January 8, 2021

MACRO STRATEGY

# The Blockchain Blockbuster:

## Yapese Stones to Central Bank Digital Currencies

### Key Takeaways

- Blockchain, a revolutionary way of transmitting information trustlessly through time, has captured the imaginations of software developers, economists, and now, central bank policymakers worldwide. Blockchain is a version of distributed ledger technology, a system whose fundamental structure dates back hundreds of years to the Micronesian island of Yap.[1]
- Stablecoins have emerged as a new way to transact value in the cryptocurrency space. Instead of being claims on network equity, such as Bitcoin, existing stablecoins seek to mimic the price of real-world assets, such as the United States Dollar (USD). A central bank digital currency (CBDC) would effectively be a class of stablecoin.
- Motivations for creating CBDCs include an interest in furthering financial inclusion globally, impeding criminal use of cash, improving electronic payments infrastructure, enhancing policy tools, and, in the case of the United States, strengthening the reserve status of the U.S. Dollar. Other CBDCs are likely attempts to offer a different reserve currency option.

MetLife Investment Management

- A true CBDC launch among Western countries seems unlikely to occur anytime soon. The head of the European Central Bank, Christine Lagarde, suggested that it could take anywhere from two to four years.[2]
- China is expected to be the first major sovereign power to implement a large scale CBDC initiative, further expanding the footprint of its digital economy and potentially laying the foundation for at least partial yuanization of countries along the Belt and Road.

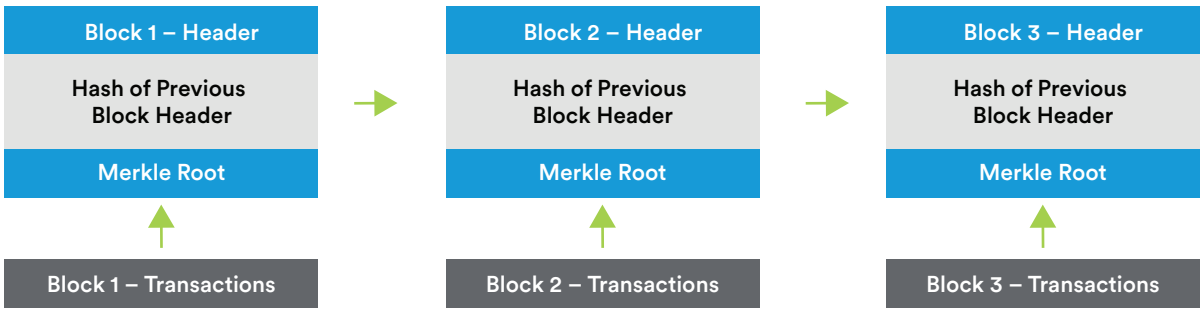
Even in its short existence, the introduction of blockchain technology into the various facets of economic life has served to change the way society interacts with the market and government. Supply chain tracking, insurance claims processing, real estate trading, computational power allocation, and secured identification are some of the many ways this burgeoning technology is having a very real impact on our everyday lives. That said, blockchain was originally created with the facilitation of commerce in mind. By fusing the payment system into the monetary unit itself, money can be improved both through lowering costs and enhancing trust. Bitcoin, the first use case of blockchain technology, opened the proverbial doors to a new method of financial interaction. Central banks have taken note of the recent rise of cryptocurrency as a potential final settlement layer for economic activity and are seeking to build upon this technology in order to better align monetary policy with their mandates as well as to provide for a more inclusive banking infrastructure. In this paper, we explore the origins of blockchain technology, the evolution of cryptocurrency as a type of money alternative, and how central banks are planning to harness its power to modernize their institutions

# Blockchain, A Primer

## The Building Blocks

Before any conversation can begin regarding how and why blockchain technology is used, it must first be properly defined. A blockchain is a series of records, or "blocks," linked together in a "chain" designed to securely store information across time without the need for a trusted third-party. Each block records recent transactions, retains an account of previous transactions via an embedded cryptographic hash, and assigns to every block a timestamp of when the transactions occurred. In this way, individuals can keep a secure record of what happened and what is transpiring, all while allowing for a method that links the past to the future without the need for a central authority. No block in the chain can be altered without affecting all other blocks subsequently generated. Indeed, the act of altering transactions in any single block directly changes that block's cryptographic hash and, therefore, the hashes of all blocks that came afterward.

**Diagram 1 | Basic Blockchain Structure**




*Source: WikiMedia.org, MetLife Investment Management (MIM)*

It is in this way that blockchain solves the "double-spending" problem where someone could use the same digital currency unit in two different transactions without the parties involved knowing. Instead, the block's embedded cryptographic hash, by inherently being a record of all previous transactions, acts as a check on the problem of double-spending by rejecting any transaction where the unit of account's ownership had already been marked as changed. In order to double-spend, a malicious actor must alter the block in which the targeted transaction occurred, but in doing so must then change each subsequent block's transaction hash. This quickly becomes a very expensive and time-consuming endeavor, especially for large networks, that is likely to render the value of accomplishing such a task useless.

## A Brief History of Distributed Ledgers

The fundamental concept behind blockchain money harkens back hundreds of years to a tribe in Micronesia known as the Yap. The Yapese are probably best known for their use of a verbal public distributed ledger to record the transfer of money between families. For this culture, money consisted of large, heavy wheels of limestone known as rai stones, which lay about the island. The value of each rai stone depended on its history, beauty, and heft. Heavier and more nicely carved stones, as well as those with important stories tied to them, commanded a higher value. Because rai stones could not be moved without significant effort, the Yapese would convene a quorum of tribesmen whenever a transaction was set to occur. Each family would then alter their ledger based on what was announced at the gathering. As such, if an individual claimed that a transaction occurred that was not recorded in this manner, it would be considered illegitimate.

Notice that Yapese stone money did not need to physically change hands. As stated previously, stones were rarely touched. Due to the effort involved in moving a stone, doing so was often a sign of power, wealth, or the importance of the transaction. Indeed, the true money was arguably the payment system itself. In fact, there is a story of an individual who tried to move their stone by boat, only to have it sink to the bottom of the ocean. Despite the wheel being lost forever, the Yapese still considered it to be a legitimate unit and continued to assign ownership to it for use in later transactions. As shown, the Yapese used no technology yet boasted a monetary system inherently dependent on i) a single source of truth (i.e., the transaction quorum) and ii) the distributed nature of the public ledger (i.e., each family's record).

In modern times, blockchain technology has its origins in the 1980s and 1990s when a series of cryptographers proposed ways of linking information across time in a trustless manner. Satoshi Nakamoto, which could very well be the pseudonym for a group of anonymous cryptographers, built on earlier initiatives to produce the world's first functioning blockchain protocol, named Bitcoin, by using a cryptographic hash function of previous transactions to solve the distributed systems conundrum known as the Byzantine Generals' Problem (BGP). This dilemma's name comes from a thought experiment where two or more generals are besieging a city and must coordinate in order to launch an effective attack, but in doing so are using a messenger that passes through unfriendly territory. This substantially increases the odds of information tampering. Nakamoto solved this problem in a unique way, outlining the methodology in a 2008 whitepaper that laid the foundation for a new kind of currency.

