★★★★★★

Chapter 8

Digital Assets: Relearning Economic Principles

Multiple financial crises have struck the United States during the last two centuries. Many of these crises have been caused by institutions that function like banks but are not registered or regulated as banks, so-called shadow banks. For example, the 1907 crisis—then called a "panic"—was mainly caused by trust companies, which were State-chartered entities that competed with banks for deposits. Because these trusts were not part of the central payments system, and thus processed only a small amount of payments, they did not hold a large amount of cash relative to deposits. To earn profits, they made as many loans as possible. After a series of events in October 1907 set off a rush for withdrawals, several trusts faced a run and were forced to suspend credit and liquidate assets, acting as a catalyst for a larger fire sale in financial markets. To save the financial system, J. P. Morgan, owner of the eponymous bank, and a small number of other financial leaders individually chose which banks to bail out (Moen and Tallman 2015). This helped government policymakers realize that when faced with a crisis, the financial system, as then constituted, would rely on a privileged group of individuals seeking to maximize their own profits rather than on institutions that had an obligation to protect the public's interest. This realization helped lead to the creation of the Federal Reserve—the centralized entity that first aimed to serve as the lender of last resort and, over time, also obtained the exclusive power to issue U.S. dollar notes and manage the Nation's monetary policy.

Fast forward 100 years, and digital asset proponents are now aspiring to create a decentralized financial system without relying on governments and their regulatory frameworks, which were shaped by important lessons learned from multiple previous crises, including the 1907 panic. Digital assets are electronic representations of value and operate as part of a complex and interconnected digital ecosystem. Crypto assets are a subset of digital assets that use cryptographic techniques and distributed ledger technology (DLT) but exclude central bank digital currencies (U.S. Department of the Treasury 2022a). DLTs rely on networks to store and process transactions.

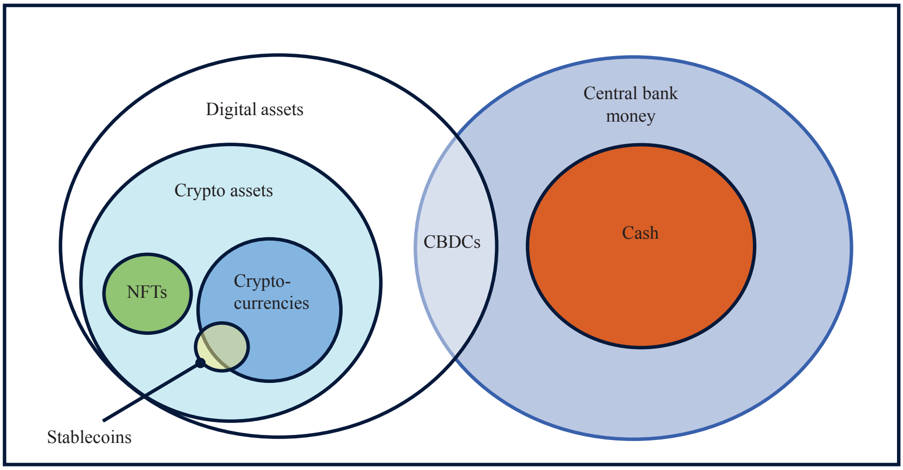
This chapter primarily examines crypto assets, whose proponents have been relearning the lessons from previous financial crises the hard way. In addition to the decentralized custody and control of money, it has been argued that crypto assets may provide other benefits, such as improving payment systems, increasing financial inclusion, and creating mechanisms for the distribution of intellectual property and financial value that bypass intermediaries that extract value from both the provider and recipient. Looking under the hood at these arguments, however, shows a more complicated picture. So far, crypto assets have brought none of these benefits. Meanwhile, the costs generated by several of their aspects—such as those for consumers, the physical environment, and the financial system—are not only substantial but are also being accrued in the present. Indeed, crypto assets to date do not appear to offer investments with any fundamental value, nor do they act as an effective alternative to fiat money, improve financial inclusion, or make payments more efficient; instead, their innovation has been mostly about creating artificial scarcity in order to support crypto assets' prices—and many of them have no fundamental value. This raises the question of the role of regulation in protecting consumers, investors, and the rest of the financial system from panics, crashes, and fraud related to crypto assets. Even so, as companies and governments experiment with DLT, it is conceivable that some of their potential benefits may be realized in the future.

The Perceived Appeal of Crypto Assets

This section reviews the potential benefits that crypto assets may offer, as often touted by their proponents, while the next section evaluates what they have actually achieved. To introduce the digital asset landscape, figure 8-1 illustrates certain types of digital assets. The label "cryptocurrency" is used in the industry to connote a crypto asset that is promoted to be an alternative payment instrument. "Stablecoin" is also an industry label for a form of crypto asset that is purportedly backed by a portfolio of underlying assets and claimed to have a stable exchange value with these assets. While some stablecoins mainly aim to become payment instruments, other stablecoins mainly aim to provide returns from investments. Regardless of the label used, a crypto asset may be, among other things, a security, a commodity, a derivative, or another type of financial product, depending on the facts and circumstances. Nonfungible tokens are the other primary type of crypto asset; they use DLT to track ownership of digital goods but are not a main focus of this chapter.

The term "crypto asset" excludes digital currencies that may be issued by a central bank. Though central bank digital currencies might be designed to operate using DLT, there is no requirement for them to be on DLT, and a central bank digital currency does not necessarily involve using DLT (White House 2022a).

Figure 8-1. A Taxonomy of Digital Assets and Central Bank Money



Sources: CEA analysis; Hoffman (2022).
Note: NFTs = nonfungible tokens. Not drawn to scale. Cash represents currency as well as reserves. Regardless of the label used, a crypto asset may be, among other things, a security, a commodity, a derivative, or other financial product, depending on the facts and circumstances.

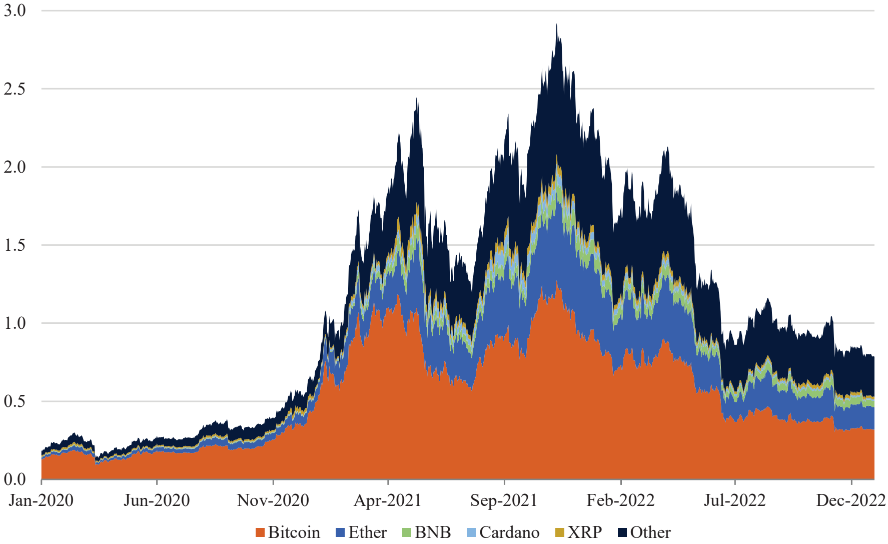
Crypto assets have gained substantial popularity in recent years—particularly since the beginning of the COVID-19 pandemic in 2020. As shown in figure 8-2, the estimated market values of selected crypto assets have increased significantly in recent years and reached a collective peak of nearly $3 trillion in November 2021. As of the end of December 2022, crypto assets collectively had a reported market value of a little under $1 trillion, due to a large downturn in prices over the year, and largely reflecting the failures of certain prominent crypto asset projects and firms.

The development of crypto assets and their underlying distributed ledger technology have the potential to transform industries and business models. Recognizing both the potential opportunities and actual risks of crypto assets, in March 2022, President Biden signed Executive Order 14067, "Ensuring Responsible Development of Digital Assets" (White House 2022b), which tasked the Administration to study the effects of these novel assets. As a result, departments and agencies of the Federal Government have produced nine reports examining the implications of crypto assets for consumers, businesses, financial stability, national security, and the physical environment (White House 2022c).

The first crypto asset, Bitcoin, was launched in 2009, shortly after the global financial crisis, as something of a repudiation of the existing financial intermediaries that caused the crisis (Nakamoto 2008). Bitcoin was

Figure 8-2. Market Capitalization of Selected Crypto Assets, 2020–22

Trillions of dollars (nominal)



Source: Coin Metrics, Inc; Federal Reserve Board of Governors Financial Stability Report.
Note: Total market cap figures are subject to revision from Coin Metrics.

Box 8-1. What Are the Functions of Money?

In early history, bartering was a common way for people to exchange goods and services. Bartering, however, takes time, because individuals need to find another person who is willing to trade one physical good or service for another. A workaround for this was the invention of money; some of the earliest forms of money appeared in about 1200 BCE (Tikkanen, n.d.). Money's key innovation was to facilitate trade between individuals by using an item that had a common representation of value that was widely agreed upon by members of society. That is, instead of having to take a goat everywhere and hoping to find someone who wanted the goat, money enabled individuals to carry something that everyone valued, such as polished beads, which could be exchanged for a wide variety of goods and services (Jordan 1997).

The first money was in the form of things like seashells, beaver pelts, and even large stones (Tikkanen, n.d.; Hudson's Bay Company History Foundation 2016; Goldstein and Kestenbaum 2010). Eventually, money took the form of "specie," or coins such as gold and silver, which could be produced to a specific standard of weight (Velde 2012). While money like specie money was decidedly more convenient than carrying around a goat, it was still cumbersome to transport. To get around this, paper money was created, which was substantially easier to transport. To ensure that paper money still had financial value, it was "backed" by specie (Tikkanen, n.d.). That is, the paper money essentially served as a promissory note for specie sitting in a bank, and it could be freely redeemed.

This system worked well, but it had a key vulnerability that became a common theme of many crises: banks could earn higher profits by issuing more paper currency than the amount of specie they held in their vault. For example, a bank could hold 50 gold coins, but could issue 100 units of a paper currency, each giving the holder the right to 1 gold coin. Then, if all holders of the currency demanded their money back at the same time, the bank would not have enough gold coins to meet the holders' redemptions (Diamond and Dybvig 1983). This dynamic—referred to as a bank run—also has a long history, dating back to as early as the fourth century BCE (Flood 2012).

