build complex applications like decentralized finance applications. There has been an incredible amount of innovation in Ethereum and there has also been an incredible amount of innovation since Ethereum.

But the market is not necessarily paying for innovation alone. First and foremost, it is paying for trust. Bitcoin was the first one, and Bitcoin platforms (e.g., exchanges) have gone through a lot of challenges/accidents and survived. Bitcoin is also most widely adopted.

Q: What are your thoughts on DeFi big picture? What do you think are the most interesting use cases?

Ethereum will likely be the second asset that has regulatory clarity, where the SEC has widely indicated is probably not a security, and has hedging instruments without which Wall Street cannot really actively participate in the market.

The CME recently launched Ethereum futures (Feb. 2021, link), which further enable this perception of regulatory clarity. I think Ethereum futures on the CME will create the foundation for institutions to buy/sell and create Ethereum actively for clients and their own book.

DeFi is a very interesting and complex topic. Overall though, DeFi is essentially an evolution of the same Bitcoin dream. The idea of Bitcoin was peer-to-peer financial services on the Internet. This is something Marc Andreessen wanted to do during the Netscape days, but the technology was not there.

Now with Bitcoin and blockchain, the technology is there to create decentralized peer-to-peer money. As a result, what we are seeing is applications which allow more complex financial interactions. You can do derivatives, lending on Ethereum.

Currently, I use my iPhone and plug into AT&T's network. Similarly, or at least that's what we are working towards, there will be this Internet-based infrastructure of financial services that can be embedded into applications in the future and those will be essentially distributed algorithms working on a Blockchain.

Q: What institutional changes have helped the crypto market?

PayPal is massive. PayPal has 345 million users around the world. PayPal's crypto announcement (October 2020, link) arguably marked a point where Bitcoin was seen as mainstream by institutions, hedge funds, and family offices. More recently, Visa announced it will consider using crypto for payments (January 2021, link).

Additionally, corporates like MicroStrategy and conservative financial institutions like Mass Mutual, buying Bitcoin as an inflation hedge has also created a certain fear of missing out among institutions.

Moreover, in the last two or three years, there has been a lot of investment into the creation of infrastructure that is institution friendly. I can hold Bitcoin in my wallet, but it is very easy to lose it. Crypto custodians like BitGo, like Paxos have been building regulated infrastructure. Then you have institutional venues like FalconX and others that can execute some large orders in a systematic way.

Q: To what extent do you see greater adoption of cryptocurrency as a threat to the current financial market structure?

The current payments infrastructure does not necessarily work so well. I do not want to pay 2.5% on every transaction to a network of acquirers, processors, and Visa and what not. If you are living in the U.S., wire transfers and ACH (Automated Clearing House) are costly and create a lot of friction for users.

It has been pretty clear that better technology is now available, whether it is for payment infrastructure or for consumer payments. It is not just blockchain. There is just much better technology around, whether it is for data analytics, transaction processing, scaling databases or to replace messaging in the SWIFT network.

There is better technology available, but this has not been really utilized. Whether it is point-of-sale systems, all the way down to SWIFT, all of these are really entrenched, not just because of regulation but also due to network effects.

It is not just cryptocurrencies that are trying to change that, but regulators too are trying to change that with the European Payment Services Directive (PSD2) and Open Banking initiatives etc. The U.S. has really been a laggard in this space, which is disappointing, but that is where stablecoins create a lot of opportunity.

U.S. payments infrastructure is a great disappointment. For some reason, we still have checks. Hopefully, blockchain and cryptocurrencies will provide a different experience of intelligent wallets and digital money tokens that have complex behaviors and can be used for different purposes.

Cross-border payments remain difficult and expensive for most people. I could go on all day, but cross-border payments are still painful and correspondent banking networks still have a lot of friction. Sure there are protections, but what is the cost of these protections if you exclude a lot of people out of the system?

There is an ideological side to this as well, and I am not neutral to it. I think the current entrenched players do not necessarily help open up greater access, especially where it is not profitable to serve certain customers without documentation and so on.

A lot of people are excluded out of the system because of lack of documentation in the wider world. Sure, we do not experience it living in the U.K. or the U.S., but it is a genuine problem for people around the world and India has tried to solve it with a digital identity system. Other countries that have not, are trying to.

Hopefully, the combination of these technologies, whether it's cryptocurrencies or others that have come online, will create a different experience.

I believe PayPal and Visa have done a lot of work in crypto. They have been looking ahead and they have been way ahead of the game. Visa is partnering with USDC. They are already thinking beyond what the world will look like when Visa is not just a card company, when this does not have to work through the current infrastructure.

Visa is already looking at it and saying — what does the future look like? In a mobile-first world, what will the users see? How will they interact with payments? How will they actually do transactions? How will they see their money? How do they experience money in their wallets?

Q: Do cryptocurrencies not consume significant amounts of energy? Should we be using it for transactions?

Everybody gets into Bitcoin first, but then you start looking at the technology and you say, wait, what else is out there? Bitcoin is very hard to program and extremely energy intensive to secure. Newer blockchain platforms such as Ethereum are either using or migrating to proof-of-stake algorithms which do not require extraordinary electricity consumption.

What we realized with Bitcoin is that it is prone to centralization, as in it requires expensive mining hardware, and then you create these mining pools, which are very difficult to run unless you have a lot of working capital and significant investing capacity and access to cheap electricity. This often leads to significant price volatility as miners sell their inventory on the market.

Bitcoin mining pools have become relatively centralized because of the economics of mining and research in this area is going on extensively. After all, we are 10-12 years old in this space, but technology has come a long way, and we are going to see a lot of experiments with proof-of-stake that will address many of these issues.

Bitcoin is not going to move away from proof-of-work, and there are experts who believe that proof-of-stake is never going to be as secure as proof-of-work. I have seen some simulations that argue otherwise. Hopefully we will move to more sustainable algorithms which do not require this kind of energy consumption.

Q: Can you explain proof-of-stake versus proof-of-work

Both proof-of-work and proof-of-stake are referred to by engineers as “Sybil Resistance” algorithms i.e., algorithms designed to select the next block for adding to a blockchain.

In proof-of-work, computers running blockchain software (nodes) compete to solve a very difficult cryptographic puzzle and the node that solves the puzzle becomes eligible for proposing the next block. The node that wins this contest is rewarded in the form of a block reward (newly minted cryptocurrency).

This system creates an incentive for people running blockchain nodes to devote more and more compute power to win more and more block reward. Running more computers requires more energy which leads to proof-of-work networks like Bitcoin consuming an extraordinary amount of energy.

In the case of Bitcoin, the network consumes more electricity than the whole of Netherlands today. This is partly why some environmentalists on social media were surprised by Tesla’s recent $1.5 billion Bitcoin purchase.

Proof-of-stake blockchains rely on the 'stake' that each blockchain node posts to become eligible for voting. The stake is a bond that a node has to post to be considered for voting on the next blocks. This bond can be 'slashed' or 'confiscated' if the node behaves against the rules of the network, or is offline for too long.

The higher the stake, the higher say the node has in selecting the next block. Nodes are rewarded for participating in the voting process in form of a 'staking yield' or additional coins. This process is vastly more energy efficient than Proof of Work as posting a bond and voting does not require much computing power.