## Bitcoin, Bit by Bit

In his Bitcoin whitepaper, Nakamoto describes the structure of the proposed protocol and why his method of using a CHF as the effective timestamp that tethers blocks of transactions together has the practical effect of solving the BGP. With the protocol, blocks are produced via a computational exercise known as "proof-of-work" in order to maintain agreement among ledger holders. In proof-of-work, actors known as "miners" compete to solve a mathematical puzzle that links current transactions to the previous block's hash. Once the link, called a "nonce," is found the solution is

then easily verifiable as being true by anyone using the network. Miners are rewarded for the time and energy expended in solving the puzzle through an allocation of new Bitcoins, essentially the protocol's version of monetary inflation. This "block reward" decreases over time at known "block heights," or a set number of blocks since the genesis, or beginning, block and have come to be known as "the halving(s)."

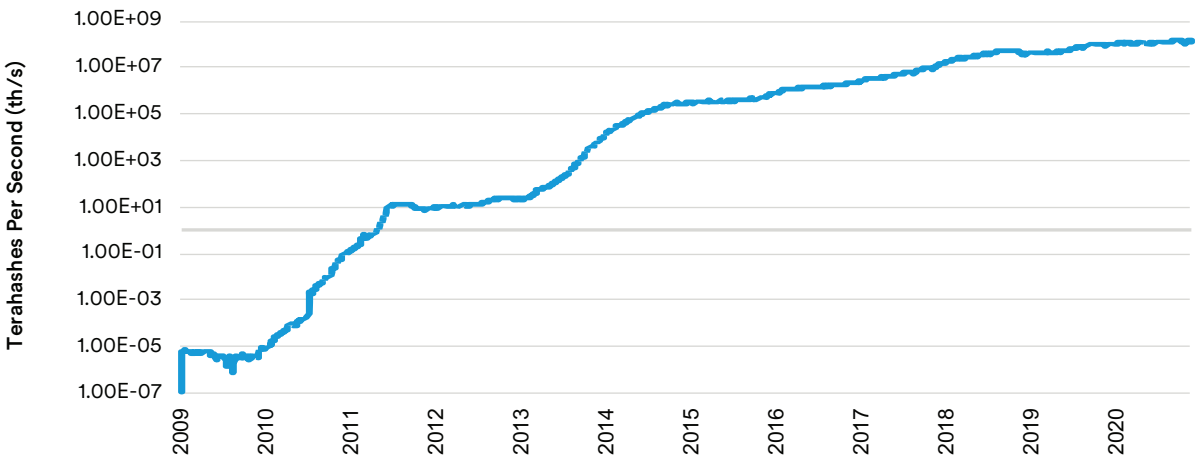
**Table 1 | Bitcoin Halvings**

| Date | Block Height | Market Price | Block Reward (BTC) |
|---|---|---|---|
| 11/28/12 | 210,000 | $12 | 25 |
| 7/9/16 | 420,000 | $663 | 12.5 |
| 5/11/20 | 630,000 | $8,740 | 6.25 |
| ~ 6/2024 | 840,000 | N/A | 3.125 |
| ~ 6/2028 | 1,050,000 | N/A | 1.563 |
| ~ 6/2032 | 1,260,000 | N/A | 0.781 |
| ~ 6/2036 | 1,470,000 | N/A | 0.391 |
| ~ 6/2040 | 1,680,000 | N/A | 0.195 |
| ~ 6/2044 | 1,890,000 | N/A | 0.098 |

*Sources: Blockchain.com, MIM*

The difficulty of solving said mathematical computation changes such that the average time between solutions corresponds to a preselected gap, set at ten minutes average for Bitcoin. Increasing numbers of miners competing for block rewards forces the hash algorithm (known as SHA256 in the case of BTC) to make the computation harder to solve in effort to regulate this average gap. The amount of computational power behind Bitcoin's blockchain security is approximated in Figure 1 and is measured in terahashes, or trillions of hashing operations performed, per second. This system of CHFs, coupled with miner incentives, creates the practical foundation for a purely digital form of money that effectively controls for the BGP. Thus, Bitcoin's protocol allows all users to trust that each new block accurately represents the true state of the network.

**Figure 1 | Bitcoin Hash Rate (Log Scale), 7-Day Average**




*Sources: Blockchain.com, MIM*

Going back to the example of the Byzantine generals, a malicious actor would find it hard to prove that their message was legitimate because they would almost invariably produce a false solution to the mathematical puzzle or, if the puzzle happened to have been solved correctly, it would have occurred within a nonstandard time period. In other words, individuals looking to attack the generals' line of communication would take too long to produce a solution or would simply find the wrong one. The sheer volume of power behind the Byzantine army's hashing and unhashing of messages would render the besieged city's efforts at tainting the communication line utterly useless.

After Nakamoto's invention, computer scientists and cryptographers began to build further upon on the protocol, introducing new ways for their networks to reach "consensus," or agreement, among distributed holders of the public ledger. Innovations such as "proof-of-stake," where new blocks are minted in some relation to network equity at-risk, and Directed Acyclic Graphs (DAGs), where individual transactions are linked together in a lattice-like structure without the need for blocks, came into existence as bleeding-edge methods to reach systemic agreement among users. An entire generation of cryptocurrencies that came after Bitcoin have chosen to use consensus mechanisms that differ, sometimes substantially, from Nakamoto's original design. Most famous of these is Ethereum (ETH), which has slowly moved from a proof-of-work consensus mechanism to a proof-of-stake model, which went live on December 1st, 2020. Despite these innovations, proof-of-work remains the most battle-hardened consensus model in the cryptocurrency space.

## Digital Danger

Despite Nakamoto's revolutionary methodology, there remain a variety of ways to attack blockchains in order to cause real financial loss. This is especially true with smaller networks that do not have large amounts of computing power securing them. In general, there are three main ways to attack a blockchain network: Distributed Denial-of-Service (DDOS), Sybil, and 51% attacks.[3] In order to counter these potential assaults, public blockchains have adopted their own methods to mitigate the chances of the network being compromised.

In the case of a DDOS attack, the assailant floods the network with low-cost transactions. This effectively slows down the system by forcing legitimate transactions to take longer than they realistically should. As stated, many blockchains have found a way around this type of malicious behavior, but some communities are cautious regarding solutions. One of the main selling points of a public blockchain is its open access and censorship resistance. If a blockchain begins to pick and choose which transactions the community thinks are legitimate and which aren't, it may lead to migration away from that project as users express fear that such power could be misused or even abused.

In a Sybil attack, sometimes called an Eclipse attack, one node masquerades as many and effectively surrounds honest nodes in an attempt to block critical information from coming or going. The main way of mitigating this issue is by making the cost of creating a node high enough to deter such behavior. In the case of Bitcoin, each miner is a node and the cost of mining tends to be rather high, both with regard to electricity usage and hardware expense. With proof-of-stake consensus, a node is created using locked coins, or network equity at-risk. The higher the amount of coins that must be locked up, the greater the cost of producing a node and the higher value at-risk an assailant would need to provide in order to attack the network. There is certainly a delicate balance in public blockchains between the cost of setting-up a node and network decentralization. As indicated previously, each cryptocurrency project has their own way of dealing with this issue.