Eventually, institutions and faith in currencies—particularly the U.S. dollar—became strong enough that specie was not needed to assuage investors' concerns about what was "backing" the currency. This led to the creation and adoption of "fiat" currency, or currency issued by the government that is not redeemable for specie. Fiat currency's value is largely a function of (1) the currency being the only instrument with which individuals can pay taxes; (2) the strength of the government's institutions, such as the legal system and military; and (3) a shared social trust in the value of the money itself (Bank of England 2020).

Money, as defined in the Uniform Commercial Code and certain other specialized sources, is a medium of exchange currently authorized or adopted by a domestic or foreign government (U.S. Commercial Code, n.d.). In contrast, here the economic functions and common understanding of money are considered. For a type of money to actually be useful in the economic sense, there must be *wide agreement about its value*—either derived from assets backing it (e.g., the gold standard) or from things like institutions and social trust. Money serves three core functions: as a medium of exchange, as a unit of account, and as a store of value (U.S. Department of the Treasury 2022b).

First, money can serve as a medium of exchange if it can be used *widely* to trade for goods and services. For example, the U.S. dollar can be used for purchasing anywhere in the country, and even in many places abroad. In contrast, for example, while cigarettes are often used inside prisons to trade for goods and services, they cannot be used to purchase groceries or buy plane tickets (Lankenau 2007).

Second, money can be considered a unit of account if it acts as a benchmark upon which the values of different goods and services can be compared. For example, instead of estimating how many chickens it would take to trade for one cow, a person can instead simply express the value of chickens relative to cows through their respective monetary values—so if 1 chicken costs $10 and 1 cow costs $2,000, then a person can simply use their relative dollar values to conclude that 200 chickens are worth the same as 1 cow.

Finally, money can be a store of value if its purchasing power does not fluctuate dramatically over short intervals of time. For example, the number of apples a $10 bill can buy does not vary much from one day to the next. This is one reason why very high levels of inflation—so-called hyperinflation—can create uncertainty in the purchasing power of money.

"Sovereign money" is money issued by the governing authority of an independent country. Sovereign money can easily satisfy money's functions to serve as a medium of exchange and as a store of value over time. This is because sovereign money is an information-insensitive asset; it is unlikely that one side of a transaction is acting based on private information about the value of sovereign money (Gorton and Zhang 2022). The more information-sensitive an asset is, the less likely it is to be a medium of exchange. For example, if there is a high possibility that someone is buying gold to protect themselves against losses from holding another asset, the gold seller may decide that it is better not to exchange gold for that asset. Sovereign money is also a liability of the central bank, meaning that its value is backed by the bank. The U.S. dollar is widely accepted as a medium of exchange, and it is also a store of value. Indeed, roughly half of all international trade is invoiced in dollars (CRS 2022). This does not mean that all sovereign currencies have the features of money. For example, Zimbabwe's currency lost its role as a store of value in 2007, when its annual inflation rate rose to over 66,000 percent (Siegel 2008). In Zimbabwe's case, consumers and firms shifted toward the widespread use of other sovereign currencies, which effectively replaced Zimbabwe's currency (Noko 2011).

Bank deposits can also act as money. Banks offer deposit accounts to their customers, and these deposits are pegged one-for-one against sovereign currencies. The value of this private form of money is generally supported by a nexus of regulatory and supervisory requirements, such as capital and liquidity requirements, designed to protect the customer against a possible bank run. This account-based private money is linked to an individual person or entity. In contrast to sovereign currencies, there are limits on account-based money to circulate. For example, if Jeff writes a check to Greta to pay rent, Greta's check from Jeff represents money that belongs to Jeff (i.e., the money is linked to his deposit account), and she can redeem it in exchange for circulating currency (cash). Although Greta is legally allowed to exchange Jeff's check for gasoline, third-party checks are not widely accepted as a payment method. Hence, in reality, Greta first needs to cash the check and then purchase gasoline.

designed as a purported peer-to-peer payment system that does not rely on intermediation by a "trusted authority" to keep track of transactions. Instead, Bitcoin uses cryptography to record transactions across an open ("permissionless") network of computers.[1] These transactions are recorded digitally on a "blockchain," which uses cryptographic techniques to link transactions to each other in a manner that makes it challenging to edit or tamper with previous transactions. Because the Bitcoin blockchain is a public ledger, network participants can view and validate transactions as they happen in real time.[2] The supply of bitcoins is capped to ensure that each unit retains value, since digital assets otherwise could be reproduced perfectly forever, and they would have no value if there were an unlimited supply. This "artificial scarcity" was one important feature of Bitcoin, and has been replicated by many new crypto assets introduced since Bitcoin.

[1] There are also "permissioned" DLTs, where all nodes have to be given permission to participate in the network. However, if the trust in the network is established by authentication, that runs counter to the purpose of the trustless system.

[2] Formally, the network tracks the "unspent transaction output" from transactions for each account, which represents the transfer of specific units (e.g., like coins being transferred between individuals), or by how much available funds exceed withdrawals.

Both the number of crypto assets and their combined market value have risen over time, reflecting their increasing popularity around the world. There are several possible benefits that proponents claim for this popularity of crypto assets. These claims are reviewed in the next subsections.

Claim: Crypto Assets Could Be Investment Vehicles

People invest in assets with the hope of making returns on their investments by accepting a certain level of risk of loss. For example, traditional investments such as equities and bonds offer a certain level of expected returns for their risk exposure. Similar to these traditional types of assets, it has been argued that crypto assets are also investment vehicles that offer an expected return for a given risk exposure. Hence, depending on the risk appetite of investors, one might invest in crypto assets with the hope of quickly making a large profit. Moreover, some have argued that crypto assets can serve as a hedge against inflation, hoping their value will keep pace with or rise more than the rate of inflation.

Claim: Cryptocurrencies Could Offer Money-like Functions without Relying on a Single Authority

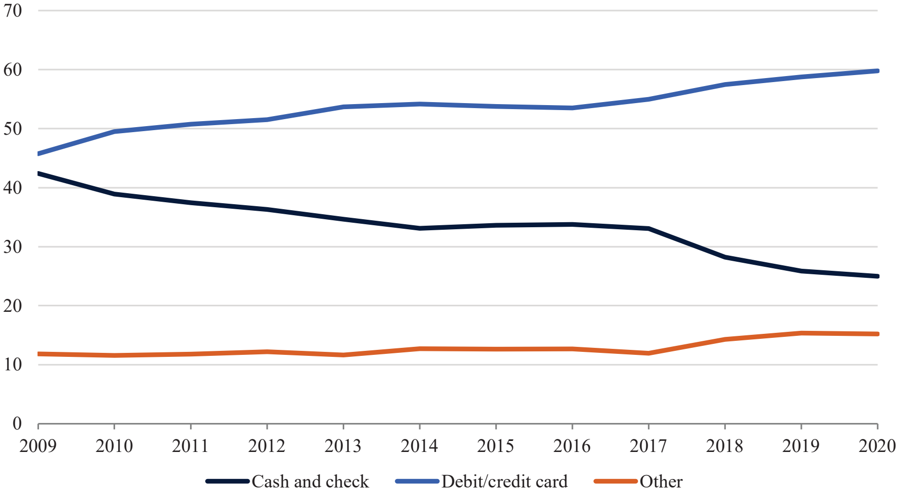
One stated goal of cryptocurrencies has been to create a financial system that is "censorship resistant" and unable to be controlled by a government, instead distributing control among pseudonymous global actors that do not rely upon any trust in existing financial institutions. In particular, some cryptocurrencies aim to replace central authorities that issue money by instead relying on a distributed network, with benefits spread across the network that issues representation of value that can be minted and transacted without central authorities. For example, when implementing monetary policy, governments can profit from issuing money because the value of money is generally higher than the cost of issuing it (this is called "seigniorage"). In contrast, many cryptocurrencies aim to distribute the profit from issuing a cryptocurrency by rewarding participants that can verify a transaction through a consensus mechanism (Acemoglu 2021). In this process, participants can be rewarded with the new issuance of a cryptocurrency as well as transaction fees, earning them a profit for supporting the distributed network that maintains the cryptocurrency. This could be seen as a novel way to distribute the profits from issuing new assets. Box 8-1 discusses the functions of money.

Claim: Crypto Assets Could Enable Fast Digital Payments

In recent years, the usage of cash has declined dramatically as the usage of digital payments has increased substantially. Figure 8-3 demonstrates the trends in cash and check transactions against those in debit/credit payments,

Figure 8-3. Payment Types Used in the United States Over Time

Percentage of payments in a typical month



Sources: Federal Reserve Bank of Atlanta; CEA calculations.

which are forms of digital transactions. In the last decade, payments in cash and checks have declined dramatically, while digital payments have notably increased.

As the demand for digital payments increases, it has been argued that stablecoins could be used as near-instant 24/7 payment instruments (Liao and Caramichael 2022). As of December 22, 2022, there were about 200 stablecoins, with an estimated market size of roughly $140 billion. The two crypto assets Tether and USD Coin alone accounted for roughly 80 percent of the total market of stablecoins.[3] Since stablecoins try to be pegged to a reference asset such as the U.S. dollar (or another currency, or a basket of currencies), proponents argue that stablecoins could eliminate exchange risk when used as a settlement method. That is, if one stablecoin is always worth $1, then an individual using a stablecoin to buy or sell goods has the expectation that its nominal purchasing power will not change dramatically after their transaction. Stablecoins have been suggested as a possible way to simplify cross-border transactions and remittances.

Claim: Crypto Assets Could Increase Financial Inclusion

Some segments of the U.S. population are unbanked, meaning they do not own a bank account. Others are underbanked—that is, they own bank accounts but often use expensive nonbank financial services. Black households have disproportionately higher rates of being unbanked and underbanked (FDIC 2022). Crypto assets often are promoted as a tool for

[3] Market capitalizations exhibit volatility. See, e.g., CoinMarketCap (2023).

reaching these populations to improve their access to financial services and build wealth to achieve upward mobility. For example, many crypto assets do not impose minimum account requirements or charge overdraft fees, in contrast to some traditional banking institutions. Unbanked individuals cite such attributes as primary reasons they do not have bank accounts (FDIC 2022). A recent report found that minority households are more likely to have invested in crypto assets than other households (Faverio and Massarat 2022).