Q: How will Diem (Libra) impact the crypto world? Also, how will CBDCs and DCEP impact the crypto world?

Diem (Libra) is an interesting experiment and Diem has built a very robust and well-designed technology which uses blockchain primitives (i.e., protocols) to prevent double spend without relying on an inefficient database like blockchain.

However due to the geopolitical impact, Facebook may have allegedly had on U.S. elections, the Brexit vote, and the Edward Snowden incident, I do not see European governments accepting money to be issued or controlled by an entity with a significant influence from Facebook.

Especially in Europe, but also in many other countries around the world, concerns about the impact of Facebook or another private company controlling money/digital identity and the systemic risks associated with large scale privately issued money are all too real and unlikely to disappear anytime soon.

CBDC is a very different idea from Internet-based money like Bitcoin, and the economic case for retail CBDC outside economies that lack functioning payment systems is still weak. In China, the use case appears to be to extend its geopolitical influence and also to avoid private companies dominating domestic payments.

Stablecoins like Circle's USDC provide the path to retail CBDC for developed economies but even in this area, currently there's very little demand for non-USD stablecoins and in spite of the vehement protestations and creative narratives of cryptocurrency enthusiasts, the U.S. dollar, in its many forms very much remains the unit of account and the reserve currency, even for the crypto ecosystem.

Q: How do you see the evolution of infrastructure addressing security, trust, compliance?

Custody is an incredibly competitive business. A lot of entrepreneurs saw that given the sheer number of exchange hacks, losses, and what we saw with Mt. Gox and others. Every year we have seen several hundred million or couple of billion worth of losses for the last 6-7 years due to hacks and thefts.

It was pretty clear that this infrastructure, as it existed, was not suitable for protecting customer assets, especially for investors managing other people's money. All of that infrastructure has become really mature with Bitgo, Paxos, Anchorage, Fireblocks and quite a few other names coming online with progressively better technology.

Some of their technology actually uses the same infrastructure (e.g., hardware security modules) that banks are very comfortable with, and have used for years, but also provide a lot of operational security controls and processes to prevent against human risk and insider threats on.

That entire field has become much more mature, thanks to extensive investment, talent and technology going into the custody space. Most recently banks have been building their own infrastructure as well. We are going to see banks play a role here, and custody is a natural function for banks to safeguard customer assets.

External Expert View: Monica Singer

Monica Singer
Decentralized Blockchain Solutions Expert

Professor Monica Singer was the first CEO of South Africa's Central Securities Depository (CSD), Strate (Pty) Ltd which she set up in 1998 until she resigned in August 2017 to work on decentralized blockchain solutions.

In October 2017, Monica was appointed as South Africa Lead for Consensys, being the biggest blockchain company in the world.

Monica also participates as:

- Board member of the South African Institute of Chartered Accountants (SAICA)
- Professor of Practice in the School of Accounting in the University of Johannesburg.
- Board member of the Accounting Blockchain Coalition which is defining market practices for accounting, auditing and taxes of crypto assets.

Q: Why did you switch from traditional finance to crypto and decentralized finance?

More than 20 years ago I was asked to transform the financial markets in South Africa from a paper-based market where checks and share certificates were the only way to settle the trades on the Johannesburg Stock Exchange (JSE) to a digital clearing and settlement system. In 1997, the JSE was doing 4,000 trades a day where the settlement of these trades took at last two weeks to take place.

By the time I left Strate, the central securities depository in South Africa, the company I created and ran for 20 years, the daily volume on the JSE was on average 350,000 trades a day with a 3-day settlement cycle with no failures to settle those trades every day. South Africa was then categorized as one of the top 10 financial markets in the world due to the efficiencies we had achieved.

In 2015, I read Satoshi Nakamoto's Bitcoin whitepaper and it changed my life once again. For years at Strate, I wanted to achieve more efficiencies but the market practices would not allow me to implement them. For example, the issuer never has access to real-time information on who is buying/selling. The investor has to rely on the broker/custodian banks to keep them informed on what is in the portfolio. Also, settlement is delayed by three days and there were many challenges in payment of complex corporate actions and even voting at Annual General Meetings — to name a few of the current challenges in the legacy financial markets.

Satoshi explained that the solution was to decentralize record-keeping and have one version of the ledger, i.e., the shared version of the truth. In this way, you could have real-time delivery versus payment — the issuer could see the ledger of the transactions on their stock real-time and the investor could have their own investment wallet and track transactions across counters, brokers and custodian banks (which would not be needed as trusted intermediaries) in real-time.

As the Internet would be used for these transactions, huge costs and complex implementations of technology changes (as the system was running mainframes and using SWIFT as the messaging layer), would disappear. The introduction of new technology would not only reduce costs, reconciliations, frictions, and the inefficiencies but would open up a whole new world of new products and services that could be combined with the real time settlement of any financial instrument and even new asset classes like the digital representation of art, metals and real estate.

The decision was clear, I had to resign, as I did not want to stay to re-arrange the chairs on the Titanic. I was very lucky that a couple of weeks after I resigned in 2017, Joseph Lubin, the creator of ConsenSys, approached me and asked me to join him. I have been with ConsenSys since 2017, and loving every moment of being able to create the Internet of value, using Ethereum and many blockchain applications across industries that will deliver the promises made/imagined in the Bitcoin whitepaper and later on in 2014 in the Ethereum whitepaper.

Q: Why is crypto big in Africa?

Africa is a melting pot of migration, remittances, and under-banking. People in Africa send and receive money across countries. People usually rely on family members and neighbors to send/receive money to/from other countries, which is cumbersome and very expensive. Traditional bank and payment rails work poorly intra-Africa. People who switched to crypto realized they can bypass middlemen, expensive money changers, banks and financial institutions.

Further, countries in Africa do not offer deposit insurance. People face counterparty risk when they hold money with banks. Many Africans are unbanked/underbanked, as they do not open a bank account or use bank transfers, as bank penetration remains critically low. Cryptocurrency enables transferring money via the Internet.

There are now many stablecoins (digital money that is collateralized by either fiat, crypto, gold, or even just a mathematical formula). These stablecoins are also becoming very popular as they are used as a unit of account and a medium of exchange. Cryptocurrencies, due to the fluctuation in value, are more a store of value and many argue that Bitcoin is a better store of value than gold.

Diem will be launched to 2.3 billion users of Facebook/Instagram/WhatsApp, and has the potential of facilitating money transfers between users without using a bank or money transfer entity. The use of Diem will ensure that the costs, delays, and risks faced by people in transferring physical funds from one country to another, will be reduced.

There are risks from stablecoins issued by private companies. For example, the popular stablecoin Tether — there is no clarity if this coin is really backed 1:1 with the USD dollar as the private company that issued it says that they are.

Other risks are that banks will be left out of this very lucrative business. Meanwhile, central banks will lose the influence, they currently have in setting monetary policy and controlling, in many countries that have exchange controls, the flow of funds.

It is imperative that central banks must consider implementing a CBDC at the retail level, so that depositors will be encouraged to use a digital currency that is a liability on the central bank's balance sheet and not private company issuing stablecoins.

In many countries in Africa, due to the inability of banks to offer efficient payment rails, the telecommunication companies have created a system call M-Pesa. The trouble with M-Pesa, even though it has served the purpose of facilitating payments, is that the liability of failure is in the balance sheet of the Telcos.

