The Blockchain Revolution: Decoding Digital Currencies

David Andolfatto and Fernando M. Martin

Cryptocurrencies and decentralized finance have grown considerably since the publication of the white paper on bitcoin in 2009. This article presents an overview of cryptocurrencies, blockchain technology, and their applications, explaining the spirit of the enterprise and how it compares with traditional operations. We discuss money, digital money, and payments; cryptocurrencies, blockchain, and the double-spending problem of digital money; decentralized finance; and central bank digital currency. (JEL E42, E44, E58, G21, G23, G28, G34)

Federal Reserve Bank of St. Louis *Review*, Third Quarter 2022, *104*(3), pp. 149-65.
https://doi.org/10.20955/r.104.149-65

INTRODUCTION

Few people took notice of an obscure white paper published in 2009 titled "Bitcoin: A Peer-to-Peer Electronic Cash System," authored by a pseudonymous Satoshi Nakamoto. The lack of fanfare at the time is hardly surprising given that innovations in the way we make payments are not known to generate tremendous amounts of excitement, let alone inspire visions of a revolution in finance and corporate governance. But just over a decade later, the enthusiasm for cryptocurrencies and decentralized finance spawned by Bitcoin and blockchain technology has grown immensely and shows no signs of abating.

Because cryptocurrencies are money and payments systems, they have naturally drawn the interest of central banks and regulators. The Federal Reserve Bank of St. Louis was the first central banking organization to sponsor a public lecture series on the topic: In March 2014, presenters outlined the big picture of cryptocurrencies and the blockchain by discussing its possibilities and pitfalls.[1] Since that time, the Bank's economists and research associates have published numerous articles and explainers on these topics.[2] This article represents a continuation of this effort to help educate the public and offer our perspective on the phenomenon as central bankers and economists.[3]

David Andolfatto is a senior vice president and economist and Fernando M. Martin is an assistant vice president and economist at the Federal Reserve Bank of St Louis. This article is derived from their essay published in the 2021 annual report of the Federal Reserve Bank of St Louis: https://www.stlouisfed.org/annual-report/2021/essay.

Understanding how cryptocurrencies work "under the hood" is a challenge for most people because the protocols are written in computer code and the data are managed in an esoteric mathematical structure. To be fair, it's difficult to understand *any* technical language (e.g., legalese, legislation, and regulation). Because we are not technical experts in this space, we spend virtually no time discussing the technology in detail.[4] What we offer instead is an overview of cryptocurrencies and blockchain technologies, explaining the spirit of the endeavor and how it compares with traditional operations.

In this article, we explore four key areas:

1. Money, digital money, and payments
2. Cryptocurrencies, blockchain, and the double-spend problem of digital money
3. Understanding decentralized finance
4. The makeup of a central bank digital currency

MONEY, DIGITAL MONEY, AND PAYMENTS

It is sometimes said that money is a form of social credit. One can think of this idea in the following way: When people go to work, they are in effect providing services to the community. They are helping to make others' lives better in some way and, by engaging in this collective effort, make their own lives better as well.

In small communities, individual consumption and production decisions can be debited and credited, respectively, in a sort of communal ledger of action histories. This is because it is relatively easy for everyone to monitor and record individual actions. A person who has produced mightily for the group builds social credit. Large social credit balances can be "spent" later as consumption (favors drawn from other members of the community).

In large communities, individual consumption and production decisions are difficult to monitor. In communities the size of cities, for example, most people are strangers. Social credit based on a communal record-keeping system does not work when people are anonymous.[5] Producers are rewarded for their efforts by accumulating money balances in wallets or bank accounts. Accumulated money balances can then be spent to acquire goods and services (or assets) from other members of the community, whose wallets and bank accounts are duly credited in recognition of their contributions. In this manner, money—like social credit—serves to facilitate the exchange of goods and services.