Claim: Crypto Assets Could Improve the United States' Current Financial Technology Infrastructure

The distributed ledger technology that underlies many crypto assets is based on a number of technological advances. It addresses the problem in certain circumstances of establishing trust and a consensus on the true history of transactions among a group of "mutually suspicious" parties. It is effectively a shared database whose contents can generally be trusted, even though it is operated by entities that generally do not have a reason to trust one another. For crypto assets, the database stores the set of transactions that have occurred among network participants. In addition, more recent developments in DLT have enabled new features and improved efficiency, such as "smart contracts," which automatically trigger particular actions without the need for ongoing oversight. Box 8-2 further describes how Bitcoin and distributed ledgers work.

The Reality of Crypto Assets

This section investigates the claimed benefits reviewed earlier in the chapter and presents the risks and costs of crypto assets.

Crypto Assets Are Mostly Speculative Investment Vehicles

As shown in figure 8-4, compared with many other asset types, crypto assets are very volatile, and, hence, highly risky. Because they are very volatile, crypto assets can be used for speculation, an investment strategy that seeks to make a profit from short-run trading. One reason many crypto assets are highly volatile is that many of them do not have a fundamental value. For example, stocks are claims on the future profits of firms and debt is a claim on interest and principal payments. Even commodities such as gold and silver have fundamental values, because they can be used in jewelry and for special manufacturing purposes (Nogrady 2016). Conversely, unbacked crypto assets are traded without fundamental anchors, suggesting that their market prices only reflect speculative demand, or market sentiment, not claims on cash flow. Relatedly, the U.S. Department of Labor (2022) issued

Box 8-2. How Does Bitcoin Work?

This box explains how Bitcoin functions, as it was the first crypto asset. Subsequent crypto assets have often incorporated key features from this design. Bitcoin relies on several innovations, including the novel use of a hash function, a well-established cryptographic technique.

What is a hash function? A hash function, which is sometimes called a “one-way” algorithm or “trap-door” algorithm, uses a mathematical algorithm to take an input (e.g., a number, a string of letters) and produce an output that satisfies three requirements: (1) reproducibility—or running the algorithm on the same input always produces the same output; (2) irreversibility—or even knowing the algorithm, it is not possible to easily invert the output to recover what the input was; and (3) collision avoidance—or any unique input string must produce exactly one unique output. This is a “one-way” function, in that there is no efficient way to recover the input from just the output; the only way would be to hash every possible input to see if it matches the output. Figure 8-i gives examples of hashed output.

The hash function is usually quick and has many applications. For example, most websites do not store a person’s actual password on their servers; instead, they store a hash of the password. That way, if there were ever a hack of their systems, the hackers would only have the hashed versions, which would not work as passwords and could not easily be used to determine passwords. When you log onto a website, its server hashes the password you enter and compares that with what is stored in its database and only lets you in if they match. Note that a change of the input as seemingly small as from “hello” to “Hello” usually creates a drastically different hash, and that a vastly different phrase produces a hash that is equally random. Two key participants in the Bitcoin space are users and miners.

Users. Crypto assets generally require a user to have a “wallet.” A digital wallet is a software application, piece of hardware, or other device or service that stores a user’s public and private cryptographic

Figure 8-i. Examples of Hashed Output

Input Text	Hashed Output (in hexadecimal using the SHA-256 algorithm)
hello	2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
Hello	185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969
The quick brown fox jumps over the lazy dog	d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592

Source: CEA analysis.

keys, which allow users to interact with one or more blockchains and send and receive crypto assets. Users can have custodial wallets, which are provided and maintained by an intermediary or third-party provider, or non-custodial wallets, also known as unhosted wallets, for which users are responsible for their own wallets and private keys. For Bitcoin, wallets have an associated "private key," typically a randomly generated string of digits, which can be hashed to derive a "public key." The public key similarly can be used to generate the wallet's address using a different, known hash function. Anyone can initiate a transfer to a wallet if they know its address. This is used as either the source or destination of transfers on the Bitcoin blockchain. However, to send crypto assets, one needs to know the private key for the wallet that is sending (Outten 2021). In particular, someone wanting to send crypto assets can construct the transaction, create a hash of it, and combine that with a private key to create a digital signature of the transaction. A useful analogy is that the public key is akin to your home address, while the private key is the physical key to your home. It is the difference between letting someone know where you live versus giving them access to your house. Any node of the network can then compare the hash of the digital signature with the public key, and with the hash of the transaction data, and determine if the transaction is valid. Nodes will reject any invalid transactions, so private keys are required to transfer crypto assets.

From the perspective of the user, who typically uses a wallet app to manage this process, all that is needed is the knowledge of the addresses of the sending and receiving accounts, the private key if sending, the amount, and a fee. The fee incentivizes miners to include the user's transaction in an upcoming block. A transaction with a high fee is more likely to be included in upcoming blocks than one with a low (or zero) fee. This means that transactions with low fees may takes days to be processed or may not be processed at all.

Miners. The key part of the Bitcoin ecosystem that is different from physical currency is that there are no central, trusted arbiters of truth. Instead, the system operates by consensus among nodes of the network about what the truth is (i.e., the distribution of bitcoins across all wallets). This means, in theory, that governance of the cryptocurrency is arbitrated by network participants, not a central authority, although control in some blockchains is more centralized as there may be a significant concentration among network participants that effectively consolidates governance between a few parties.

The Bitcoin blockchain uses what is called the SHA-256 algorithm (developed by the National Security Agency and the National Institute of Standards and Technology), which, for any text input, always produces a 64-digit (256-bit) hexadecimal output string (Brown 2002). The Bitcoin blockchain and many other cryptocurrencies use a "proof-of-work" method to achieve a consensus among all the nodes of the network.

Miners monitor the network and maintain a pool of transactions that are yet to be validated. In a proof-of-work network, the network's miners are competing to be the ones to successfully mine the next block of transactions in the chain. The actual way this is accomplished is that the miner puts together a candidate block of transactions to include as well as a "block header," or some metadata for the block (Rybarczyk 2020). These metadata include the hash of the last successfully mined block of the chain, the version of software used, and some technical parameters that are explained just below: the target difficulty, a digital signature unique to the block of transactions they are including (the "Merkle root"), and the "nonce." They then take all the information in the block header, combine it into one string, and push it through the SHA-256 algorithm to get the hash of that information.

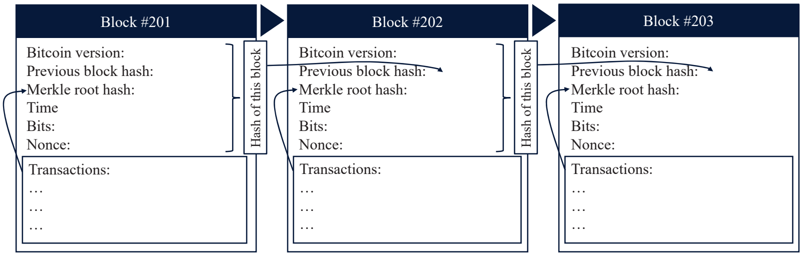
Here is the competition aspect: the nonce field is a number that miners can choose arbitrarily. Their goal is to pick a nonce such that the resulting hash—a hexadecimal number—is less than the target—also a hexadecimal number—currently set by the blockchain. Given how the hashing process works, there is no way to do this efficiently; a miner must continue trying different numbers until they are successful. Since the nonce must be an 8-digit hexadecimal number, a little over 4 billion nonces can be tried. If no possibility is successful, the miner needs to get creative in how to try new hashes against the target, such as changing the set of transactions that are included in the block, which changes the Merkle root in the header, thus changing the proposed block's hash. While finding a valid nonce and set of transactions requires a large amount of brute-force computing power, verifying that a proposed block is valid is trivial—nodes just need to compute the hash of the proposed block and compare it with the target—and this means that once a block is found to be valid and is broadcast across the network, a consensus can be quickly reached that it is a valid block. At that point, it is added to the chain, and competition commences on adding the next block of transactions, the next element of truth in the system.

Miners receive two types of compensation for the work that they do: the fees that are included in the transactions they choose to put in a block; and the "miner reward," defined by the blockchain's protocol. For Bitcoin, the mining reward was initially 50 bitcoin for every mined block, but this has diminished due to a "halving rule." This rule limits the total supply of bitcoins to 21 million over the lifetime of the coin and means that every four years, the payout for mining a new block falls in half. The reward was 6.25 bitcoin, as of December 31 2022; but, given prevailing prices, this was worth over $100,000 (Coindesk 2022). The "target" difficulty parameter is adjusted every two weeks to ensure that a new coin is mined roughly every 10 minutes. As the number of resources dedicated to mining has increased, higher levels of difficulty have been required to keep pace. In the five years before October 2022, the number of attempts to mine a typical block of the Bitcoin chain increased by a factor of 19 (BTC 2022). Once the maximum supply of 21 million bitcoins is reached (which is projected to occur in about 2140), miners will only benefit from transaction fees (Timón 2016).

Why does the blockchain mechanism "work"? Once the blockchain is running, suppose a bad actor wanted to modify the history of the blockchain by, for example, inserting a fraudulent transaction in an earlier block. In theory, this would not work, since any other node of the network could immediately verify that this block did not previously belong in the chain because no subsequent block would point to its (changed) hash as being its predecessor. So, a bad actor would need to recompute the entire chain, from the fraudulent block to the current one, with new hashes, which would require an inordinate amount of computing power. This highlights the origins of blockchain technology in ensuring trust among mutually suspicious groups (Chaum 1982). Figure 8-ii demonstrates how a blockchain is formed.