The way forward to reduce this risk is for central banks to issue CBDC and get the Telcos to be part of the second-tier that would have the interface with consumers. This is the reason we recently read that Pay Pal has announced they will be open to helping depositors open e-wallets on behalf of central banks. Facebook with Diem has also made similar moves. I believe this is the right evolution for Telcos in countries where mobile money has become the norm.

Q: How do you transfer money using crypto?

It is pretty simple, just like any other mobile wallet app. You download the app and get your KYC done using digital documents and/or biometrics. Once you are an approved customer, you can load money into the app from your bank account by doing a simple bank transfer to the account of the crypto exchange you chose to use. The amount transferred is reflected under the user's account in the app, which can be used to buy any cryptocurrency available on the app. Once you buy a cryptocurrency, you have the private key to that amount of crypto.

We have a mantra: Not your key, Not your crypto.

We encourage users to put their crypto in 'cold storage' (i.e., on an external USB with password protection, where the private keys are stored) and not keep the crypto under the custody of the exchange where you trade it.

For sending/transferring cryptocurrency, one needs to select the receiver's private key to which cryptocurrency needs to be transferred. After the transfer, the cryptocurrency will be reflected in receiver's wallet and gets deducted from sender's balance. This is done in seconds without any intermediaries working hours or costs.

Q: When did regulators get more informed about crypto? Are CBDCs coming?

The use-case of crypto picked up in 2016 and in 2017 when everyone thought they could get into crypto to get rich. Then the bubble burst and we went through what we call a crypto winter where the prices of all coins dropped dramatically and many people got out of the market.

It was only in 2018-19 that central banks and regulators started announcing their stance on crypto as the market for cryptocurrencies had started to attract more users and the institutional investors started to come into this market.

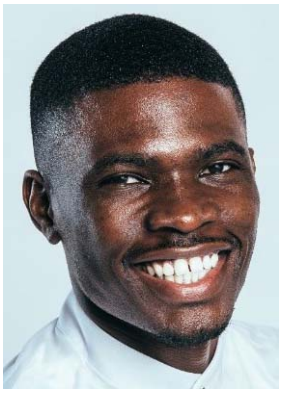
Then Facebook announced their intention to issue their stablecoin and that set the cat amongst the pigeons as all the risks I mentioned above become a possibility that central banks and regulators could not ignore. The concept of CBDC makes perfect sense for the central banks, especially in Africa, as it has all the things crypto has in terms of technology (e.g., blockchain) but still gives them all the control over it. CBDC will help regulators achieve much needed financial inclusion for the underbanked and unbanked population of Africa.

As CBDC will be implemented in the Internet of value, that in itself will allow users to benefit from the Internet and if the CBDC is implemented using blockchain technology, which it should, it will allow for the many benefits of programmable money and the ability for these digital currencies to be used interchangeable with other stablecoins and cryptocurrencies.

Micro payments and many other products and services will be available to anyone that has access to the internet either by mobile phone or directly by logging into a website. There are many solutions being built that will not require data to access the internet on real time so it will take into account the reality that in Africa not everyone has access to data or electricity.

We are at the beginning of the evolution of Web 3.0 and we cannot at this stage imagine all the new products and services that will become available to everyone. What is clear is that this technology will wait for no one and the sooner service providers get on into this bus the better for them to ensure that the users do not abandon them as they will have so many choices at the reach of their hands.

External Expert View: Temitope Alabi



Temitope Alabi
CEO and Co-founder, Afriex

Temitope Alabi is CEO and Co-founder of Afriex, which aims to make it easier to send/receive money cross border.

Q: What was the Eureka moment that led to your business idea?

Before founding Afriex, I used to travel around the world teaching governments and big corporates blockchain technology. I would often find myself having to pay for expenses with money that was sitting in my U.S. bank account. Traditional remittance products took so long and were so expensive that I knew I could do it better with crypto. I would buy Bitcoin from crypto exchange using my U.S. debit card and sell the Bitcoin in the foreign country using decentralized platforms like localBitcoins.com. Transfers were faster and much cheaper. I quickly realized that this could be a product.

Q: When did your business begin and how did it grow?

The app launched on the app store in October 2019 but was still nascent. Most of our customers were family members and people who knew us. In May 2019, we got into Y Combinator. At that point we knew we needed to grow so my co-founder and I sent a text message to 50 people each telling them about Afriex. COVID-19 was also a factor which meant many people were staying indoors and looking for online options for sending money back home. Over the following six months we grew 20x and now process millions of dollars each month in crypto remittances.

Q: Who are your peers and competitors?

Very few companies are doing exactly what we do, but there are two groups of companies that can be compared to Afriex. One group is traditional remittance providers like Transferwise, MoneyGram, and Western Union. These companies have built their businesses on top of the traditional banking system. This results in high fees and slow transfer times. Afriex uses stablecoins which move in minutes, not days, and allow us to source better exchange rates. The second group of companies are cryptocurrency exchanges which require users to be tech savvy in order to access fast/cheap global payments. Afriex makes this technology accessible for everyone. We built the product in a way that could go mainstream as quickly as possible.

Q: Why use crypto for foreign exchange (FX) trades?

Crypto exchanges are essentially open-markets for FX, which allow companies like Afriex to acquire FX at a better exchange rate than the ones that are set by banks.

Q: How big is crypto in Nigeria? What is the impact of the recent CBN ban?

According to various sources, Nigeria is one of the top 2 or 3 big markets for cryptocurrency in the world. Much of this is based on an inflationary national currency and strict capital controls. In a move to reign in all crypto activity, the Central Bank of Nigeria (CBN) has banned its member banks from working with cryptocurrency exchanges.

This has caused a big shake-up in Nigeria and in the crypto economy as a whole. Many crypto users are being driven to decentralized exchanges and peer-to-peer platforms, where they can transact without banks. Afriex is continuing to monitor the situation on the ground and hopes to see Nigeria return to its rightful place as one of the largest crypto-enabled countries in the world.

End Note: Tony McLaughlin on Fiat 2.0

Tony McLaughlin
Emerging Payments & Business Development
Citi Treasury and Trade Solutions

We are at an inflection point in the history of money, faced with different paths to modernize payments. For much of the previous 80 pages we outlined how different forms of tokenized digital money will grow in the coming decade, how they work and some of their individual pros and cons.

However, despite our view that the different manifestations of tokenized digital money will grow and likely gain share during the 2020s, we believe: (1) different digital currency form factors will co-exist, (2) it is not a zero-sum game, and (3) the overall pie of digital money, tokenized and account based, will continue to grow.

In this context, we also need to work on Fiat 2.0. The 21st century digital economy is always on and hyper-connected, but the banking system is not. We need to move the banking system from batch processing to real time and bring it in to the application programing interface (API) economy. The whole structure needs to sit on top of a good digital identity solution.

World of Platforms

We believe the Cryptopian thesis often begins by misdiagnosing the nature of the problems in the payment space.

For example, many say SWIFT is too slow and their network will be faster. This is a surprising argument as SWIFT uses electrons to send messages over a secure network with extremely high speed, security, and reliability. Distributed ledger technology (DLT) electrons are not faster than SWIFT electrons.

The real problems can be understood by comparing the reality of 21st century digital platforms that operate 24x365 in an interactive manner and the reality of the banking system, which is still largely based on batch processing and store & forward messaging.