Lastly, a 51% attack occurs when the majority of the nodes securing a network are controlled by a single malicious actor, who then attempts to effectively rewrite history. This allows the assailant to double-spend any transaction(s) they choose by spending on the original "honest" chain, mining a "private" side chain, and then broadcasting their private chain after the good or service has been

rendered. On the private chain, the spending never occurred and the malicious actor now has both the good they received for their original coins on the honest chain as well as the coins existing on the new private chain. Because of proof-of-work's inherent "the longest chain is the true chain" characteristic, once the assailant has their desired good, they broadcast the private chain to the world, which will now become the public chain. 51% attacks mostly occur with smaller networks whose hash rate, or the overall amount of computing power directed at securing the network, is small enough so that someone can effectively engulf the network's hash rate with relative ease. Projects have learned to mitigate this issue in a variety of ways, but no single solution has been adopted by all. With Bitcoin, accomplishing this kind of attack is rather difficult because the amount of hashing power needed tends to be prohibitively expensive.

## New Kids on the Block

The rise of Bitcoin in the early 2010s resulted in heightened interest among individuals who found the new technology fascinating, and liberating, namely computer scientists, software developers, economists, and cryptographers around the world. These groups saw the work that Satoshi Nakamoto had done and looked to improve on the original Bitcoin whitepaper, correcting the protocol where they believed flaws existed. Programmers worked to build upon the underlying technology behind Bitcoin to provide heightened value in the areas of smart contracts, transaction speed, security, and privacy. A number of cryptocurrencies were developed to satisfy needs that were in demand and which represented the frontiers of cryptographic thought. Table 2 provides a brief overview of some of the landmark coins launched by developers in the cryptocurrency space. A select few are discussed in greater detail to better outline cryptocurrency's growth narrative.

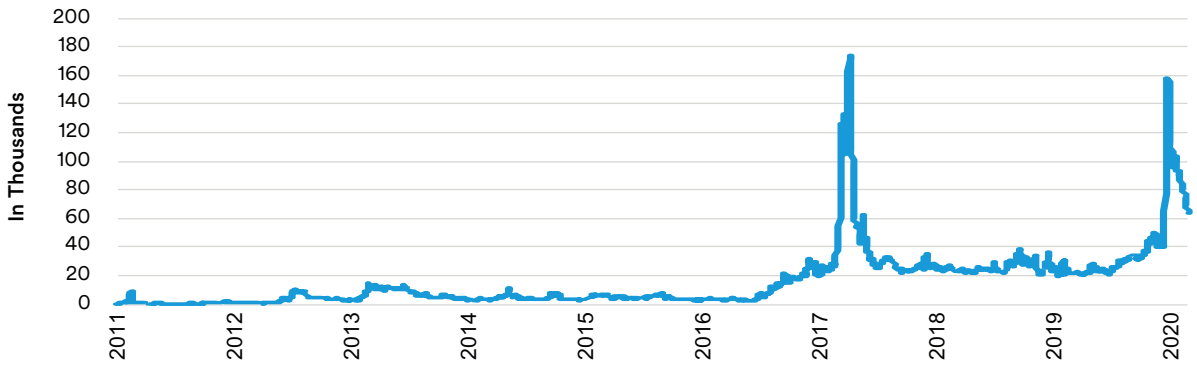
**Table 2 | The "Altcoin" Revolution**

| Coin | Inception Year* | Current Market Cap** | Market Cap Rank** | Description |
|---|---|---|---|---|
| Litecoin (LTC) | 2011 | $5.9B | 5 | Seen as a real-world, value at-risk testnet[4] for Bitcoin upgrades. |
| Monero (XMR) | 2014 | $2.7B | 15 | A privacy-centric coin that obfuscates information about the sender, receiver, and the amount transacted. Commonly used in online illicit activity. |
| Ethereum (ETH) | 2015 | $71.2B | 2 | The leading smart contract coin used in decentralized applications for blockchain-based finance, AI, storage, oracles, identification, and supply chain tracking. |
| Cardano (ADA) | 2015 | $5.2B | 8 | Created by one of Ethereum's founders, Charles Hoskinson, Cardano is similar in nature except with an egalitarian focus on pushing "power to the edges" of society.[5] |
| Decred (DCR) | 2016 | $363M | 52 | DCR combined advances in both proof-of-work and proof-of-stake consensus models to produce a currency that boasts its own decentralized governance system, allowing it to maintain a decentralized treasury, voting system, privacy, and exchange. Decred has been likened to a decentralized corporation.[6] |
| Polkadot (DOT) | 2016 | $4.7B | 9 | Founded by Dr. Gavin Wood, the author of Ethereum's yellow paper,[7] DOT seeks to work in concert with Ethereum and other smart contract blockchains to create a more functional, interoperable ecosystem. |
| Dai (DAI) | 2017 | $1.1B | 25 | The main product of the cryptocurrency project MakerDAO, DAI tokens are collateralized by volatile cryptocurrencies in a complex smart contract mechanism that ties the value of each DAI token to roughly $1 without the need for reserves held by a trusted third-party. |
| Chainlink (LINK) | 2017 | $4.7B | 7 | The brainchild of Sergey Nazarov, LINK works as the underlying token collateralizing a decentralized system of oracles that deliver information from the real-world directly into public blockchains. |

*Sources: CoinMarketCap.com (CMC), MIM*
*May refer to either an early Initial Coin Offering or mainnet launch year.
**As of 12/16/2020

By way of history, the very first alternative cryptocurrency, or "altcoin," was created by Charlie Lee, a former engineer at Google and Coinbase, in late 2011 and was given the name Litecoin (LTC). Litecoin changed Bitcoin's protocol in three distinct ways: the maximum number of coins, the hashing algorithm, and the average time between transactions. Litecoin increased its maximum supply (relative to Bitcoin) from 21mm to 84mm, used a hashing algorithm known as Scrypt instead of SHA256, and cut Bitcoin's 10-minute average block schedule down to just 2.5 minutes. In this way, Charlie Lee hoped that LTC would become something of a testing ground for upgrades to the Bitcoin protocol by using a network with real value attached as a result of the tradeability of LTC tokens. In other words, it would be expected that upgrades would have an impact on the price of the token and would reflect the quality of the technology used. This is also the case with exploits that are not discovered in testnet experimentation because of a lack of financial incentive. By upgrading its mainnet, hackers would be able to use the LTC chain as something of honeypot, or financial reward, where bugs could be harnessed to extract value from the chain, such as stealing funds from a given address and selling those coins on the darknet. In 2017, Charlie Lee saw his wish realized when Litecoin became the first major chain to adopt the Segregated Witness, or SegWit, upgrade meant to lower BTC's on-chain bloat.[8] After it was evident that SegWit had no detrimental impacts on LTC's functionality or value, Bitcoin then adopted the upgrade later that year.