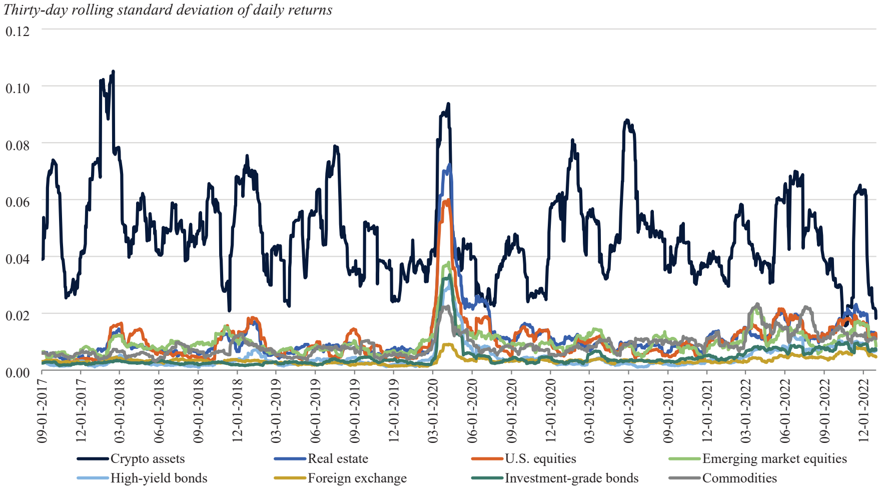
Many other blockchains have a design similar to that of Bitcoin, although with different parameters and features, such as smart contracts. Ethereum, for example, allows more daily transactions than Bitcoin, is calibrated to have blocks added every 12 seconds, and recently switched its consensus protocol to be less energy-intensive (Etherscan 2022). An important criticism of crypto assets is their energy intensity. A more complete discussion of the technological options of blockchain design is beyond the scope of this chapter.

Figure 8-ii. Blockchain Blocks Linked by Hashed Values of Their Contents



Source: CEA compilation.
Note: "Bits" refer to the current difficulty level of mining a new coin. It is stored in an encoded manner, but a lower target implies a higher difficulty. As of October 2022, it required testing approximately 31 trillion nonces to mine a block of Bitcoin.

Figure 8-4. Volatility of Crypto Assets versus Certain Traditional Assets, 2017–22



Sources: Bloomberg L.P.; CEA calculations.

guidance to protect investors' retirement plans with respect to this asset type. Recall that one of the purported benefits of crypto assets like Bitcoin was to hedge against inflation, meaning that their value does not erode as inflation increases. But as inflation increased globally in the second half of 2021 and in 2022, the prices of crypto assets collapsed, proving them to be, at best, an ineffective inflation hedge.

Cryptocurrencies Generally Do Not Perform All the Functions of Money as Effectively as Sovereign Money, such as the U.S. Dollar

As discussed in box 8-1, money serves three functions: as a unit of account, which means that it acts as a benchmark upon which the values of different goods and services can be compared; as a medium of exchange, which means that it can be used to trade goods and services; and as a store of value, which means that the amount of goods and services that a unit of the money can buy does not fluctuate dramatically over short intervals of time. Although cryptocurrencies currently serve each of these functions, they only do so in limited ways in the United States, so they do not serve, from an economic perspective, as an effective alternative to the U.S. dollar.

For the first monetary function question, cryptocurrencies can serve as a unit of account, given that the relative values of goods and services can be expressed in cryptocurrency (e.g., a single chicken in commerce is worth roughly 0.0001 bitcoin). However, individuals would likely need to first convert bitcoins or other cryptocurrencies to dollars to understand relative values as cryptocurrencies are not as effective as the U.S. dollar as a medium of exchange (discussed below). Thus, cryptocurrencies currently do not fully serve as units of account.

The second question is whether cryptocurrencies can serve as a medium of exchange. The answer is that in the United States, they are not as effective a medium of exchange as the U.S. dollar. This is because they can be used to purchase other cryptocurrencies and to buy goods and services at a smaller number of firms relative to the U.S. dollar (Modderman 2022). The strength of the U.S. dollar is derived from several important factors, such as faith in government institutions and the legal system, but cryptocurrencies lack these factors.

Third, cryptocurrencies currently experience substantial amounts of volatility, and thus are not stable stores of value. For example, the value of a bitcoin (relative to the U.S. dollar) increased by over 1,000 percent from March 2019 to March 2021, and then decreased by over 70 percent from November 2021 to October 2022. This volatility means that anyone who is using bitcoins to store their savings is subject to high-volatility risk in their purchasing power. As figure 8-4 shows, the volatility of cryptocurrencies outpaces those of many other financial asset types. Cryptocurrencies regularly exhibit a similar amount of volatility as U.S. equities experienced at the onset of the COVID-19 pandemic.

There is also tension in an asset being promoted as both money and an investment vehicle. As money, the instrument should have a stable value, suggesting limited price volatility. But as a risky asset, it should experience price volatility, for which an investor would be compensated with a high expected return. Holding everything else constant, the riskier an asset is, the less likely it can effectively serve as money.

In sum, in addition to generally being speculative assets, cryptocurrencies currently are not effective alternatives to sovereign money such as the U.S. dollar. As mentioned above, most cryptocurrencies do not have fundamental value, but that is not a requirement for them to function as money. In fact, sovereign money does not have a fundamental or intrinsic value (Berentsen and Schär 2018). Even so, sovereign money can easily satisfy money's requirements, as discussed in box 8-2. The main reason for this is that the value of sovereign money is backed by a trusted institution—the central bank. One important feature of many cryptocurrencies is validating transactions through consensus mechanisms, which are a way to distribute profits from new issuance among participants such as cryptocurrency miners that verify the cryptocurrency transactions. (See box 8-3 for the impact of cryptocurrency mining on the physical environment.) Hence, the supply of cryptocurrency generally increases with the number of verified cryptocurrency transactions. In the case of a new issuance of sovereign money, monetary policy reasons play a major role, and the resulting profits from the new issuance of sovereign money accrue to governments. In advanced

Box 8-3. Crypto Asset Mining as a Risk to the Environment

The growth of trading in crypto assets has necessitated a corresponding increase in the mining of crypto assets. As discussed in box 8-2, crypto asset “mining” (cryptomining for short) is a process by which high-powered computers perform calculations to verify transactions using distributed ledger technology for some kinds of crypto assets (White House 2022d).

Cryptomining can be lucrative for successful miners, which are compensated with the crypto assets they are mining but which also consume large amounts of energy. According to recent estimates by Goldman Sachs, cryptomining accounted for more than 2 percent of U.S. power consumption as of early 2022. The amount of electricity used to mine bitcoins in the United States is similar to what is used to power all the country’s home computers or residential lighting (White House 2022d). A recent inquiry by Congress into the electricity consumption of cryptominers found that just seven of the largest cryptomining operations in the United States had a combined capacity of 1,045.3 megawatts as of February 2022, with plans to expand capacity significantly in the coming months and years. For comparison, these miners alone could use roughly as much power as all residential units in Houston, the Nation’s fourth-largest city (Tabuchi 2022).

While comparing usage across different types of activities is difficult because not all activity is recorded on-chain, some have estimated that in 2021 mining a single bitcoin used roughly the same amount of electricity as nine years’ worth of the average American household’s consumption (Huang, O’Neill, and Tabuchi 2021). Bitcoin additionally uses more energy than several entire *countries*, such as Finland, Belgium, and Chile (University of Cambridge 2022). Globally, Bitcoin accounts for 0.42 percent of all electricity usage. This effectively means that Bitcoin is using the same amount of electricity as a medium-sized advanced economy.

Not all cryptomining operations consume the same amounts of power. Energy-intensive consensus mechanisms, such as a proof-of-work, use substantial amounts of power by encouraging machines in a network to race against each other to solve a mathematical puzzle. Bitcoin, which accounted for over of a third of all crypto assets’ value as of December 2022, is the most notable crypto asset that is mined using proof-of-work. Ethereum, conversely, switched in September 2022 from a proof-of-work consensus mechanism to a proof-of-stake consensus mechanism that selects specific miners to validate a transaction at a given point in time, thereby reducing electricity usage in exchange for reducing the security of the network and increasing the power of individual actors vis-à-vis the network’s intensity. There are benefits and drawbacks from different consensus mechanisms, and they have different energy, transparency, and security attributes. Despite Ethereum's switch to proof-of-stake, Bitcoin has not announced plans to make a similar change.

Evidence suggests that cryptomining has substantial costs for local communities and has few, if any, attendant benefits. Cryptomining facilities produce substantial noise pollution, which has been compared to a "jet-like roar" (Williams 2022). Cryptomining facilities can also lead to increases in local air and water pollution (White House 2022d).

Local cryptomining operations also push up community electricity prices, as increased electricity consumption forces generators to rely on more expensive energy sources and, in the case of communities with hydropower where cryptomining operations are often located, reduces electricity surpluses. For example, in the Mid-Columbia Basin of Washington State, an energy surplus produced by hydroelectric dams originally pushed down electricity prices for both residents and businesses. But after cryptomining facilities began placing additional demand on the energy grid, exports of energy surpluses decreased, substantially raising residential electricity prices (Samford and Domingo 2019).

Continuously running an electricity grid at maximum capacity can cause grid equipment that was not designed for such high-intensity usage to degrade over time, increasing the risk of fire in vulnerable communities. In places like Texas, which expects to add 27 gigawatts of additional cryptomining demand in the next four years—equal to roughly 30 percent of the generation capacity of the entire Texas grid—cryptomining could increase the likelihood of power crises, where demand overwhelms the grid's ability to provide sufficient generation (Calma 2022).

Furthermore, the intensive nature of mining bitcoins requires frequently replacing machines, and as the old equipment becomes nonfunctional, it can become "e-waste," which often contains toxic chemicals and heavy metals that can leach into soils if not properly disposed of (de Vries and Stoll 2021). Just as mining energy-usage comparisons are difficult, comparing e-waste across activities is imprecise, especially because old machines used to mine bitcoins may be temporarily retired but then used again if the price increases enough (White House 2022d). With that being said, some have estimated that it would take as much as 114,000 Visa transactions to generate the same amount of e-waste as a single bitcoin transaction. Alternatively, a single bitcoin transaction may generate more e-waste than 2.7 iPhones (Digiconomist 2022).

economies such as the United States, the profits from the issuance of sovereign currency benefit taxpayers by lowering tax needs, as central banks effectively return these profits as government revenue.