When banks try to serve ‘always on’ platforms and their ecosystem users, the crunching of gears is all too evident. One way to think about the FinTech phenomenon is that these companies are building bridges between an analog clockwork banking system and modern digital platforms.

This issue will only become more pressing as more business is conducted on platforms. McKinsey estimates that some $60 trillion of economic activity will resolve into platforms by 2025. And these platforms are increasingly global, which further stretches their integration with a largely domestic set of banking infrastructures.

Digital platforms are going to service the financial needs of their participants on the supply side and the demand side. The race is on as to who will provide those financial services — the banks, FinTechs, or Big Techs themselves.

Fiat Currency Stack

We see no reason to alter the structure of central bank money at the base of the pyramid, followed by commercial bank money, and electronic money offered by regulated non-banks as a digital representation of client funds held within commercial banks.

Proposed changes to this structure are likely to have destabilizing effects. Payments is not solved by tinkering with this structure — this is a distraction from where the real work lies in different layers of the fiat currency stack. This stack is the set of domestic/international systems that enables modern money movement.

This includes Real-Time Gross Settlement (RTGS), Automated Clearing House (ACH), real time payments, card schemes, open banking, SWIFT, CLS, and e-money. But if we are to fix payments for the 21st century, we need to begin with the base layer, which is digital identity.

The Age of Consent

India's payment transformation has been built on top of the national ID scheme called Aadhaar, or 'foundation' in Hindi. Indeed our very concept of the fiat currency stack is inspired by the notion of the India stack. While Aadhaar's usage in payments and banking is under discussion, its catalyzing effect so far is undeniable.

Sweden is famously on the verge of becoming a cashless society, based on payment apps like Swish, which are based on a federated Bank ID. The Bank ID in Sweden is used by almost all adults on average 60 times per month to access government, banking, and other digital services.

Whether a national scheme like Aadhaar, a bank consortium like Bank ID in Sweden or a wider consortium like Itsme in Belgium, the foundation of a modern payments system and digital economy is the ability for consumers, businesses and machines to transact securely and with appropriate privacy through good digital ID schemes.

Next Generation RTGS

Central bank money is the cornerstone settlement asset providing finality and security of the fiat currency system. If national currencies are to stay relevant in the digital age, then the settlement asset needs to be available 24x365. The U.S. dollar and other major currencies need to be 'always on' anywhere that people want to transact in it with finality of settlement.

This will generate a host of benefits such as the ability for CLS to run continuously rather than during a small window of the day when all RTGS systems are operational. The foreign exchange and money markets may ultimately operate 24x365 and we will move away from the 20th century concept of 'cut off times'.

The transition to always on RTGS will require major changes at banks in terms of technology and processes. This move from batch processing to real time is going to throw up lots of interesting questions, including some fundamental ones such as the nature of overnight interest.

Payments equals identity plus messaging plus settlement. If we are to fix domestic and international payments then 24x7 availability of the core settlement asset is one of the foundations.

Request to Pay

The experience of Unified Payments Interface (UPI) in India is a lesson for all of us as we consider the perfect fiat currency stack. UPI is an example of what we call a 'Request to Pay' (R2P) scheme that enables the payee to send an electronic request to a payer, seeking their consent to the payment through a strong customer authentication. All roads lead back to digital identity.

All merchants want a simple and inexpensive way to collect from consumers and businesses. Existing methods have some deficiencies — direct debit is resisted by billers due to rights of revocation and by payers because of lack of control. Card payments are expensive in many markets and subject to fraud and chargebacks.

UPI shows how these pain points can be addressed through a modern R2P scheme but it has also been a layer for incredible innovation, such as Google Pay's innovative offering and UPI payments embedded into WhatsApp.

We would argue for a universal R2P capability that works for consumer and business payments, both online and at Point of Sale.

Open Banking in a World of Platforms

Regulators have done the banking community a great favor in helping them enter the API economy, but they have also pushed banks into compliance mode in many cases. All too often banks are seeing open banking as more of a threat than an opportunity and doing the bare minimum to comply with regulations.

This is a mistake given what we mentioned earlier about the world of platforms — the only way for banks to be relevant in the world of platforms is to show up with a full suite of retail and wholesale banking APIs. We believe that APIs should be standardized at the global level rather than by national associations.

Digital transformation for banks is not about a branch that looks like an Apple Store, a fancy app or an innovation lab with pilots running on DLT, machine intelligence, or big data. Digital transformation for a bank is when they can do basic things like lend through APIs, which few can do.

Super Apps

Once we have federated digital ID, always-on RTGS, well formed R2P schemes, and a full suite of banking APIs, there will be a burst of innovation on the front end.

Google Pay in India is a great example of a next generation app — a departure from the traditional model of binding a wallet to a credit/debit card, Google Pay binds the wallet to the bank account, which is instantly available and secured by digital ID.

VIPPS in Norway is even more advanced than the famous Swish app in Sweden. It is built by a bank owned consortium and would give the Chinese super apps a run for their money in terms of functionality and clean design.

Increasingly consumers and businesses will interact with financial services not within dedicated apps but as they transact in digital platforms. An Airbnb host will be able to obtain a home improvement loan based on their rental earnings from within the platform.

The enhancements so far solve for the financial layer of domestic payments, but they are also part of the solution for international payments.

SWIFT

SWIFT is a standards body and secure messaging network that covers over 10,000 banks. Recently SWIFT gpi has delivered transparency to international payments and led to an improved end to end service, with around 50% of payments reaching the beneficiary within 30 minutes.

SWIFT made it clear that it will help the community deliver an instant cross-border payments experience. We see SWIFT becoming a secure API hub that supports interactive messaging between banks during different stages of a transaction lifecycle — pre-validation, the transaction itself, synchronized settlement, and post transaction.

SWIFT is also moving to enable connectivity into national faster payments schemes which will further improve the end to end service as these schemes roll out internationally and become ubiquitous.

Tokenizing Commercial Bank Money

While there are several improvements that can be made to account-based systems, as discussed above, there is potential to build new payments rails based on distributed ledger technology (DLT) and cryptographic tokens to expand the functionality of the regulated financial system.

A range of cryptocurrency models are being developed — some are intangible assets that are not backed by anything, others may operate in a regulatory grey zone, while central bank digital currencies would extend access to central bank liabilities. Tokenized commercial bank money would add to these options.

How about a future of digital money in which users can hold accounts with traditional ledger balances and wallets holding tokens that represent commercial bank money or e-money? Tokenized commercial bank money will be redeemable on demand at par value with account based forms of these instruments.

By tokenizing commercial bank on a multi-entity and multi-jurisdictional basis, it will be possible to deliver the benefits of tokenization, such as programmability and 24x365 instant settlement either domestically or internationally. Also, it will be possible to do it within the existing legal and regulatory framework in a compliant manner.

The world needs an upgraded financial system — most informed observers agree on this. Will an upgraded fiat 2.0 system arrive fast enough? Will it be enough? Or do we need a financial architecture that includes next generation digital currencies, be they centrally issued or de-centralized?

This reports sets out some of the options for the future of money. Let us know what you think.