The monetary object representing this social credit may exist in physical or nonphysical form. In the United States, physical cash takes the form of small-denomination Federal Reserve bills and U.S. Treasury coins. Cash payments are made on a peer-to-peer (P2P) basis, for example, between customer and merchant. No intermediary is required for clearing and settling cash payments. As the customer debits his or her wallet, cash is credited to the merchant's cash register, and the exchange is settled. Hardly any time is spent inspecting goods and money in small-value transactions. Some trust is required, of course, in the authority issuing the cash used in transactions. While that authority is typically the U.S. government, there is no law preventing households and businesses from accepting, say, foreign currency, gold, or any other object as payment.

When people hear the word "money," they often think of cash. But, in fact, most of the U.S. money supply consists of digital dollars held in bank accounts. The digital money supply is created

as a byproduct of commercial bank lending operations and central bank open market operations. Digital money is converted into physical form when depositors choose to withdraw cash from their bank accounts. Most people hold both forms of money. The reasons for preferring one medium of exchange over the other are varied and familiar.

Digital dollar deposits in the banking system are widely accessible by households and businesses. This digital money flows in and out of bank accounts in the form of credits and debits whenever a party initiates a purchase. Unlike with cash, making payments with digital money has traditionally required the services of a trusted intermediary. A digital money payment is initiated when a customer sends an encrypted message instructing his or her bank to debit the customer's account and credit the merchant's account with an agreed-upon sum. This debit-credit operation is straightforward to execute when both customer and merchant share the same bank. The operation is a little more complicated when the customer and merchant do not share the same bank. In either case, clearing and settling payments boils down to an exercise in secure messaging and honest bookkeeping.

CRYPTOCURRENCIES, BLOCKCHAIN, AND THE DOUBLE-SPEND PROBLEM OF DIGITAL MONEY

One can think of cryptocurrencies as digital information transfer mechanisms. If the information being transferred is used as an everyday payment instrument, it fulfills the role of money. In this case, a cryptocurrency can be thought of as a money and payments system.

Every money and payments system relies on trust. The difference between cryptocurrencies and conventional money and payments systems lies in where this trust is located. In contrast to conventional systems, no delegated legal authority is responsible for managing and processing cryptocurrency information. Instead, the task is decentralized and left open to "volunteers" drawn from the community of users, similar in spirit to how the internet-based encyclopedia Wikipedia is managed. These volunteers—called miners—work to update and maintain a digital ledger called the blockchain. The protocols that govern the read-write privileges associated with the blockchain are enshrined in computer code. Users trust that these rules are not subject to arbitrary changes and that rule changes (if any) will not benefit some individuals at the expense of the broader community. Overall, users must trust the mathematical structure embedded in the database and the computer code that governs its maintenance.

Managing a digital ledger without a delegated accounts manager is not a trivial problem to solve. If just anyone could add entries to a public ledger, the result likely would be chaos. Malevolent actors would be able to debit an account and credit their own at will. Or they could create social credit out of thin air, without having earned it. In the context of money and payments systems, these issues are related to the so-called double-spend problem.

To illustrate the double-spend problem, consider the example of a dollar stored in a personal computer as a digital file. It is easy for a customer to transfer this digital file to a merchant on a P2P basis, say, by email. The merchant is now in possession of a digital dollar. But how can we be sure that the customer did not make a copy of the digital file before spending it? It is, in fact, a simple matter to make multiple copies of a digital file. The same digital file can then be spent twice (hence, a double-spend). The ability to make personal copies of digital money files would effectively grant each person in society his or her own money printing press. A monetary system with this property is not likely to function well.

Physical currency is not immune from the double-spend problem, but paper bills and coins can be designed in a manner to make counterfeiting sufficiently expensive. Because cash is difficult to counterfeit, it can be used more or less worry-free to facilitate P2P payments. The same is not true of digital currency, however. The conventional solution to the double-spend problem for digital money is to delegate a trusted third party (e.g., a bank) to help intermediate the transfer of value across accounts in a ledger. Bitcoin was the first money and payments system to solve the double-spend problem for digital money without the aid of a trusted intermediary. How?