Stablecoins Can Be Subject to Run Risk

Some cryptocurrencies, specifically stablecoins, are promoted to have the potential to be fast digital payment instruments. A fundamental problem with stablecoins is one that has been known in the traditional banking sector for centuries: *run risk* (Humphrey 1975). If stablecoin holders wish to redeem their stablecoins for $1 each, this will require the stablecoin issuer to liquidate some of its reserves (Adams and Ibert 2022). Depending on how liquid these reserves are, and the state of broader financial conditions, this liquidation may lead to disruptions in the markets for the reserve assets and reduce the market value of the issuer's remaining reserves because the sales of the reserve assets put further downward pressure on the prices of remaining reserves. If reserves are falling in value at the same time holders are seeking redemptions, then the issuer may receive less than $1 for each $1 placed in stablecoins, thereby causing the stablecoin issuer to become insolvent. In fact, money market funds, which have balance sheet characteristics that a number of stablecoins purport to have, faced runs during the 2008 financial crisis and at the onset of the COVID-19 pandemic in 2020 (Schmidt, Timmermann, and Wermers 2016; Anadu et al. 2021).

Deposits in bank accounts can be used to make payments, and banks aim to maintain parity between deposits and dollars; that is, $1 deposited in a bank account can be withdrawn for $1 at a later point in time. One important distinction between stablecoins and bank deposits is that in the United States, bank deposits are subject to a comprehensive set of regulatory and supervisory requirements. In contrast, stablecoins are not subject to requirements designed to maintain this exchange rate.

A different approach to maintaining a stablecoin that does not fully rely on holding reserves is the so-called algorithmic stablecoin of TerraUSD (and the closely linked Luna token), which had the stated objective to maintain its exchange rate peg with the U.S. dollar using an algorithm (Baughman et al 2022). The idea behind the Terra/Luna coins was that Terra (known as UST) was a stablecoin pegged to $1 and was maintained through arbitrage (Wong 2022). Theoretically, 1 UST could always be traded for $1 worth of Luna. If the value of Terra ever fell below $1, arbitrageurs could exchange 1 Terra for $1 worth of Luna, a different coin. In theory, this would allow the arbitrageur to make a gain, decrease the supply of Terra (the exchanged token was "burned"), and raise the value of Terra. If the value of Terra rose above $1, arbitrageurs could buy ("mint") 1 UST in exchange for $1 of Luna, making a small gain but increasing the supply of Terra and pushing down its value. This was meant to be the mechanism to keep the value of Terra at $1, although there was also a reserve of other cryptocurrencies kept to support the peg, but not enough to fully cover the market value of Terra. At one point, Terra was the world's fourth-largest stablecoin, in part due to the fact that people who were willing to deposit UST on Anchor, a smart contract-lending protocol, which promised investors an annual interest rate of 19.5 percent on their investments (Briola et al. 2023). Eventually, a run occurred as a few major withdrawals in May 2022 knocked UST off its $1 peg, leading to a stampede out of Terra into Luna, depressing Luna's value, and ultimately causing the total crash of the two cryptocurrencies.

Another key risk of stablecoins for U.S. retail users is that redemption may be a secondary concern for liquidity on crypto asset trading platforms. As noted in the Financial Stability Oversight Council's "Digital Asset Financial Stability Risks and Regulation Report," U.S. retail customers cannot directly redeem the two largest stablecoins (Tether and USD Coin) for dollars (U.S. Department of the Treasury 2022a). Stablecoin holders that lack redemption rights may be unable to find willing counterparties to exit their stablecoin positions.

Gorton and Zhang (2021) evaluate a number of solutions to the run risk of stablecoins. For example, they assert that if stablecoins are required to be fully backed by safe assets, they would risk attracting funds that would ordinarily go to banks, which make loans. This would have the potential to hurt credit availability for individuals and firms. In subsequent research, Gorton and Zhang (2022) argue that stablecoins could challenge the government's monetary authority to have an exclusive monopoly on currency issuance and disrupt financial stability.

Stablecoins currently have a few major impediments against becoming fast payment instruments. For one, stablecoins are too risky to satisfy this need at present. Additionally, as discussed below, general concerns about consumer and investor protections in the crypto asset space also apply to stablecoins (U.S. Department of the Treasury 2022a). Nevertheless, there is continuing experimentation in using distributed ledger technology for digital payment systems. While crypto assets are currently not payment or settlement technologies for the rest of the financial system, it is still possible that in the future, their underlying DLT could be adapted into a payment or settlement system for the broader financial system.

Crypto Assets Can Be Harmful to Consumers and Investors

For consumers and investors to use crypto assets to access financial services, the crypto asset industry must have sound consumer, investor, and market protections. However, many participants in the crypto asset industry are not acting in compliance with existing laws and regulations, and some of the most common unlawful activities in the crypto asset industry are scams especially aimed at retail investors (U.S. Department of the Treasury 2022a). One of the principal areas where there is mass noncompliance is disclosure surrounding crypto assets that are securities. This lack of disclosure prevents investors from recognizing that most crypto assets have no fundamental value. For example, many fraudsters develop intricate and professional-looking websites that purport to offer investors an exciting, high-return investment opportunity. When a victim gives crypto assets to the criminal to invest, the criminal can simply abscond with the funds. Examples of this includes a matter in September 2021, when the U.S. Securities and Exchange Commission (SEC) filed an action against the platform BitConnect for allegedly committing $2 billion worth of fraud (SEC 2021a). In its action, the SEC alleged that BitConnect purported to offer investors a "lending" program using a "proprietary volatility software trading bot," but instead simply took investors' crypto assets and transferred them into digital wallets controlled by the criminals. To date, the SEC has filed charges alleging a number of fraudulent offerings and other types of misconduct involving crypto assets (SEC 2022).

In May 2021, the Federal Trade Commission (FTC) released a post detailing the increase in scams involving crypto assets since October 2020 (Fletcher 2021). Between October 2020 and May 2021, more than 7,000 people reported losses from these scams, which totaled more than $80 million, with a median loss of $1,900. One particular type of scam identified by the FTC is "giveaway scams," where promoters claim to instantly multiply a given number of crypto assets but instead appropriate the crypto assets upon receipt. According to the FTC, young people were most susceptible to this type of fraud; those between 20 and 39 years of age lose far more money to investment fraud than any other type, more than half of which was attributable to crypto assets.

In November 2022, the Consumer Financial Protection Bureau (CFPB) released a bulletin summarizing the consumer complaints it had received about crypto assets (CFPB 2022). In a period of less than four years, from October 2018 to September 2022, the CFPB received more than 8,300 complaints related to crypto assets, with the majority received since 2020. In this period, roughly 40 percent of crypto asset complaints handled were primarily frauds and scams. Transactional issues with crypto assets and issues with assets not being available when promised made up about another 40 percent of complaints. Other risks identified in the CFPB's bulletin included romance scams and "pig butchering," difficulty obtaining restitution, and fraudulent transactions.[4]

[4] Pig butchering refers to a practice where scammers develop close personal relationships with a victim in order to convince them to set up crypto asset accounts from which the scammers can steal.

Furthermore, there can be conflicts of interest at crypto asset platforms. For example, some crypto asset platforms combine exchange, brokerage, market making, and clearing agency functions. This vertical integration of products and services has long been prohibited in traditional markets and leads to risks to customers. For instance, a platform that combines exchange and market making functions would have an incentive to trade ahead of its own customers, and would have less incentive to seek out best executions for its customers. FTX, one of the largest crypto asset platforms until 2022, reportedly transferred billions of dollars in customer accounts to its affiliated trading firm, Alameda Research (Goldstein et al. 2022). By borrowing against FTT, the native token of FTX, Alameda Research reportedly made risky bets and lost a large fraction of FTX customers' funds (Tortorelli and Rooney 2022). In November 2022, FTX and its affiliates declared bankruptcy and the price of FTT posted massive losses; at this time it is unclear whether FTX customers and creditors will get their funds back (Ge Huang, Osipovich, and Kowsmann 2022).

There Have Been Limited Economic Benefits from DLT Technology

The ability of DLT to solve the difficult problem of ensuring that two parties that do not have a reason to trust each other can nonetheless transact securely is a notable achievement of computer science. This solution has led to excitement about DLT, with even some enthusiasm that this technology will change the way business is done (Iansiti and Lakhani 2017). DLT and blockchain technology are not necessarily suitable for all applications; some considerations have been proposed for successful blockchain technology applications (Yaga et al. 2018). See box 8-4 for the proposed DLT use cases. However, at its core, DLT is simply a database, and many proposed DLT-based projects do not actually employ decentralization (as discussed below). Some have sought to profit from the hyperbole of blockchain—it has become a common tactic for non-crypto-related businesses to announce a "pivot to blockchain" to generate interest in a product or enterprise (Griffith 2018). For example, in December 2017, a beverage maker named "Long Island Iced Tea" added "Blockchain" to its name—though changing nothing substantive about its business—and its stock shares tripled in value (Cheng 2017). Ultimately, three persons involved with the firm were charged with insider trading by the SEC, which alleged that these insiders used the "pivot to blockchain" tactic to increase the firm's share prices before they sold their stakes in the firm (SEC 2021b).

In addition, many prominent technologists have noted that distributed ledgers are either not particularly novel or useful or they are being used in applications where existing alternatives are far superior. For example, Bruce Schneier (2019), a cybersecurity expert, has called crypto assets "useless"

Box 8-4. Proposed Uses of Distributed Ledger Technology

The excitement generated about DLT has drawn substantial investment capital and has prompted governments and firms outside the crypto asset industry to experiment with its underlying technological processes. In some cases, this excitement has led to large writedowns or failed projects. Here, we review three current cases and give examples of experimentation.

Walmart Canada and supply chains. A commonly touted use for distributed ledger technology is supply chains, where a single, distributed ledger could improve traceability throughout a supply chain and reconcile records between a firm and its multiple suppliers (Laaper, n.d.). In 2021, Walmart Canada launched a blockchain that attempted to handle payment disputes between 70 third-party freight carriers. An article in the *Harvard Business Review* dubbed the experiment "a tremendous success," noting that before the blockchain system, 70 percent of invoices were disputed, but after the rollout, that share dropped to less than 1 percent (Vitasek et al. 2022). Though seemingly impressive, the firm that partnered with Walmart Canada to develop the blockchain platform stated in a report describing the project that the platform ran on "more than 600 virtual machines (VMs) to securely store and manage data points from thousands of transactions per day" (Hyperledger Foundation, n.d.). This implies that each VM is, at a maximum, handling 17 transactions per day. For reference, a minimally configured AWS (Amazon Web Services) RDS (relational data store) database with two VMs configured with best practices could process thousands, if not tens of thousands, of transactions per second (Amazon 2017). Furthermore, a prominent technologist stated that it was not even obvious what functional role blockchain was playing in the system, and that the program was more akin to using an existing technology in an inefficient way (Orosz 2022).