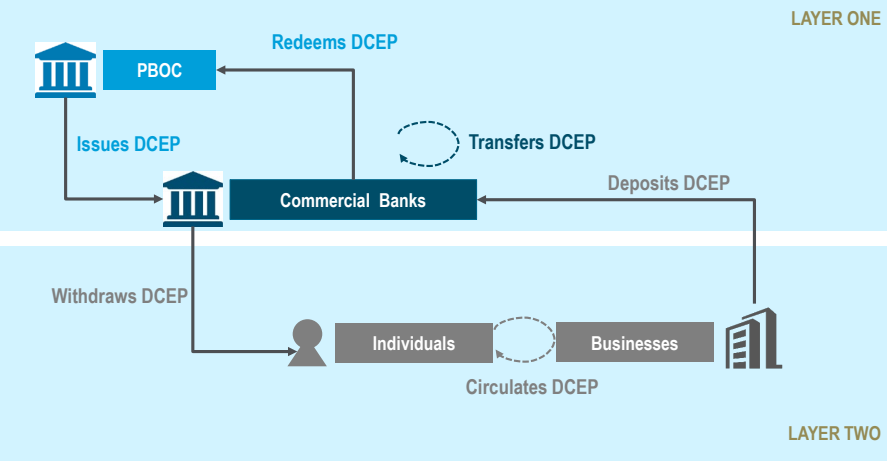
Appendix

DCEP Technical Details: Issuance & Circulation

DCEP will follow the traditional two-tier structure of "central bank-commercial bank/ other operating agencies" (i.e., same as the current monetary issuance & circulation system), where the PBOC will first issue DCEP to commercial banks/other commercial operating agencies, and then ask these agencies to distribute the DCEP to the public.

According to the PBOC, key rationales for adopting the two-tier system include: (1) to give full play to resources, talents, and technological advantages of commercial institutions, so as to fully mobilize market forces, promote innovation and achieve survival of the fittest between commercial institutions; (2) to curb public demand for cryptographic assets and consolidate China's monetary sovereignty; (3) avoid financial disintermediation. As DCEP is more competitive given unlimited credit endorsement by the PBOC, under the single-tier structure, i.e., PBOC issuing DCEP directly to public, may have an extrusion effect on bank deposits, thus affect banks' ability to lend and increase the real economy financing cost; and (4) not to change the existing money delivery system and monetary policy transmission mechanism.

Figure 62. Structure of the Two-Layer Prototype System of PBOC's DCEP

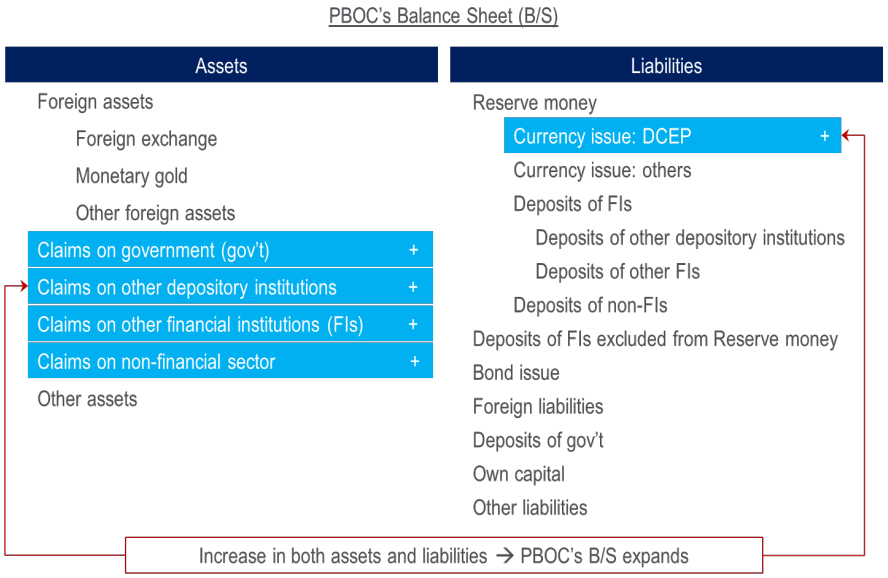


Source: Digital Currency Research Institute of PBOC, Citi Research

1. Potential Forms of DCEP Issuance

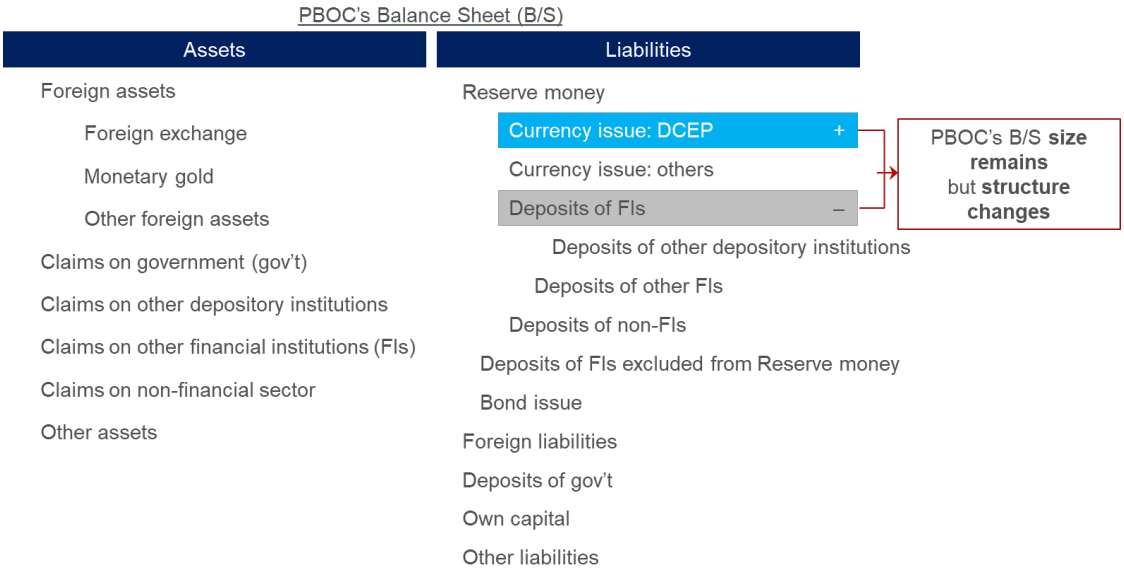
- **With PBOC balance sheet expansion**, where PBOC issues DCEP as a way to provide financing for commercial banks or purchase bonds (Figure 63).
- **Without PBOC balance sheet expansion**, where DCEP issued is used to substitute existing PBOC liabilities e.g., commercial banks' deposit reserves, central bank bills etc. (Figure 64).