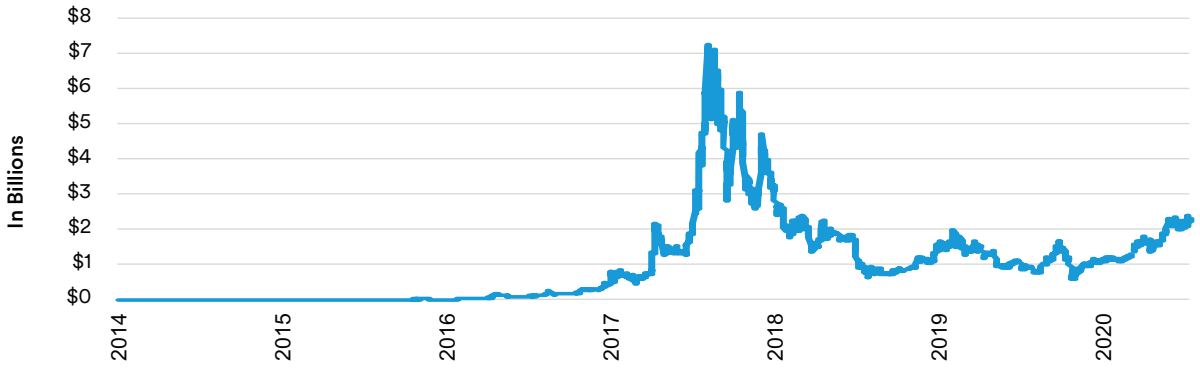
**Figure 2 | Litecoin (LTC) Transactions, 7-Day Moving Average**




*Sources: CoinMetrics.com, MIM*
As of 12/16/2020

Another notable cryptocurrency is Monero (XMR), a privacy-centric project that appeared in early 2014. Although it wasn't the first-ever privacy chain, it eventually became one of the most popular projects and remains so to this day. Monero is a "fork," or copy, of another cryptocurrency known as Bytecoin (BCN), and looked to build upon the original protocol's design in several ways. One of them was by eventually upgrading the hashing algorithm while another was seeing to it that the new protocol would have a more evenly distributed supply. Privacy coins are created from the ground up in such a way as to obfuscate where coins come from, where they are going, and the value transacted. Indeed, the only actors who know how much was sent and to where are the receiver and the sender. Monero is probably most well-known for being one of the leading cryptocurrencies used in illicit activities and, as such, has come under significant regulatory scrutiny around the world. The government of South Korea recently banned the trading of privacy coins, which includes XMR, with many other nations expected to follow suit. There are numerous privacy coins in existence today, such as Zcash (ZEC) and Horizen (ZEN), with Monero being one of the largest in terms of market capitalization.

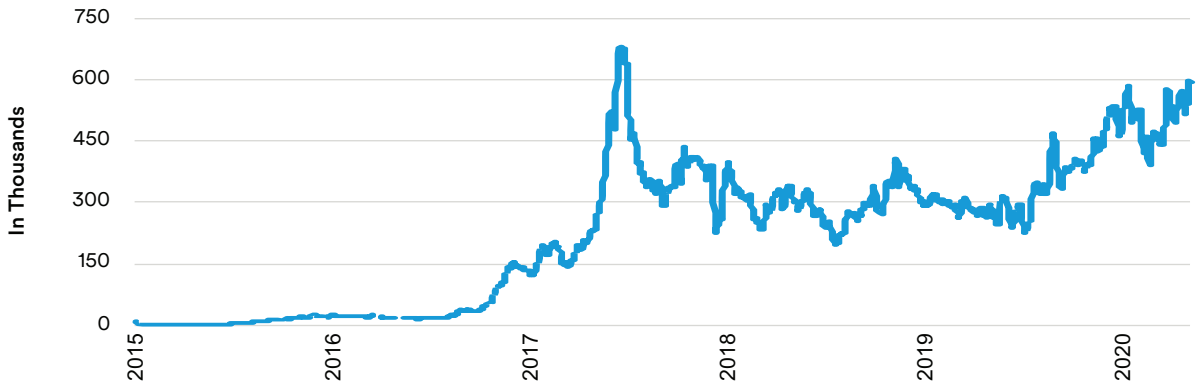
**Figure 3 | Monero (XMR) Market Capitalization**




*Sources: CMC, MIM*
As of 12/16/2020

Lastly, Ethereum is one of the most important coins in cryptocurrency and second only to Bitcoin in terms of market capitalization. In many respects, the project has been a ground-breaking success and has pushed the boundaries of what is possible in the space. Unlike Bitcoin, Litecoin, or Monero, Ethereum isn't only used for simple transactions. ETH also has the capability of harboring what are known as "smart contracts," or code that allows the user to execute an automated command in order to achieve a certain end. Some of these smart contracts are used for fun, such as games of chance and gambling. Others allow for a whole host of different use cases. Smart contracts have been deployed in order to enable decentralized data storage, finance (i.e., lending and derivatives), artificial intelligence, betting markets (i.e., event probability discovery), and much more. Ethereum, whose Initial Coin Offering (ICO) occurred in 2014, ushered in a new fleet of cryptocurrencies where users could benefit not only from transactional activities but also from a technology comparable to that of a decentralized world computer. Smart contracts are still today in their infancy, but developers have made significant strides, pressing against their limits with each passing year.

**Figure 4 | Ethereum (ETH) Active Addresses**



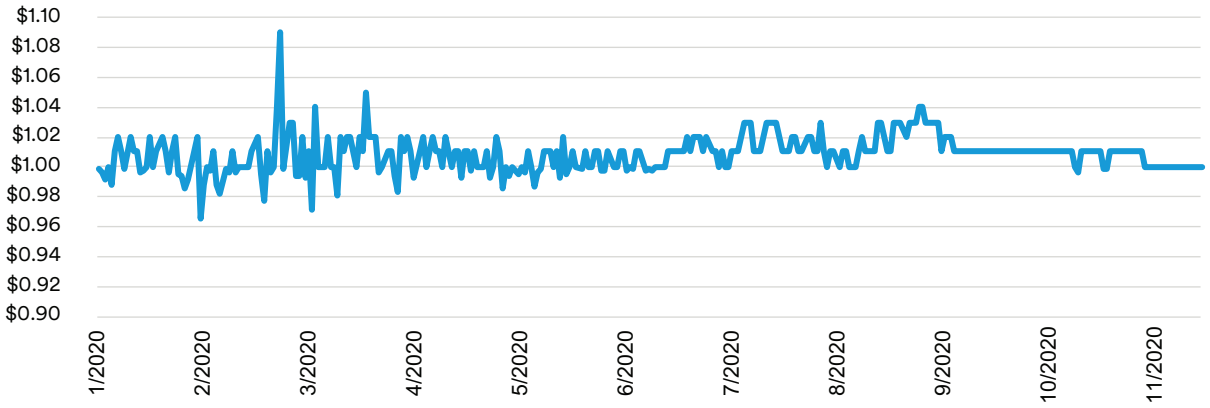

*Sources: CMC, MIM*
As of 12/16/2020

## Rise of the Stablecoins

As we approach the subject of CBDCs, a discussion regarding what exactly stablecoins are and how they relate to what has been presented so far, as well as what has yet to be considered, is in order. Fundamentally, stablecoins are altcoins, or alternative cryptocurrencies to Bitcoin. That said, the code base for many stablecoins comes from the same technological roots as Bitcoin or Ethereum. More specifically, nearly all stablecoins exist as ERC-20 tokens, which is the standard smart contract code that allows for the issuance of distinct coins on the Ethereum blockchain. However, unlike Litecoin or its altcoin peers, the value of most stablecoins isn't as volatile as other cryptocurrencies because nearly all are built to match the value of the USD. In fact, the vast majority of stablecoins are pegged to the USD, in one way or another. Other less common stablecoins mimic exposure to precious metals, equities, or foreign currencies.