Helium and the decentralized Internet. Helium is a company that is attempting to build a peer-to-peer wireless network by allowing users to buy "hotspots"—small devices that can send data over long distances—that can, together, create a Wi-Fi network. When the company was founded, it did not intend to have crypto assets as a central part of its business model (Roose 2022). Instead, it attempted to use traditional economic incentives for those helping build the network by simply sharing some of the fees from network users to hotspot owners. In 2019, however, the company pivoted and attempted to make crypto assets central to its business model by creating an incentive system where users that purchased hotspots that cost roughly $500 (and thus contributed to the network) were rewarded with Helium crypto asset tokens. If the prices of tokens rose, then so, too, would the reward for owning a hotspot, thus encouraging more users to build out the necessary network infrastructure.

After this pivot, large venture capital firms like Andreessen Horowitz (also known as a16z) helped Helium raise hundreds of millions of dollars in equity (Seward 2021). Alameda Research (the failed hedge fund affiliated with FTX) was also a large investor in Helium. Despite the sizable funding and widespread interest, Helium came under scrutiny in July 2022, when its cofounder tweeted that the company had generated $2 million a month in fees from new users joining (buying hotspots), but only $6,500 (0.3 percent) of that was from users actually using the Internet service (Levine 2022). Furthermore, a Forbes investigation in September 2022 found that the executives of the firm gave themselves and their families a windfall in Helium tokens early in the company's history that was not publicly disclosed (Emerson, Jeans, and Liu 2022). Also, in September 2022, Helium ended the use of its own blockchain, which purportedly incentivized broader provision of Internet access as a core feature ("proof of coverage") and shifted its operations and coins to the Solana blockchain, the same technology on which many other speculative crypto assets are traded, calling into question whether this use could be distinguished from any other type of crypto asset (Yaffe-Bellany 2022). Although these pieces of news may present a significant headwind for Helium's future, the Helium token nonetheless has a market value (as of December 22, 2022) of over $253 million (CoinMarketCap 2022).

Nonfungible tokens and virtual real estate. Nonfungible tokens (NFTs) are digital assets that are not interchangeable. Each NFT is unique, with its ownership recorded on a distributed ledger. Ownership of an NFT can pass between two users by recording the transaction and transferring it on a blockchain. NFTs often contain a pointer to a digital object, such as an image file. As a famous example, in March 2021 Jack Dorsey, the cofounder and former CEO of Twitter, auctioned off an NFT of an image of his first tweet on Twitter from 2006, with the winning bid coming in at more than $2.9 million (Locke 2021). While anyone could create ("mint") a new NFT of the same digital image (and the digital image can be easily reproduced), the original transaction is maintained on a blockchain, so it would not truly be the same (OpenSea 2022). This highlights the "artificial scarcity" view of crypto assets.

Borri, Liu, and Tsyvnski (2022) studied the market for NFTs from 2018 to 2021 and created an index of NFT value based on the repeat sales method. They found the average NFT market return was 2.5 percent a week in this period, although with a weekly standard deviation of 19 percent. This highlights the volatility and variability of NFT returns. The market for NFTs cooled in 2022; the owner of Dorsey's tweet listed it for sale in April 2022 for $48 million, but the highest bid as of January 4, 2023, was about $82,000 (OpenSea 2022).

NFTs can be a natural way to track ownership of virtual real estate. Several different "metaverses" have begun offering "land" in virtual worlds. Ownership of land translates into the title of a virtual property being recorded on a distributed ledger. What one does with their land depends on the platform—on Decentraland, a large metaverse platform, owners are free to develop their land as they see fit: they could open a store selling virtual goods, create a game app for visitors, build a gallery for their virtual art collection, or build a virtual "house" (Kamin 2021). Dowling (2022) studied the value of land in Decentraland and found that the daily values of the virtual land tokens between 2019 and 2021 changed with extreme volatility. As in the physical world, location matters—while the average transaction value for a property in the data set is $1,311, a firm paid $2.5 million for land in Decentraland's Fashion District (Putzier 2021).

Experimentation. The current uses discussed above have demonstrated only limited, if any, economic benefits so far. Even so, proponents still claim that this technology could find productive uses in the future as companies and governments continue experimenting with potential uses; however, they often use "permissioned" networks of machines that have been authenticated as a trusted member of the network (Oracle 2022). For example, it is possible that distributed ledger technologies can be used to improve the settlement and clearing processes of banks (Bech et al. 2020). In fact, as mentioned above, banks are experimenting with distributed ledger technology to improve the efficiency of trading, clearing, settlement, and custody (Yang 2022). In addition, the New York Innovation Center of the Federal Reserve Bank of New York (2022) is participating in an experiment with the notion of a regulated liability network, a conceptual financial market infrastructure that could enable transactions between regulated financial institutions potentially using DLT.

and has noted that despite claims of being decentralized and trustless, blockchain-based applications are in practice neither; often, users access their crypto assets by going to a limited set of crypto asset platforms, and a small group of miners perform the majority of mining in most crypto assets, an activity that has costly implications for the physical environment, as discussed in box 8-3. When it comes to the "trustlessness" of blockchains, Schneier notes that a blockchain does not eliminate the need for trust but simply shifts trust away from individuals and institutions to a technology—along with all its features and bugs.

James Mickens, a leading computer scientist who studies distributed systems, has stated that in addition to not actually being decentralized and trustless, blockchains are often a very poor fit for their purported uses (Mickens 2018). This is primarily because the instant that the identity of a person or firm is needed (as is the case for supply chains, medical records, and land deeds), existing technologies can solve the same problem in a much more efficient way. For example, many of the cybersecurity benefits of an immutable, distributed blockchain can be replicated through existing features like tamper resistance (the ability to not change digital signatures at a later point in time) and nonrepudiation (a receipt of a sender of information's identity that is delivered to both the sender and receiver of information, thus guaranteeing that both parties have processed the information) (World Bank, n.d.; NIST, n.d.).

Proponents of blockchain technology claim that it will not only improve firms' performance but also be the backbone of an entirely new Internet. Web3—the so-called new Internet—purports to retain all the privacy/networking benefits of the earliest versions of the Internet that existed roughly before 2000 (often called "web1," which featured decentralized, community-governed open protocols), while keeping the high functionality of various features of web2 (the current version of the Internet) without the existing dependencies on large centralized firms like Google and Apple (Dixon 2021). However, Moxie Marlinspike (2022), the cryptographer and founder of the messaging app Signal, argues that the reason the current Internet features so much centralization is because it makes things easier, for two specific reasons. First, he argues that a decentralized Internet would require individuals and firms to host their own servers. However, centralized hosting of servers can be done much more cheaply and reliably by large entities and therefore benefits from economies of scale. Second, he notes that protocols—or the rules that Internet systems run on—are much more difficult to change than platforms. That is, centralized, non-open-source protocols can be managed by a single entity (as opposed to many), facilitating a wider variety of features that can change with much greater speed than if they were decentralized. Marlinspike also notes that web3 is already trending toward a centralized structure because of the ease and convenience that centralization brings, but in a much clunkier way than if traditional technology were being used. He specifically notes that "once a distributed ecosystem centralizes around a platform for convenience, it becomes the worst of both worlds: centralized control, but still distributed enough to become mired in time."

Table 8-1. Top Ten Crypto Derivative Platforms by Open Interest

Rank (1)	Exchange (2)	24-Hour Open Interest (Nominal $) (3)	24-Hour Volume (Nominal $) (4)
1	BTCEX	$8,314,364,513	$7,180,531,116
2	Binance	$7,714,660,817	$32,741,616,672
3	BTCC Futures	$5,103,831,418	$7,968,963,153
4	Deepcoin	$4,781,751,226	$9,854,658,307
5	BingX	$4,334,560,170	$5,165,147,675
6	Bitget Futures	$4,331,916,947	$5,414,169,494
7	OKX	$3,586,501,924	$8,449,781,644
8	Bybit	$3,397,272,483	$8,090,497,597
9	MEXC Global	$3,228,041,626	$2,263,323,835
10	Bitmart Futures	$2,707,627,218	$4,283,383,129

Source: CoinGecko. Data were collected on January 19, 2023.

The Risks of Financial Innovation

While the crypto assets ecosystem and its underlying technology introduce the potential for newfound efficiencies, efforts to challenge basic economic principles have frequently resulted in financial calamities. The economist Hyman Minsky hypothesized that financial crises often follow a similar cycle, whereby initially strong investments turn increasingly more speculative until a bubble bursts (Minsky 1992). Further, Minsky stated that this repeatedly happens because regulators are initially vigilant in the immediate aftermath of a crisis; but as time goes on, and the instrument of speculation changes, regulators take a less proscriptive approach to not harm "innovation" (Minsky 2008). According to Minsky, this relaxed regulatory environment invariably leads to another crisis. Indeed, other economists have argued that the most effective financial regulation has been introduced only *after* a crisis has occurred (Gorton 2012). Minsky's theories became popular in the aftermath of the global financial crisis, when complicated financial products involving mortgages that exacerbated the crisis were initially hailed as innovative, and individuals discussing their risks were labeled "Luddites" by prominent commentators (Cassidy 2008; Wheatley 2013).

Minsky's writings, as they apply to past financial crises, may prove instructive for policymakers today. Fortunately, there has not yet been a systemic crisis caused by crypto assets, in part because they are not yet fully integrated with the rest of the financial system, giving policymakers time to act appropriately. The risks presented by crypto assets stem from excessive speculation, high leverage, run risk, environmental harm from crypto asset mining, and fraudulent activities that harm retail investors and corporations. Because crypto assets appear to be here to stay, policymakers should consider these risks to avoid a “Minsky moment” caused by crypto assets.

Other Risks from Crypto Assets

Some risks that apply to crypto assets require further examination. Many of these risks are not unique to crypto assets; combined with innovative technology, they pose challenges for policymakers and regulators trying to minimize risks while encouraging responsible innovation.