Figure 63. DCEP Issuance that Expands PBOC's Balance Sheet



Source: "Economic Analysis of Digital Currencies", Yao Qian and Chen Hua, Citi Research

Figure 64. Digital DCEP Issuance that Does NOT Expand PBOC's Balance Sheet



Source: "Economic Analysis of Digital Currencies", Yao Qian and Chen Hua, Citi Research

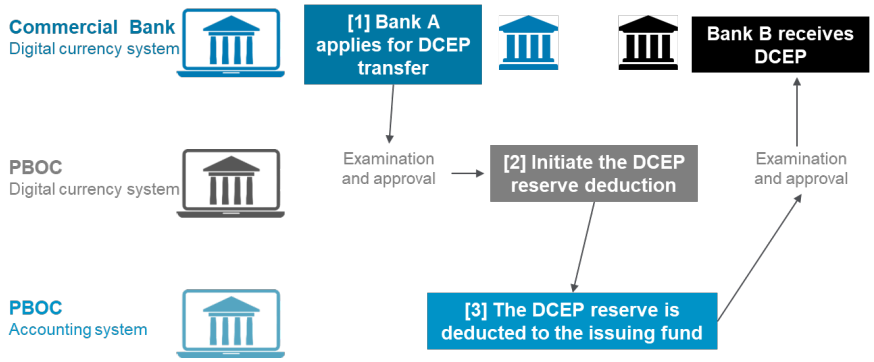
2. Circulation between Commercial Banks

In typical interbank transactions, excess reserves serve as the medium of exchange. We believe DCEP will serve similar function as excess reserves, and follow similar transaction processing flow/accounting rules.

- **Transaction flow:** In a transaction where Bank A makes an interbank transfer to Bank B: (1) Bank A will first send a numeric code to the PBOC which contains the receiver, amount, effective date info etc.; (2) PBOC reviews and approves the request, void the old DCEP, issues new DCEP, and modifies the amount and ownership info in the code sent by Bank A; and (3) send the newly issued DCEP to Bank B (Figure 65).

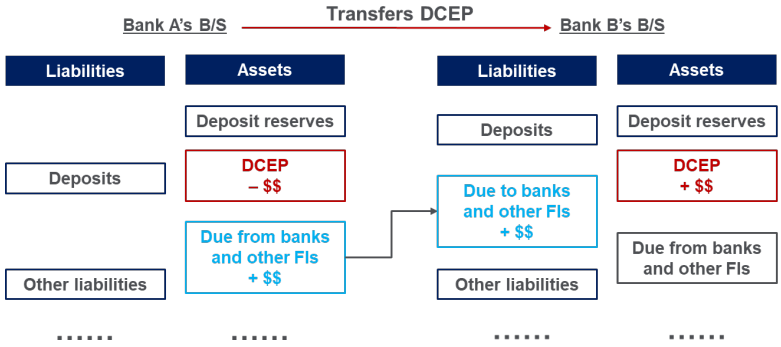
- **Accounting rules:** Similar to how a cash-backed interbank placement is recorded except that the deduction/addition is applied to the DCEP reserves on banks' balance sheet (Figure 66).

Figure 65. DCEP-backed Interbank Transfer Process



Source: Digital Currency Research Institute of PBOC, Citi Research

Figure 66. How a DCEP-based Interbank Transfer Changes Commercial Banks' Balance Sheets



Source: Digital Currency Research Institute of PBOC, Citi Research

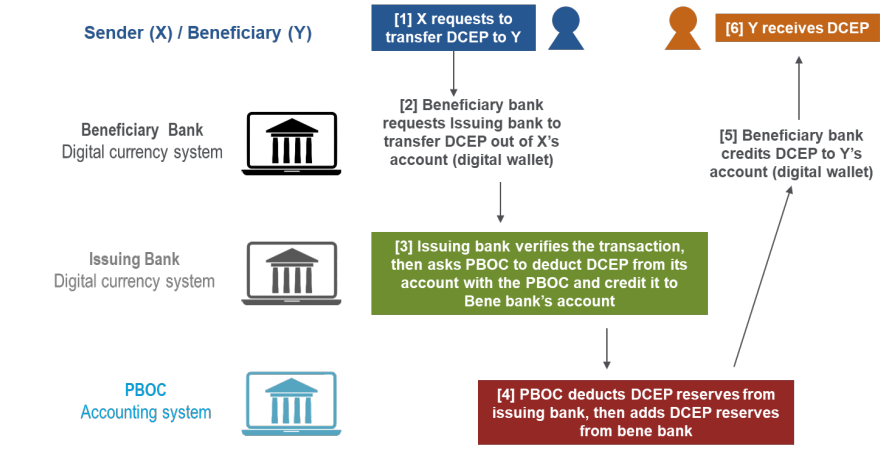
3. Circulation between Individuals/Businesses

Though the accounting rules of a DCEP-backed retail payment is largely the same as for a cash-backed payment, their transaction flows are quite different. We illustrate the details below using an example where sender (X) purchases fixed assets from beneficiary (Y) using DCEP.

- **Transaction flow:** (1) X initiates a DCEP transfer request in the app (facilitating the DCEP digital wallet) or by swiping the chip card, instructing issuing bank to transfer DCEP to Y's account held at beneficiary bank (Bene Bank); (2) Bene Bank requests DCEP transfer from issuing bank; (3) Issuing bank verifies details from Bene Bank with info in X's request, approves the transaction and asks PBOC to help facilitate the transfer; (4) PBOC completes DCEP transfer, deducting DCEP reserves owing to Issuing Bank and crediting DCEP reserves owing to Bene Bank; (5) Bene Bank credits DCEP to Y's account upon receiving PBOC's confirmation (Figure 67).

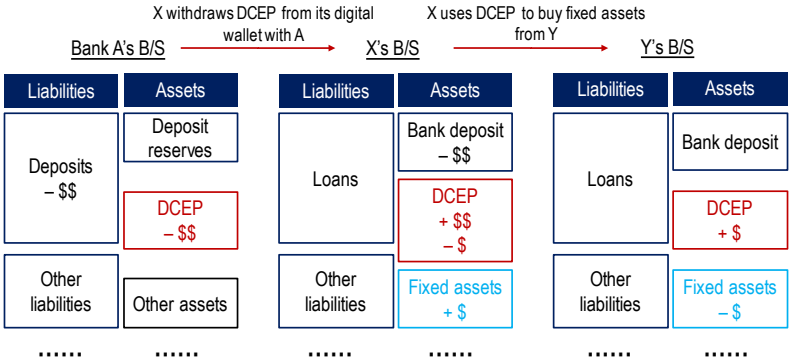
- **Accounting rules:** same as how a cash-backed interbank placement is recorded except: (1) deduction/addition applied to DCEP balance on individual/businesses' balance sheet; and (2) deduction/addition applied to DCEP reserves on banks' balance sheet (Figure 68).

Figure 67. DCEP-backed Payment Flow



Source: Digital Currency Research Institute of PBOC, Citi Research

Figure 68. How a DCEP-backed Payment Changes Individual/Corporate Balance Sheets



Source: Digital Currency Research Institute of PBOC, Citi Research

Technical Route: Partial Blockchain Adoption

According to the PBOC, it is technologically neutral and does not necessarily rely on one fixed technological path in DCEP. It has initiated a 'horse racing' model where several designated operators have adopted different technical routes for developing DCEP, and those that will eventually be accepted by the people and the market, will win the game in the end.

While blockchain has been a widely adopted technology backing most digital currencies, the PBOC noted that given DCEP aims to replace M0 and achieve retail-level adoption, it demands high concurrency with the capability to process at least 300,000 Transactions per Second (TPS), which the current blockchain technology is not able to support (Libra is expected to handle 1,000 TPS and Bitcoin handles only 7 TPS).

As such, we believe it is likely that blockchain will not be adopted by DCEP at issuance level, but it can be adopted by commercial banks in distribution of DCEP.