Many stablecoins, such as USD Tether (USDT) or USD Coin (USDC), are backed by reserves held at issuing organizations. Other stablecoins use a complex system of smart contracts to maintain their pegs. The most well-known of these is Multi-Collateral Dai (DAI), an upgrade to the Single-Collateral Dai (SAI) produced by a cryptocurrency project known as MakerDAO (MKR). The process by which this occurs is rather complex and a full discussion is beyond the scope of this paper, but some higher-level explanation is certainly warranted. Effectively, MKR creates a series of Collateralized Debt Positions (CDPs) backed by volatile cryptocurrencies, such as Ethereum, that have been locked away by users in order to produce DAI tokens. When the market price of DAI extends too far above one USD, users can purchase more collateral, lock it up to produce DAI, and then sell the newly minted tokens into the market in order to reap an arbitrage profit. The reverse is also true. That is to say, when the price of a DAI token falls too far below one USD, users will purchase DAI, unlock the collateral used to create the coins, and then sell that collateral into the market. In this way, DAI's market value floats around one USD, but is rarely exactly one USD. There is always a price band within which arbitrage profit, after taking transaction costs into account, just isn't worthwhile. DAI's dollar peg has arguably become more stable over time as upgrades to the protocol have dampened the token's deviations.

**Figure 5 | Multi-Collateral Dai (DAI) Price**




*Sources: CMC, MIM*
As of 12/16/2020

Stablecoins have generated increasing interest from both cryptocurrency users and the finance industry. Recently, the U.S. Office of the Comptroller of the Currency approved federal banks to issue their own stablecoins, holding fiat currency in reserve as backing. This was a step forward for the integration of traditional banking with the cryptocurrency space. Banks can now issue their own cryptocurrencies and participate in the broader ecosystem, at least to the extent allowed by law. However, this ruling by the Office of the Comptroller of the Currency only applied to stablecoins issued with a one-to-one backing against a select fiat currency and did not allow for the issuing of stablecoins supported by baskets of fiat currencies. The latter was the hallmark characteristic of Facebook's proposed Libra stablecoin.

## CBDCs: The Future of Base Money?

### "Banking the Unbanked"

Although Bitcoin was created by an individual(s) who sought a decentralized digital monetary alternative to fiat currencies and precious metals, practical use of Bitcoin in economic transactions began to show a certain egalitarian side of the technology. Although Westerners had viewed Bitcoin with something of a child-like curiosity, peoples of various emerging market countries began to look at the technology in a much more serious light.[9] While people living in developed markets find it relatively easy to interact with the financial system, this isn't uniformly the case around the world. Indeed, there are vast populations who have no or limited access to financial services for a variety of reasons. Some lack the proper documentation while others face high costs of being onboarded into the banking system, or both. There are also legitimate trust issues surrounding financial services institutions in some countries that those in healthier economies are not accustomed to.

Bitcoin was able to cater directly to this underprivileged group early on due to the simplicity of "opening an account," which simply means having your own Bitcoin wallet, as well as the ease of transacting in the currency. In order to securely hold Bitcoin and use it, all that was necessary was a smart phone and an internet connection. These are two technologies that have seen immense global penetration over the last two decades and have provided meaningful informational access to individuals outside of the banking system, known as the "unbanked." Entire charitable campaigns, spearheaded by various international nongovernmental organizations, sought to use Bitcoin as a way of enhancing the financial interconnectedness of those in emerging markets who were effectively barred from the security of traditional banking services common in developed markets. A 2017 whitepaper from the Bank of Canada lists this as one of the principal reasons cited for central bank interest in CBDCs, especially among non-advanced nations.[10] The Kansas City Federal Reserve has itself noted that "though there is rarely one primary motivation given for a CBDC, both the private sector and central banks cite financial inclusion as a motivation for issuing a digital currency."[11] Terms such as "banking the unbanked" and "enhancing financial inclusion" are common references to this global need for open access to basic financial services.

### Look for the Motives

Central banks also have motivations beyond the egalitarian ideal of "banking the unbanked." This is especially true of advanced nations who generally boast a citizenry that has a relatively simple time engaging with traditional financial institutions. This isn't the case absolutely, but it is inarguable that the problem of the unbanked is skewed toward developing nations. As such, monetary authorities in more developed nations require additional reasons for CBDC issuance. The Bank for International Settlements (BIS) has noted that "there are a large and diverse number of motivations driving central banks' interest in CBDCs. Differences between emerging market economies and advanced economies are especially pronounced but individual jurisdictions can also vary significantly depending on their circumstances."[12]

The Bank of Canada whitepaper referenced earlier gives us some additional clues as to what these motivations may be. Researchers on the topic point to the growing digital economy and the need to improve payment systems in such a way as to facilitate commerce in a world where physical cash use is in decline. To this end, Bitcoin and other cryptocurrencies have also looked to fill this gap, making the need for a CBDC that competes with the more decentralized options necessary. In this way, central banks and the financial system can hold off any threats to control over the financial system cryptocurrencies may engineer. In other words, the advent of cryptocurrency itself may be as good a motivation as any for monetary authorities to develop a CBDC.

CBDCs are also seen as potentially enhancing financial stability in advanced countries by allowing for more direct control of the money supply by the central bank. This is especially true about money that is circulated among individuals engaged in everyday economic activity. Efficiencies related to improving existing payment systems, which will be discussed later, and further inhibiting criminal activity are also considered meaningful enough motivations for central banks to explore the topic of CBDCs in earnest. In addition, an already established and strong CBDC global network can work to enhance the sanction powers of the U.S. government as well as allow for increased use in official foreign dealings. Lastly, from the perspective specifically of the Federal Reserve and the United States, providing an answer to China's digital yuan efforts, which will also be discussed shortly, should strengthen the reserve status of the U.S. Dollar and may help stave off potential efforts at yuanization, especially among countries along China's Belt and Road.

## The ABCs of CBDCs

In order to discuss CBDCs in any significant capacity, we felt it critical to touch on blockchain technology, the development of cryptocurrencies with a special emphasis on both their monetary and extra-monetary characteristics, and introduce stablecoins as a type of alternative cryptocurrency. It is this progression of events that has led to the significant increase in CBDC interest. Indeed, in many ways CBDCs are themselves stablecoins, at least with respect to the token-based model. Currently, there are two main forms CBDCs are expected take: a token-based and an account-based model. Under a token-based system, CBDCs are effectively tradeable tokens on a(ny) given blockchain(s) and represent a one-for-one claim against currency held at the central bank. In an account-based scheme, all users hold accounts directly at the central bank with money exchanged between them being executed nearly instantaneously.