Leverage risks. Crypto asset derivative platforms—where investors can buy and sell financial derivatives linked to crypto assets—have seen substantial growth in the past two years (Damalas et al. 2022). Table 8-1 shows that the top 10 platforms for crypto asset derivatives, which account for roughly 76 percent of all volume in these derivatives, have over $47 billion in open interest and roughly $91 billion in daily trading as of January 18, 2023. According to one international regulator, one of the largest platforms, Binance, refuses to provide adequate and reliable information in response to regulatory requests (FCA 2021).

Exchanges frequently tout the high amount of leverage they offer clients, stating that investors can take up to 100-to-1 leverage (debt-to-equity ratios) (Pechman 2021). These derivative platforms can create financial instability because positions with high leverage (debt-to-equity ratios) can amplify a shock to prices of crypto assets and lead to large losses and even defaults (U.S. Department of the Treasury 2022c). In particular, leverage leaves little room for prices to fall in a short amount of time, as steep price declines could induce brokers to issue large margin calls, thus forcing broader liquidation (Carapella et al. 2022).

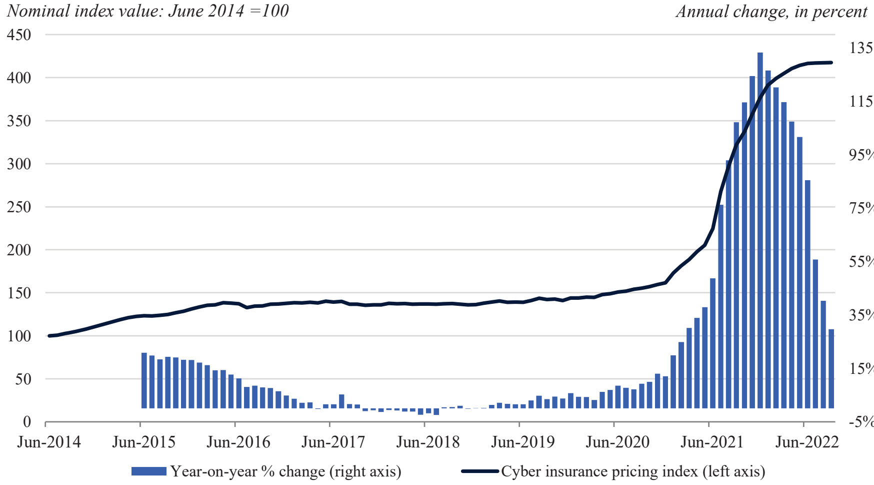
A relatively new application of DLT in financial markets where there is a relatively unknown amount of leverage is so-called decentralized finance (DeFi). DeFi attempts to offer financial products, such as loans, on the blockchain through the use of “smart contracts” (Carapella et al. 2022). The basic promise behind DeFi is to replace financial intermediaries, instead linking savers directly with borrowers (or buyers with sellers), allowing them to save on the spread that traditional intermediaries charge for creating the match with software. Though DeFi applications claim to help broaden access to credit by decreasing intermediation fees, they create serious risks to investors and cause at least two risks for the broader financial system: the use of significant leverage, and the performance of regulated functions without compliance with appropriate regulations. DeFi platforms acting as unregulated banks, broker-dealers, exchanges and other entities subject to regulation should be operating in compliance with existing regulations and rules. DeFi lending platforms effectively receive funds from investors and use them to generate loans, promising interest to investors. This dynamic inherently causes run risks, where more investors try to redeem more of their funds than the platform can accommodate at a given time, thus causing the platform to either suspend convertibility or fail outright (Carapella et al. 2022). Furthermore, DeFi presents the opportunity for "synthetic leverage," whereby investors can mask the true amount of leverage they are undertaking from the party from which they are borrowing (Tian 2021). If DeFi were limited to small, retail investors, the failure of a DeFi platform could still hurt these investors, but the shock could be relatively contained. Banking agencies issued a statement that expressed concerns with business models that are concentrated in crypto-asset-related activities or have concentrated exposures to the crypto asset sector (Federal Reserve Board 2023).

Price volatility. Most crypto assets experience substantial price volatility. Holding such volatile assets could present challenges for large financial institutions if they were permitted to hold crypto assets, as the volatility would lead to constant changes on the asset side of their balance sheets. This volatility, in turn, could increase funding costs for banks and other financial institutions, thereby requiring banks—which fundamentally borrow so as to be able to lend—to increase the funding costs (interest rates) that they charge, leading to tighter credit conditions.

Currently, this contagion risk is relatively muted, given that banks are limited in their ability to conduct crypto-related activities, such as acting as custodians of crypto assets (i.e., holding crypto assets for clients, not on their own balance sheets) (OCC 2020). Indeed, banking regulators such as the Federal Reserve have issued guidance requiring regulated financial institutions to inform their regulator before engaging in crypto-asset-related activity (Gibson and Belsky 2022). But other, less-regulated financial institutions, such as hedge funds, are increasingly investing in crypto assets. Such activity of lightly regulated or nonregulated entities can lead to "liquidity spirals," as described by Brunnermeier and Pederson (2007). These spirals occur when a dramatic crash in the price of an asset—such as a crypto asset—leads a hedge fund to be margin-called, requiring the fund to sell off other positions to meet the margin call. If enough funds are exposed to the asset or assets with declining prices, then sell-offs could be broad enough to cause a deterioration in market liquidity.

Illicit finance risks. Crypto assets are the standard form of payment extorted from victims of "ransomware," whereby a malicious actor hacks an organization and demands payment to release control of the victim's network and often to purportedly forgo leaking the victim's stolen data. Crypto assets remove a critical friction in performing a ransomware hack. Because the attacker can demand that crypto assets be sent to a pseudonymous wallet

Figure 8-5. Nominal Cyber Insurance Prices Over Time



Source: Howden Nova Analytics platform.

instead of a bank account linked to a specific person, attackers can more easily launder or obfuscate payments made to them, in comparison with fiat currency (U.S. Department of Justice 2022). Importantly, like other financial assets, crypto assets can be misused for a range of illicit activities, including ransomware payments. Crypto assets have also been misused by human traffickers, by individuals exploiting children for sexual abuse, and by drug traffickers and scammers; to fund the activities of rogue regimes, such as the recent thefts by the Lazarus Group, which is affiliated with North Korea; and to finance terrorist activities (GAO 2021; U.S. Department of the Treasury 2022d). The other key illicit financing risks associated with crypto assets come from gaps in implementation of the international Anti-Money-Laundering/Combating-the-Financing-of-Terrorism (AML/CFT) standards abroad; the use of anonymity-enhancing technologies; in some cases the lack of covered financial institutions as intermediaries—and thus the absence of AML/CFT controls—in some crypto asset transactions; and service providers that are noncompliant with AML/CFT and other regulatory obligations, including compliance with sanctions obligations. With regard to the last, when crypto asset firms fail to register with the appropriate regulator, fail to establish sufficient AML/CFT controls, or do not comply with sanctions obligations, criminals are more likely to exploit their services successfully, including to circumvent U.S. and United Nations sanctions.

Ransomware uses. As hacking to receive crypto assets becomes more widespread, more firms will attempt to insure themselves against these attacks by purchasing cyber insurance. However, the existence of such insurance may not eliminate the underlying problem, and instead may even

Table 8-2. Ransomware and Downtime Costs by Country, 2020

Country (1)	Total Submissions (2)	Minimum Cost ($, Nominal) (3)	Estimated Costs ($, Nominal) (4)
United States	15,672	5,123,606,318	20,494,425,272
France	4,476	1,452,222,393	5,808,889,571
Spain	4,088	1,332,008,900	5,328,035,599
Italy	3,835	1,255,260,122	5,021,040,489
Germany	3,747	1,214,481,832	4,857,927,329
Canada	3,236	1,058,505,964	4,234,023,855
United Kingdom	2,718	878,155,444	3,512,621,775
Australia	2,072	678,541,158	2,714,164,633
Austria	819	268,888,310	1,075,553,242
New Zealand	265	86,448,688	345,794,755
Total	40,928	13,348,119,130	53,392,476,519

Source: Emsisoft Malware Lab.

create an incentive for hackers to attack insured firms and get paid by insurance. In fact, in an interview with *The Record*, a member of the Russian hacking group REvil was explicitly asked if they targeted organizations that have cyber insurance. The member responded: “Yes, this is one of the tastiest morsels. Especially to hack the insurers first—to get their customer base and work in a targeted way from there. And after you go through the list, then hit the insurer themselves” (Smilyanets 2021).

One can observe evidence consistent with this vicious cycle from cyber insurance prices. The insurance brokerage Howden compiles a “Global Cyber Insurance Pricing Index,” which broadly measures premiums for cyber insurance (Howden 2023). As shown in figure 8-5, the cost of cyber insurance has increased more than 300 percent since July 2014.

In addition to paying for ransom costs, companies affected by ransomware attacks typically are unable to maintain their business activity until they have made the payment. In its annual “State of Ransomware” report, the cybersecurity firm Emsisoft estimated the combined cost of ransom payments and business downtime to be $19.6 billion in the United States in 2020, and roughly $51 billion in total across the United States, France, Spain, Italy, Germany, Canada, the United Kingdom, Australia, Austria, and New Zealand (as shown in table 8-2) (Emsisoft Malware Lab 2021).

It is crucial to note that the costs described here are direct costs. The indirect costs are likely higher. Instead of engaging in productive activities where firms have comparative advantages, they must divert resources to activities and products that help fend off attackers, such as buying cyber insurance and adding more personnel for information technology security. Thus, both welfare and economy-wide production decrease by a multiple of the direct dollar costs of resources that firms are using to stop ransomware attacks.

Investing in the Nation's Digital Financial Infrastructure

The growth of crypto assets has revealed a demand for a faster and more inclusive financial system with a real-time payment system and circulating digital money. Some have hoped that crypto assets could act as a form of decentralized money, making the U.S. payment systems faster, cheaper, safe, and more inclusive. This vision has not been realized. That said, there are still other ways near-term progress can be made on at least some of these goals. As a regulator of and participant in the Nation's payment systems, the Federal Reserve has a historical role in maintaining these systems' integrity (Federal Reserve Board, n.d.). For example, in the past decentralized payment systems were costly, in part, because some banks did not pay the full amount of a check from other banks—so-called nonpar collection or nonpar banking (Federal Reserve Board 1988). In some cases, this was done by levying a fee on checks deposited from other banks. Shortly after the establishment of the Federal Reserve System, it started providing payment services to banks, and over time it helped eliminate nonpar banking (Federal Reserve Bank of Minneapolis 1988).