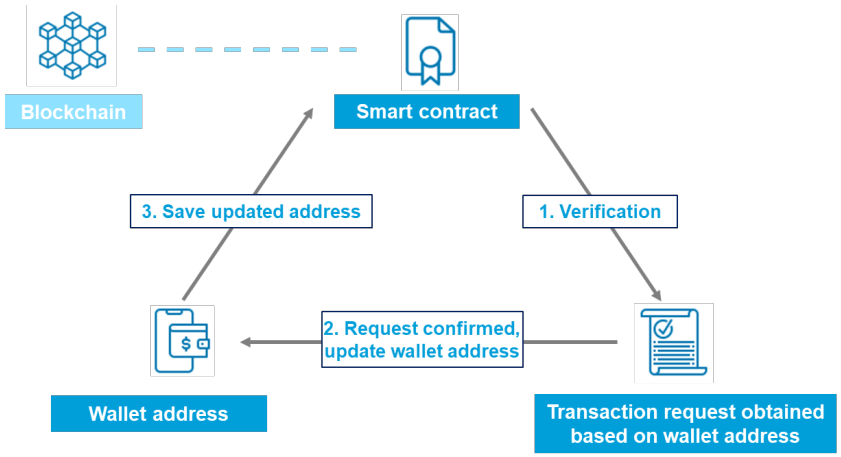
Potential usage scenarios include:

1. Digital wallet address management

The transaction request is verified based on the digital wallet address of the transferor. If the verification is approved, then it updates the digital wallet address and saves it to the smart contract, such that subsequent transactions can be conducted based on the new address.

After the original digital wallet address is updated, its binding relationship with the identity information of the transferor is cut off forcibly. Therefore, even if the original address is tracked by outsiders, it cannot be used to view the private information corresponding to the identity of the transferor, which effectively protects the privacy of the users.

Figure 69. Business Process of Digital Wallet Address Management Using Blockchain



Source: EqualOceananalysis, Citi Research

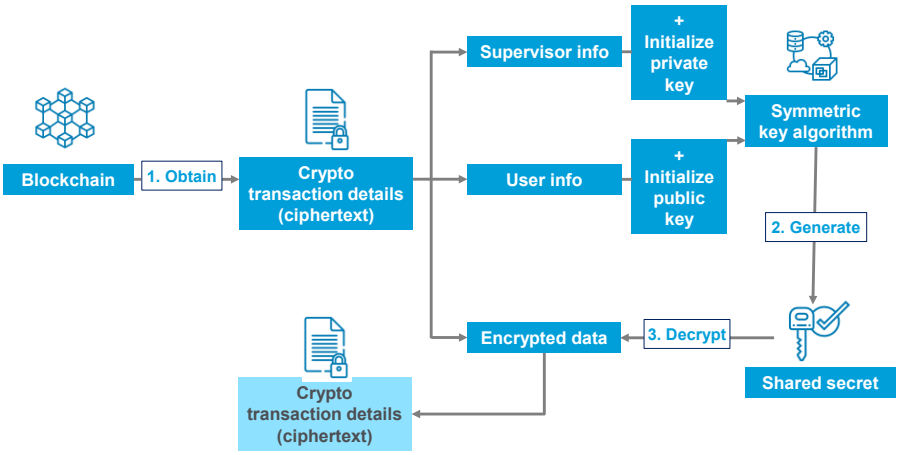
2. Transaction information supervision

First, the transaction information of DCEP is obtained from the blockchain, including information of the supervisor, information of a particular user (start with the first user) and the encrypted data.

With the initial private key of the supervisor and the user, the shared secret password of the user is generated through the symmetric key algorithm. Then using the shared secret to decrypt the encrypted data, the crypto transaction details between the supervisor account and a particular user can be obtained.

In this case, transaction information can be kept confidential from the irrelevant parties on the blockchain.

Figure 70. Business Process of Transaction Information Supervision Using Blockchain

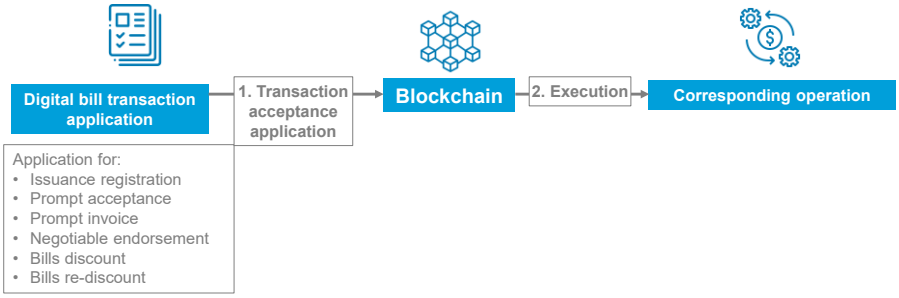


Source: EqualOceananalysis, Citi Research

3. Digital bill and currency transaction

Leveraging the technology of decentralization and immutability to realize disintermediation in value transfer, to control credit risks, and to lower the auditing expense in the market.

Figure 71. Digital Bill Transaction and Digital Currency Transaction Based on Blockchain



Source: EqualOceananalysis, Citi Research

Citi Global Perspectives & Solutions (Citi GPS) is designed to help our clients navigate the global economy's most demanding challenges, identify future themes and trends, and help our clients profit in a fast-changing and interconnected world. Citi GPS accesses the best elements of our global conversation and harvests the thought leadership of a wide range of senior professionals across the firm.

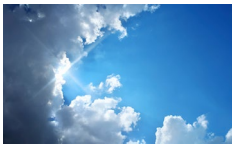
All Citi GPS reports are available on our website www.citi.com/citigps

Systemic Risk
Systemic Solutions for an Interconnected World
April 2021

Bitcoin
At the Tipping Point
March 2021

Financing a Greener Planet
Volume 1
Volume 2
February 2021

Electric Vehicle Transition
February 2021



Investment Themes in 2021
January 2021

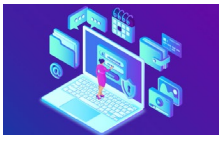
The Global Art Market and COVID-19
Innovating and Adapting
December 2020

Education: Fast Forward to the Future
October 2020

The Holistic Case for Investment in Girls
October 2020

Closing the Racial Inequality Gaps
September 2020

Negative Interest Rates
Where Is the Real Limit to Cheap Money?
July 2020



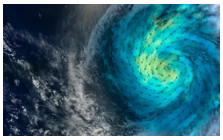
ePrivacy & Data Protection
Data Privacy & its Influence on AI Ethics, Competition & Tech Evolution
July 2020

Technology at Work v5.0
The New Normal of Remote Work
June 2020

5G and Mobile Operators
Is Virtual Becoming Real?
April 2020

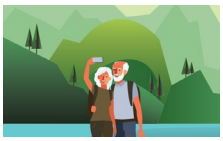
Closing the Loop on Global Recycling
Finding a Global Solution to the Patchwork of Recycling
February 2020

Disruptive Innovations VII
Ten More Things to Stop and Think About
February 2020



Building a TCFD With Teeth
What the Markets Need to Price Climate Risk
February 2020

Banking the Next Billion
Digital Financial Inclusion in Action
January 2020



Experiential Commerce
A Brave New World
January 2020

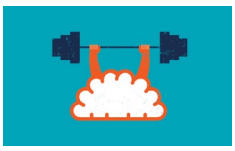
Investment Themes in 2020
January 2020

Corporate Finance Priorities 2020
January 2020

Car of the Future v4.0 – 2020 Update
The Race for the Future of Networked Mobility
January 2020