A version of the account-based model, labeled "synthetic CBDC" by Tobias Adrian,[13] the Director of the Monetary and Capital Markets Department at the International Monetary Fund (IMF), has also been proposed under which approved third-parties will provide the consumer-facing infrastructure, such as digital wallets and commercial plug-ins, while the central bank takes care of the backend accounting. We label this an indirect account-based model, in contrast to the direct version previously mentioned. Tony Richards, Head of Payments Policy at the Reserve Bank of Australia, refers to these contrasting account-based systems as one- and two-tiered systems and expects most market economies, such as Australia's, to adopt the latter.[14]

In reality, both a token-based and account-based model can co-exist. Individuals may be able to withdraw tradeable tokens from their accounts while simultaneously having accounts at the central bank, either directly or indirectly, that would benefit from near instant transfers. It could be that the withdrawal of a token from a CBDC account would require something of a fee or tax in order to provide for the cost of the service, raise government revenue from increasing money velocity, or in order to disincentivize non-account-based financial behavior. A growing number of specialists, such as David Birch of Consult Hyperion, suggest that a token-based model needs to be a part of any large-scale CBDC initiative in order to promote adoption and allow for a true replacement of physical cash. As noted earlier, much of the world, and even large populations within modernized

countries, have difficulties interacting with the financial system and depend largely on cash for day-to-day transactions. Moving solely to an account-based model could disenfranchise this group and push them further into financial isolation and desolation. There remain signficiant direct and indirect costs to joining the current financial system and an account-based model may retain some of these frictions, even if they are substantially mitigated.

From the standpoint of blockchain technology and its relation to CBDCs, a token-based system is most comparable to stablecoins and mimic many of the same favorable utility characteristics that cryptocurrencies have become well-known for. If central banks want to improve their competitiveness against cryptocurrencies, a CBDC system that implements a token-based model is arguably quite necessary. Without a CBDC token, central banks may actually drive individuals into cryptocurrencies, which is unlikely a desired outcome. In addition, at a higher level, the account-based system seems to mirror monopolization, at least on the backend, of the retail banking sector. Effectively, it is identical to everyone choosing the same bank to hold their money. It provides little in the way of true innovation and seems to only allow for more simplicity of the banking system than everyday financially on-boarded, or "banked," consumers would likely care for. Relying solely on an account-based model could, at the current pace of innovation within the cryptocurrency space, lead to near immediate obsolescence of the CBDC infrastructure. Moving solely to an account-based system may also cause concern among civil rights activists over possible government overreach of the economy and society. We see an account-based system as moving closer to absolute authoritative control of payment channels and the monetary unit itself while a token-based system would, ceteris paribus, provide consumers with transactional freedom in a similar vein as physical cash.

## Analog Central Banks Show Digital Interest

Historically, the conversation and official efforts around CBDCs is relatively new. Ecuador is notable for having created the first-ever digital currency back in 2014, only to have it shuttered in 2018 due to a lack of public trust in the central government's ability to keep its digital currency from losing value.[15] The Ecuadorian government had already experienced defaults on its obligations, something that limited interest in their CBDC from the outset. Sweden, although not having created a digital currency per se, has mostly phased-out the use of cash. Among the larger sovereigns, The People's Republic of China (PRC) has been developing its own CBDC since at least 2014[16] while the Bank of England became the first Western monetary authority to explore the topic in earnest back in 2015.[17] That said, significant interest in digital currencies among policymakers did not come about until after the bursting of the 2017 cryptocurrency bubble and the immense public intrigue generated by Facebook's Libra multi-currency stablecoin.

Since then, both the European Union and the Russian Federation have begun taking significant steps toward creating their own version of CBDC. In addition, it is rumored that China's digital yuan, which is best compared to a two-tiered account-based system,[18] may hit within extremely short order. The Middle Kingdom's interest in electronic currency is quite logical. China has made significant strides in the area of digital payment systems through AliPay and WeChat. CBDC provides an avenue for the central government to become more involved in the payments infrastructure, further the digitization of their economy, monitor economic activity more closely, and possibly allow for a more direct channel for monetary and fiscal policy. There may also be interest in targeted yuanization via a digital yuan that is intimately tied to the PRC's Belt and Road Initiative (BRI). Many countries along the Belt and Road have unstable currencies and an expansion of the digital yuan within their borders could be seen as mutually beneficial. Regarding United States efforts, a large volume of Federal Reserve speeches and publications have been presented last year on the matter, likely due to the increased focus on digital payment systems caused by the COVID-19 pandemic. However, Federal Reserve officials addressing digital currencies prior to

2020, at least in public, was relatively sparse. The United States is quite arguably behind the curve if it is serious in its desire to deploy a CBDC, but time remains to act.

Despite the sudden surge of interest, central bank digital currencies have, in some ways, been around for quite some time. Commercial banks, along with other depository institutions, store digital dollars in accounts held at the Federal Reserve. These entities do not force the Federal Reserve to hold their account values in physical dollars but are instead digital entries on the asset side of their electronic ledgers. Exploration of the CBDC topic by central banks may be less about creating a CBDC and more about widening the net that the current depository system covers. The idea is to expand the network of the Federal Reserve's digital dollars to include organizations, companies, and households not presently covered. One of the main candidates for expanded access to the Federal Reserve's digital dollar custodianship are social media companies, an industry that has seen significant popularity worldwide and one that has led the pack when it comes to electronic payment innovation.

Enabling these companies to register with the central bank and allowing them to participate more closely with the institution may very well be a major outcome of future CBDC implementation and regulation. Considering the global popularity of Facebook's WhatsApp and the success of existing electronic payment systems in other regions of the world, such as WeChat, Alipay, and M-Pesa, domestic social media companies are likely in a position to work more closely with the existing financial infrastructure. In large part, this drive for inclusion of social media companies into both the domestic and global financial framework is being fueled by rising distrust of banking systems worldwide and increased use of social media platforms as facilitators of exchange. Indeed, several journal articles have been published on this topic alone.

## Additional CBDC Considerations

From a technical perspective, the main difference between a theoretical "Fedcoin" token-based model and a stablecoin such as USDT is simply the issuing authority, assuming laws aren't passed to subvert use of the latter. There is also a matter of the technical parameters expected of a government-backed token and the number of merchants willing to accept it at launch. Naturally, before entertaining how this technology could be used as a tool in monetary and/or fiscal affairs, policymakers must fully-develop their CBDC technical specifications. Theoretical questions as to the underlying blockchain (i.e., one created by government authorities and/or a public chain, such as Ethereum), the degree of privacy allowed, smart contract compatibility, illegal use control, consumer protections, and any expected user-facing public-private partnerships must all be addressed.

Other aspects of the currency that aren't necessarily technical in nature will also need to be fleshed-out, such as if the currency will be interest-bearing, if the central banking authority will have the legal right to inject funds directly into CBDC-holding accounts as a way to stimulate economies during downturns, and how authorities plan to manage cross-border digital currency payments. Differing thoughts exist surrounding the need for interest-bearing CBDCs with some economists believing that base money should remain a zero interest-zero maturity instrument. Others see the potential for using interest-bearing CBDCs as a tool in monetary policy through which the central bank can more directly and uniformly influence saving and consumption. Additionally, the prospect of the population's accounts being held, either directly or indirectly, at the central bank opens the doors to a more efficient execution of what was just seen in the United States with Congress' Economic Impact Payments (EIPs). If accounts are all held at the Federal Reserve and have the proper identifying information to determine eligibility, funds could be provided quickly to households in the event of another downturn. This is also true of any kind of direct lending program to households central banks may consider in the future, if and when the need arises. Select CBDC issuances could also be given an expiration date, either through a

smart contract in a token-based model or a back-end accounting mechanism in an account-based model, providing another powerful tool for monetary policy.