This section first discusses an upcoming improvement to U.S. payments, which will help many consumers and businesses make cheap, instant payments. It then discusses the possibility of introducing a central bank digital currency (CBDC), which is a digital form of money. While operating under the supervision of a trusted authority, both these mechanisms have the potential to realize many of the benefits that crypto asset developers have promised.

The FedNow Instant Payment System

In terms of overall value as of 2020, the largest retail payment system in the United States was the Automated Clearinghouse (ACH) (Federal Reserve Board 2022a). ACH provides an electronic means to exchange funds between banks and other depository institutions (Federal Reserve Bank of San Francisco, n.d.). Typical ACH payments include salaries, consumer and corporate bills, interest payments, dividends, and Social Security payments. Peer-to-peer payment platforms such as Venmo complete transfers that are in and out of their platforms by accessing ACH network services through a participant bank (Venmo, n.d.). The regional Federal Reserve banks and the Electronic Payment Network are the country's two national ACH operators (Federal Reserve Board 2020). The prevalence of ACH offers many benefits; but a larger, more fast-paced economy is starting to arise. ACH payments can be processed in same-day batches between banks, throughout the day, but a standard ACH transfer can take up to three business days for funds to be settled and available to end users. In addition, ACH settlements occur only on business days (Nacha 2021). Businesses and individuals alike are increasingly in need of faster payment systems.

Advances in technology have created an opportunity for significant improvements in the way individuals and businesses make payments in today's economy. In recent years, members of Congress, staff members of the Department of the Treasury, and other experts have called for the Federal Reserve to offer a faster payment system for both businesses and retail users (Warren 2019; Mnuchin and Phillips 2018; Klein 2019). As a result of the COVID-19 pandemic and increased consumer demand for e-commerce options, many businesses have also increased their efforts to offer quicker payment options (Rathjen 2022).

In response, the Federal Reserve has prioritized designing and developing a faster payment system (Federal Register 2019).[5] The Federal Reserve plans to launch this new system, which is called the FedNow Service, later in 2023 (Federal Reserve Board 2022b). Through financial institutions participating in FedNow, businesses and individuals will be able to send and receive payments conveniently, and recipients will have nearly instant access to funds, giving them greater flexibility to manage their money and make time-sensitive payments. This service will be operational 24 hours a day and 7 days a week. This uninterrupted processing of fund transfers is an important improvement over existing payment systems (Federal Reserve Board 2022b, 2022c, 2022d). This service is different from peer-to-peer services such as Venmo in many ways. For example, funds transferred via FedNow will be available more quickly than those that must first exit a peer-to-peer payment service and then enter the ACH bank transfer process, which can take time to settle.

Beyond speed and convenience, near instant payments can yield real economic benefits for both individuals and businesses by allowing them to make time-sensitive payments whenever needed and providing them with more flexibility in managing their money. In particular, near instant payments under FedNow could bring significant benefits to vulnerable segments of the population. Slow payment systems can cost Americans billions of dollars. In addition to incurring bank overdraft fees, consumers can be forced to use high-cost alternatives like check cashers and payday lenders (Klein 2019). In 2019, it was estimated that a fast payment system such as FedNow could reduce these kinds of fees, generating savings of more than $7 billion a year for American households (Klein 2019). Because lower-income individuals are more likely to be hurt by slow payment systems,

[5] Note that there is a private faster payment system, RTP, whose adoption has been low (Clearing House 2022).

they could especially gain from these savings if FedNow is adopted widely. Using innovation productively and responsibly in this way could make banking services more inclusive.

FedNow requires commitment and active engagement by the private sector to make it interoperable, which means connecting and communicating with other payment services (Federal Reserve Board 2022c). According to the Federal Reserve, interoperability is crucial for "payment messages [to be] routed or exchanged and settled such that the sender may initiate a payment that will seamlessly reach the receiver. With interoperability, an individual or business with a bank account would be able to send a payment to another individual or business without having to choose, understand, or even be aware of the path taken by the payment." While noting that interoperability can take different forms, the Federal Reserve has maintained that it alone cannot fully establish the interoperability of FedNow; achieving this will require active partnership and collaboration with the financial industry (Federal Reserve Board 2022c).

Some have suggested that near instant digital payment systems like FedNow may reduce the need for circulating digital money (NAFCU 2022). In this case, the benefits of circulating digital money after FedNow is launched may be minimal. In fact, Federal Reserve governor Michelle Bowman commented in August 2022 that "my expectation is that FedNow addresses the issues that some have raised about the need for a CBDC" (Bowman 2022). Conversely, FedNow is intended to mainly focus on domestic payments and may bring limited improvements to the cross-border payment system, at least initially. In addition, FedNow is not a digital asset, which can be used in settlements or provide transaction programmability, roles that circulating digital money could play in the globally integrated financial system.

Central Bank Digital Currencies

It is important to note that money can come both in a physical format (e.g., cash) and in a digital format (e.g., electronic bank accounts). Thus, a central bank's digital currency is a liability of a central bank similar to cash, but it exists on a digital platform, where it can be exchanged and settled in real time. A CBDC system is made up of the CBDC itself, the public and private sector components that work alongside the CBDC, and the laws and regulations that apply to these digital assets (White House 2022a). A CBDC system can be set up in numerous different ways, such as a wholesale CBDC, which allows for access only by financial institutions (e.g., banks); and a retail CBDC, which allows for access by individuals. "That said, certain design features and questions related to the underlying infrastructure of CBDC may blur these distinctions to some degree" (U.S. Department of the Treasury 2022e).

As of January 5, 2023, 11 countries have launched CBDCs (Atlantic Council 2022). In addition, a number of foreign central banks, including the European Central Bank and the Bank of Japan, are exploring CBDCs; and some central banks, such as the People's Bank of China, are piloting a retail CBDC (Gorton and Zhang 2022). While some countries have considered using DLT for their CBDC, it is worth noting that many of the pilot programs for CBDC systems are not built on DLT; instead, they rely on a trusted central authority—a country's central bank—to operate key aspects of the CBDC system. This seems likely to be the case if a U.S. CBDC is introduced. A White House assessment of a potential U.S. CBDC system recently noted that "while a U.S. CBDC system could, in theory, be mostly 'permissionless' from a governance standpoint, this design choice introduces a large number of technical complexities and practical limitations that strongly suggest a permissionless approach does not make sense for a system that has at least one trusted entity (i.e., the central bank)" (White House 2022a). This is somewhat ironic, given that this is different from an oft-cited founding principle of crypto assets like Bitcoin, whose purported aim was to create decentralized money without any trusted central authority.

A U.S. CBDC—a digital form of the U.S. dollar—would have the potential to offer significant benefits. It could enable a payment system that is more efficient, provide a foundation for further technological innovation, facilitate faster cross-border transactions, and be environmentally sustainable (White House 2022a). It could also promote financial inclusion and equity by enabling access for a broad range of consumers (Maniff 2020). A potential U.S. CBDC could also help support other policy goals. For example, a potential U.S. CBDC could help ensure that such payment systems are aligned with the principles of human rights, democratic values, and privacy (U.S. Department of the Treasury 2022e).

There are also some risks from having a CBDC in the financial system. Similar to one-to-one backed stablecoins, CBDCs may also pose credit availability risks (U.S. Department of the Treasury 2022b). That is, a widely available CBDC could serve as a substitute for commercial bank deposits. Just as in the case of stablecoins that are fully backed by safe assets, this substitution effect could reduce the aggregate amount of deposits in the banking system, which could in turn increase bank funding expenses, and thus could reduce credit availability or raise credit costs for households and businesses. In addition, because central bank money is the safest form of money, a widely accessible CBDC would be particularly attractive to risk-averse users (and likely more so than a stablecoin), especially during times of stress in the financial system. The ability to quickly convert bank deposits into a CBDC could make systemic bank runs more likely or more severe

(Bank of Canada et al. 2021). In addition, CBDCs could cause operational risks. If the CBDC platform could not function due to a system failure or a cyberattack, it could erode investors' confidence.

Recognizing the potential benefits and risks from a U.S. CBDC, the Biden-Harris Administration has developed "Policy Objectives for a U.S. CBDC System," which reflect the Federal Government's priorities for a potential U.S. CBDC (White House 2022e). These objectives flesh out the goals outlined for a CBDC in the Executive Order. According to these objectives, the "U.S. CBDC system, if implemented, should protect consumers, promote economic growth, improve payment systems, provide interoperability with other platforms, advance financial inclusion, protect national security, respect human rights, and align with democratic values."

Conclusion

Innovation in financial services brings both risks and opportunities for the broader economy. It can challenge business models and existing industries, but it cannot challenge basic economic principles, such as what makes an asset effective as money and the incentives that give rise to run risk. Although the underlying technologies are a clever solution for the problem of how to execute transactions without a trusted authority, crypto assets currently do not offer widespread economic benefits. They are largely speculative investment vehicles and are not an effective alternative to fiat currency. Also, they are too risky at present to function as payment instruments or to expand financial inclusion. Even so, it is possible that their underlying technology may still find productive uses in the future as companies and governments continue to experiment with DLT. In the meantime, some crypto assets appear to be here to stay, and they continue to cause risks for financial markets, investors, and consumers. Much of the activity in the crypto asset space is covered by existing regulations and regulators are expanding their capabilities to bring a large number of new entities under compliance (SEC 2022). Other parts of the crypto asset space require coordination by various agencies and deliberations about how to address the risks they pose (U.S. Department of the Treasury 2022a).

Certain innovations, such as FedNow and a potential U.S. CBDC, could help bring the U.S. financial infrastructure into the digital era in a clear and simple way, without the risks or irrational exuberance brought by crypto assets. Hence, continued investments in the Nation's financial infrastructure have the potential to offer significant benefits to consumers and businesses, but regulators must apply the lessons that civilization has learned, and thus rely on economic principles, in regulating crypto assets.