The Global Art Market
Drivers of Evolution

December 2019



Education: Power to the People
Exploring Opportunities for Private Capital in Education
November 2019

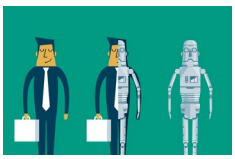
Digitizing Governments
The Journey to Enacting a Digital Agenda
October 2019

Electric Aircraft
Flightpath of the Future of Air Travel
September 2019

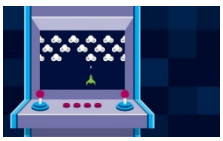
Energy Darwinism III
The Electrifying Path to Net Zero Carbon
September 2019

For Better Or Worse, Has Globalization Peaked?
Understanding Global Integration
August 2019

Factory of the Future
Flexible, Digitized, and Sustainable
July 2019



Technology at Work v4.0
Navigating the Future of Work
June 2019



Video Games: Cloud Invaders
Bracing for the Netflix-ization of Gaming
June 2019

Managing Cyber Risk with Human Intelligence
A Practical Approach
May 2019

Bank X
The New New Banks
March 2019

2019 Corporate Finance Priorities
January 2019

Investment Themes in 2019
January 2019

IMPORTANT DISCLOSURES

This communication has been prepared by Citigroup Global Markets Inc. and is distributed by or through its locally authorised affiliates (collectively, the "Firm") [E6GYB6412478]. This communication is not intended to constitute "research" as that term is defined by applicable regulations. Unless otherwise indicated, any reference to a research report or research recommendation is not intended to represent the whole report and is not in itself considered a recommendation or research report. The views expressed by each author herein are his/ her personal views and do not necessarily reflect the views of his/ her employer or any affiliated entity or the other authors, may differ from the views of other personnel at such entities, and may change without notice.

You should assume the following: The Firm may be the issuer of, or may trade as principal in, the financial instruments referred to in this communication or other related financial instruments. The author of this communication may have discussed the information contained herein with others within the Firm and the author and such other Firm personnel may have already acted on the basis of this information (including by trading for the Firm's proprietary accounts or communicating the information contained herein to other customers of the Firm). The Firm performs or seeks to perform investment banking and other services for the issuer of any such financial instruments. The Firm, the Firm's personnel (including those with whom the author may have consulted in the preparation of this communication), and other customers of the Firm may be long or short the financial instruments referred to herein, may have acquired such positions at prices and market conditions that are no longer available, and may have interests different or adverse to your interests.

This communication is provided for information and discussion purposes only. It does not constitute an offer or solicitation to purchase or sell any financial instruments. The information contained in this communication is based on generally available information and, although obtained from sources believed by the Firm to be reliable, its accuracy and completeness is not guaranteed. Certain personnel or business areas of the Firm may have access to or have acquired material non-public information that may have an impact (positive or negative) on the information contained herein, but that is not available to or known by the author of this communication.

The Firm shall have no liability to the user or to third parties, for the quality, accuracy, timeliness, continued availability or completeness of the data nor for any special, direct, indirect, incidental or consequential loss or damage which may be sustained because of the use of the information in this communication or otherwise arising in connection with this communication, provided that this exclusion of liability shall not exclude or limit any liability under any law or regulation applicable to the Firm that may not be excluded or restricted.

The provision of information is not based on your individual circumstances and should not be relied upon as an assessment of suitability for you of a particular product or transaction. Even if we possess information as to your objectives in relation to any transaction, series of transactions or trading strategy, this will not be deemed sufficient for any assessment of suitability for you of any transaction, series of transactions or trading strategy.

The Firm is not acting as your advisor, fiduciary or agent and is not managing your account. The information herein does not constitute investment advice and the Firm makes no recommendation as to the suitability of any of the products or transactions mentioned. Any trading or investment decisions you take are in reliance on your own analysis and judgment and/or that of your advisors and not in reliance on us. Therefore, prior to entering into any transaction, you should determine, without reliance on the Firm, the economic risks or merits, as well as the legal, tax and accounting characteristics and consequences of the transaction and that you are able to assume these risks.

Financial instruments denominated in a foreign currency are subject to exchange rate fluctuations, which may have an adverse effect on the price or value of an investment in such products. Investments in financial instruments carry significant risk, including the possible loss of the principal amount invested. Investors should obtain advice from their own tax, financial, legal and other advisors, and only make investment decisions on the basis of the investor's own objectives, experience and resources.

This communication is not intended to forecast or predict future events. Past performance is not a guarantee or indication of future results. Any prices provided herein (other than those that are identified as being historical) are indicative only and do not represent firm quotes as to either price or size. You should contact your local representative directly if you are interested in buying or selling any financial instrument, or pursuing any trading strategy, mentioned herein. No liability is accepted by the Firm for any loss (whether direct, indirect or consequential) that may arise from any use of the information contained herein or derived herefrom.

Although the Firm is affiliated with Citibank, N.A. (together with its subsidiaries and branches worldwide, "Citibank"), you should be aware that none of the other financial instruments mentioned in this communication (unless expressly stated otherwise) are (i) insured by the Federal Deposit Insurance Corporation or any other governmental authority, or (ii) deposits or other obligations of, or guaranteed by, Citibank or any other insured depository institution. This communication contains data compilations, writings and information that are proprietary to the Firm and protected under copyright and other intellectual property laws, and may not be redistributed or otherwise transmitted by you to any other person for any purpose.

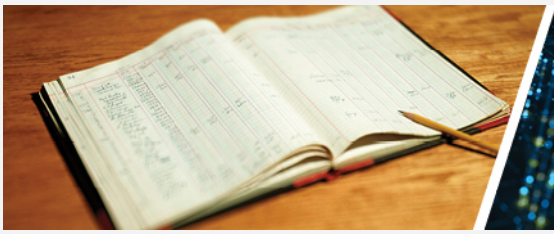
IRS Circular 230 Disclosure: Citi and its employees are not in the business of providing, and do not provide, tax or legal advice to any taxpayer outside of Citi. Any statements in this Communication to tax matters were not intended or written to be used, and cannot be used or relied upon, by any taxpayer for the purpose of avoiding tax penalties. Any such taxpayer should seek advice based on the taxpayer's particular circumstances from an independent tax advisor.

NOW / NEXT

Key Insights regarding the Future of Money

CURRENCY

Money in today's world is account-based and today's digital money is basically an electronic version of account-based money. / Digital money in the 21st century will be increasingly tokenized, driven by CBDCs, Big Tech, and wider adoption of cryptocurrency.




INFRASTRUCTURE

In the current financial structure, only commercial banks hold accounts with their central bank. / The biggest infrastructure change with CBDCs is that private citizen accounts could be held at the central bank. This would be a tectonic shift to how Central Banks are organized and would require significant legal changes.


SOCIAL CHANGE

Declining cash usage has been an ongoing trend, but recent data suggest an acceleration in the decline of cash use for payments which becomes a problem for the sizable portion of the world which is unbanked. / Financial inclusion and domestic payment efficiency remain the top motivators for CBDC development among Emerging Market and Developing Economies and could help especially decrease the number of unbanked in Advanced Economy urban centers.