Lastly, cross-border payments remain something of a dilemma for CBDCs since, as noted earlier, an important selling point for digital currency revolves around the inclusivity that such a system can provide for the "unbanked" around the world. The need to send value globally is significant and central banks will need to find a way to manage those flows in accordance with prevailing market exchange rates. Tobias Adrian believes that this may be a sticking point for CBDCs and could lead to further global dollarization, possibly even rendering certain emerging market currencies worthless. Deepening dollarization is viewed as having its own set of problems and it is possible that sovereign nations may not be interested in cross-border digital currencies if they risk undermining the sanctity of their monetary systems. Beyond issues of sovereignty, there are real economic ramifications that surround dollarization, such as the possibility of restrained long-run economic growth, as Adrian has pointed out. Others, however, are more sanguine, suggesting that existing swap lines between central banks could be used to circumvent problems related to cross-border CBDC payments.

## Lookout for the Outlook

The future for CBDCs differs somewhat from cryptocurrencies, although their paths may be intertwined at times. Bitcoin and its ilk are constantly battling to maintain a balance between three key concerns known as the "Blockchain Trilemma." The trilemma, often visualized as a triangle, consists of three issues related to sustainable public blockchain development: scalability, decentralization, and security. It is assumed in the trilemma that by strengthening any one of the triangle's vertices, at least one of the others must weaken. For instance, although Bitcoin is widely believed to be secure, there have been concerns raised regarding the centralization of mining as well as the inability of the protocol to scale during episodes of significant on-chain traffic. It was Bitcoin's scalability problem that ultimately led to a large portion of the community "forking," or breaking the protocol off, into Bitcoin Cash (BCH) in mid-2017 amid controversy surrounding the previously mentioned SegWit upgrade. Ethereum has had similar issues in this regard with the community hoping that the recent upgrade to Ethereum 2.0 will be able to more properly satisfy the trilemma than ETH's first iteration.

CBDCs are unlikely to suffer from the trilemma as it is already assumed that decentralization is not on the menu of potential features, at least not at the critical infrastructure level. An important distinction between cryptocurrencies and CBDCs is that the latter operates under the control of a central authority, either directly or indirectly. For CBDCs, scalability is likely going to be dependent on the strength of user-facing platforms and the ability of the central bank, including its public and private partners, to expand the network to its desired level. Security, since decentralization is not a concern, is simply dependent on the ability of the central bank's computer science professionals to keep hackers at bay and reduce the number of bugs that might plague the system. In the event of either a critical attack or bug, it is presumed that the central banks will have the authority both to make users whole and to provide for a timely upgrade to the system. The former, and sometimes the latter, are not normally hallmarks of public blockchain security incidents.

Before CBDCs can enter the electronic payments fray, a variety of questions, some of which have already been raised in this paper, need to be answered in detail. Lawmakers will have to pass regulations that seek to keep their CBDC program both secure and lawful but also give it the tools necessary to thrive. Appropriate timelines must be established to allow consumers, private user-facing platforms, and merchants to anticipate its launch. The launch itself will also need to be smooth in order to allow for a heightened state of trust. A botched CBDC roll-out may lead to a lack of adoption and possible discontinuation. There is also the matter of what central authorities

may be able to directly gain through CBDCs. Incentives must be structured appropriately such that both digital currency issuers and users have a reason to see the system flourish.

Realistically, given the issues raised, many of which have yet to be answered, a true CBDC launch among Western countries seems unlikely to occur anytime soon. Indeed, when the new head of the European Central Bank, Christine Lagarde, was asked about a possible timeline for a digital euro launch, she suggested that it could take anywhere from two to four years before the system would be ready for the masses. We feel the most likely scenario is that a given country's CBDC program will be finalized on a technical level first, followed by limited roll-outs in order to apply real world tests to the system, and then a mass release. Arguably the country furthest along the CBDC road, China took these exact steps in its own digital yuan development.[19] Western central banks may look to the East for clues as to how to structure their programs, in addition to consulting with several non-governmental organizations and boutique firms that specialize in electronic payments and blockchain technology.

## Summary

The advent of blockchain technology has allowed for a virtual cornucopia of possibilities for individuals, business, and governments around the world. Bitcoin, the first use-case of blockchain technology, showed that the cryptographic advances made up until Satoshi Nakamoto's 2008 whitepaper were enough to build a fully-decentralized digital currency. Twelve years later, Bitcoin continues to thrive and has been joined by a fleet of cryptocurrencies that were, at best, only a thought just a handful of years ago. It is this expansion of electronic payment systems via blockchain technology that has captured the interest of central banks who believe they are uniquely capable of providing not only a better alternative but also able to lay the foundation for an officially-sanctioned global electronic payments regime. However, just as the dreams of cryptocurrency developers tend to be rather lofty, so are those of various CBDC initiatives. Indeed, when researching CBDCs, more questions emerge than answers and many of the important technical specifications are simply nonexistent.

It has yet to be seen how CBDCs will work alongside the current banking infrastructure and how each individual country will integrate possibly differing models to create a functioning global payments system. That said, the initial spark has been set off and a flame could emerge relatively quickly as interest in CBDC seems to grow larger with each passing quarter, drawing increasing attention from investors and central bank watchers worldwide. As the world becomes ever more interconnected and digitized, it appears unlikely that CBDCs will be a passing fad and will instead receive mounting attention from authorities and consumers worldwide.

## Endnotes

[1] Further information on Yapese stone money is provided on page 3.

[2] Keoun, B. (2020, Nov. 12). Story from Policy & Regulation ECB's Lagarde Has 'Hunch' Digital Euro Will Launch in 2-4 Years. Coindesk. https://www.coindesk.com/ecbs-lagarde-has-hunch-digital-euro-will-launch-in-2-4-years

[3] Horizen Academy. (2019). Attacks on Blockchain. https://academy.horizen.io/technology/advanced/attacks-on-blockchain

[4] A cryptocurrency testnet is an alternative blockchain to the economic value chain, known as mainnet. Testnets allow developers to experiment with various upgrades in order to see the effect(s) it may have on the system. One of the core issues with a testnet is that by its nature the coins have no economic value and exploits that require value at-risk may not show immediately, or ever.

[5] Charles Hoskinson suggests that there are multiple avenues to arrive at this goal. However, Cardano has focused on engaging real-world adoption of ADA in more impoverished nations with less stable monetary policy to strengthen their financial condition.

[6] Similar to how stockholders in a public corporation are able to vote their shares to dictate and profit from the direction of the company, Decred enables its token holders to vote on initiatives ranging from the use of treasury funds for marketing purposes to authorizing upgrades to the protocol.

[7] Ethereum's GitHub (https://github.com/ethereum/yellowpaper) defines its yellow paper as "a formal definition of the Ethereum protocol, originally by Gavin Wood, currently maintained by Nick Savers and with contributions from many people around the world." It differs from a cryptocurrency whitepaper in that a yellow paper outlines the technical specifications of the protocol.

[8] On-chain bloat is less of a problem nowadays for Bitcoin due to a variety of cryptographic advances that took place over the last three years. That said, blockchain bloat occurs when there is an increase in the number of parties looking to have their transactions confirmed in a block or due to the size of transaction data broadcasted. At times, the mempool, or number of transactions awaiting confirmation, can grow exponentially. Because the Bitcoin fee mechanism somewhat mimics an auction, it creates a situation where users are continuously bidding the price of block inclusion higher as more transactions request confirmation.

[9] Mellow, C. (2017, Oct. 28). Why Bitcoin Is Right at Home in Emerging Markets. Barron's. https://www.barrons.com/articles/why-bitcoin-is-right-at-home-in-emerging-markets-1509156331.

[10] Engert, W. and Fung B. (2017, Nov.). Central Bank Digital Currency: Motivations and Implications. Bank of Canada. https://www.bankofcanada.ca/wp-content/uploads/2017/11/sdp2017-16.pdf

[11] Maniff, J. (2020, July 1). Motives Matter: Examining Potential Tension in Central Bank Digital Currency Designs. Kansas City Fed. https://www.kansascityfed.org/en/publications/research/rwp/psrb/articles/2020/motives-matter-examining-potential-tension

[12] Lane, T. et al. (2020, Oct. 9). Central Bank Digital Currencies: Foundational Principles and Core Features. Bank for International Settlements. https://www.bis.org/publ/othp33.pdf

[13] Adrian, T. (2019, May 14). Stablecoins, Central Bank Digital Currencies, and Cross-Border Payments: A New Look at the International Monetary System. International Monetary Fund. https://www.imf.org/en/News/Articles/2019/05/13/sp051419-stablecoins-central-bank-digital-currencies-and-cross-border-payments

[14] Richards, T. (2020, Oct 14). Retail Central Bank Digital Currency: Design Considerations and Rationales. Reserve Bank of Australia. https://www.rba.gov.au/speeches/2020/pdf/sp-so-2020-10-14.pdf

[15] White, L. (2018, Apr. 2). The World's First Central Bank Electronic Money Has Come – And Gone: Ecuador, 2014–2018. Cato Institute. https://www.cato.org/blog/worlds-first-central-bank-electronic-money-has-come-gone-ecuador-2014-2018

[16] Murray, R. (2020, Sept. 22). Understanding China's Digital Yuan. Foreign Policy Research Institute. https://www.fpri.org/article/2020/09/understanding-chinas-digital-yuan

[17] Bank of England. (2015, Feb.). One Bank Research Agenda. https://www.bankofengland.co.uk/-/media/boe/files/research/one-bank-research-agenda---summary.pdf?la=en&hash=B2C820FBF6A960C4A625C2DAB5B5B6CE4FEDF120

[18] John, A. (2020, Oct. 19). Explainer: How Does China's Digital Yuan Work?. Reuters. https://www.reuters.com/article/us-china-currency-digital-explainer/explainer-how-does-chinas-digital-yuan-work-idUSKBN27411T

[19] Zhang, Z. (2020, Dec. 7). China's Digital Yuan: Development Status and Possible Impact for Businesses. China Briefing. https://www.china-briefing.com/news/chinas-digital-yuan-status-roll-out-impact-businesses

## Global Economic & Market Strategy

**ALEXANDER VILLACAMPA**

*Associate, Market Strategy and Research*

Alexander Villacampa is an Associate with the Global Economic & Market Strategy team, helping the asset allocation process by furthering the firm's views on the global macroeconomic landscape and achieving this through a combination of rigorous data analysis and narrative construction. Previously, he worked as a wealth manager at Bank of America Merrill Lynch and as an investment specialist at Euro Pacific Capital. He earned his MBA in Economics from The University of Chicago Booth School of Business in 2018 and received his BA in Economics from The University of Florida in 2009. Alexander has passed the CFA Level II exam and is now studying for Level III.

**JUN JIANG**

*Associate Director, Market Strategy and Research*

Jun Jiang is a Market Strategist in Global Economic & Market Strategy team, where he helps to develop and communicate the firm's global macro-economic outlook and market views as well as assisting in the overall asset allocation and portfolio management process. Previously, Mr. Jiang was in the Global Portfolio Strategy unit, where he worked on portfolio strategy and portfolio analytics. Mr. Jiang joined MetLife in 2011. Prior to joining MetLife Investment Management, Mr. Jiang was a Credit & Portfolio Risk Management Analyst at Citigroup.

Mr. Jiang earned a Ph.D. degree in Polymer Physics from SUNY-Stony Brook in 2007 and an MBA degree from Cornell University in 2009. Mr. Jiang is a Chartered Market Technician (CMT) and Chartered Financial Analyst (CFA) charterholder.

# About MetLife Investment Management

MetLife Investment Management (MIM),[1] which had over $651 billion in total assets under management as of September 30, 2020,[2] serves institutional investors by combining a client-centric approach with deep and long- established asset class expertise. Focused on managing Public Fixed Income, Private Capital and Real Estate assets, we aim to deliver strong, risk-adjusted returns by building tailored portfolio solutions. We listen first, strategize second, and collaborate constantly as we strive to meet clients' long-term investment objectives. Leveraging the broader resources and 150-year history of the MetLife enterprise helps provide us with deep expertise in navigating ever changing markets. We are institutional, but far from typical.

For more information, visit: **investments.metlife.com**

[1] MetLife Investment Management ("MIM") is MetLife, Inc.'s institutional management business and the marketing name for subsidiaries of MetLife that provide investment management services to MetLife's general account, separate accounts and/or unaffiliated/third party investors, including: Metropolitan Life Insurance Company, MetLife Investment Management, LLC, MetLife Investment Management Limited, MetLife Investments Limited, MetLife Investments Asia Limited, MetLife Latin America Asesorias e Inversiones Limitada, MetLife Asset Management Corp. (Japan), and MIM I LLC.

[2] At estimated fair value. Includes MetLife general account and separate account assets and unaffiliated/third party assets.

**Disclosure**

For Institutional Investor, Qualified Investor and Professional Investor use only. Not for use with Retail public.

This document has been prepared by MetLife Investment Management ("MIM") solely for informational purposes and does not constitute a recommendation regarding any investments or the provision of any investment advice, or constitute or form part of any advertisement of, offer for sale or subscription of, solicitation or invitation of any offer or recommendation to purchase or subscribe for any securities or investment advisory services. The views expressed herein are solely those of MIM and do not necessarily reflect, nor are they necessarily consistent with, the views held by, or the forecasts utilized by, the entities within the MetLife enterprise that provide insurance products, annuities and employee benefit programs. The information and opinions presented or contained in this document are provided as the date it was written. It should be understood that subsequent developments may materially affect the information contained in this document, which none of MIM, its affiliates, advisors or representatives are under an obligation to update, revise or affirm. It is not MIM's intention to provide, and you may not rely on this document as providing, a recommendation with respect to any particular investment strategy or investment. The information provided herein is neither tax nor legal advice. Investors should speak to their tax professional for specific information regarding their tax situation. Investment involves risk including possible loss of principal. Affiliates of MIM may perform services for, solicit business from, hold long or short positions in, or otherwise be interested in the investments (including derivatives) of any company mentioned herein. This document may contain forward-looking statements, as well as predictions, projections and forecasts of the economy or economic trends of the markets, which are not necessarily indicative of the future. Any or all forward-looking statements, as well as those included in any other material discussed at the presentation, may turn out to be wrong.

L0121010338[exp0123][All States], L0121010339[exp0123][All States], L0121010331[exp0123][All States], L0121010329[exp0123][All States]

MetLife Investment Management