The Digital Village: Communal Record-Keeping

The cryptocurrency model of communal record-keeping resembles the manner in which history has been recorded in small communities, including in networks of family and friends. It is said that there are no secrets in a small village. Each member of the community has a history of behavior, and this history is more or less known by all members of the community—either by direct observation or through communications. The history of a small community can be thought of as a virtual database living in a shared (or distributed) ledger of interconnected brains. No one person is delegated the responsibility of maintaining this database—it is a shared responsibility.

Among other things, such a database contains the contributions that individuals have made to the community. As we described above, the record of these contributions serves as a reputational history on which individuals can draw; the credit they receive from the community can be considered a form of money. There is a clear incentive to fabricate individual histories for personal gain—the ability to do so would come at the expense of the broader community in the same way counterfeiting money would. But open, shared ledgers are very difficult to alter without communal consensus. This is the basic idea behind decentralized finance, or DeFi.

Governance via Computer Code

All social interaction is subject to rules that govern behavior. Behavior in small communities is governed largely by unwritten rules or social norms. In larger communities, rules often take the form of explicit laws and regulations. At the center of the U.S. money and payments system is the Federal Reserve, which was created in 1913 through an act of Congress. The Federal Reserve Act of 1913 specifies the central bank's mandates and policy tools. There is also a large body of legislation that governs the behavior of U.S. depository institutions. While these laws and regulations create considerable institutional inertia in money and payments, the system is not impervious to change. When there is sufficient political support—feedback from the American people—changes to the Federal Reserve Act can be made. The Humphrey-Hawkins Act of 1978, for example, provided the Fed with three mandates: stable prices, maximum employment, and moderate long-term interest rates (Steelman, 1978). And the Dodd-Frank Act of 2010 imposed stricter regulations on financial firms following the financial crisis in 2007-09 (Goodwin, 2010).

Because cryptocurrencies are money and payments systems, they too must be subject to a set of rules. In 2009, Satoshi Nakamoto brought forth his aforementioned white paper, which laid out the blueprint for Bitcoin. This blueprint was then operationalized by a set of core developers in the form of an open-source computer program governing monetary policy and payment processing protocols. Adding, removing, or modifying these "laws" governing the Bitcoin money and payments system is virtually impossible.[6] Concerted attempts to change the protocol either fail or result in

breakaway communities called "forks" that share a common history with Bitcoin but otherwise go their separate ways. Proponents of Bitcoin laud its regulatory system for its clarity and imperviousness, especially relative to conventional governance systems in which rules are sometimes vague and subject to manipulation.

How Blockchain Technology Works

As with any database management system, the centerpiece of operations is the data itself. For cryptocurrencies, this database is called the blockchain. One can loosely think of the blockchain as a ledger of money accounts, in which each account is associated with a unique address. These money accounts are like post office boxes with windows that permit anyone visiting the post office to view the money balances contained in every account.[7] These windows are perfectly secured.[8] While anyone can look in, no one can access the money without the correct password. This password is created automatically when the account is opened and known only by the person who created the account (unless it is voluntarily or accidentally disclosed to others). The person's account name is pseudonymous (unless voluntarily disclosed). These latter two properties imply that cryptocurrencies (and cryptoassets more generally) are digital bearer instruments. That is, ownership control is defined by possession (in this case, of the private password). It is worth noting that large-denomination bearer instruments are now virtually extinct. Today, bearer instruments exist primarily in the form of small-denomination bills and metal coins issued by governments. For this reason, cryptocurrencies are sometimes referred to as "digital cash."

As with physical cash, no permission is needed to acquire and spend cryptoassets. Nor is it required to disclose any personal information when opening an account. Anyone with access to the internet can download a cryptocurrency wallet—software that is used to communicate with the system's miners (the aforementioned volunteer accountants). The wallet software simultaneously generates a public address (the "location" of an account) and a private key (password). Once this is done, the front-end experience for consumers to initiate payment requests and manage money balances is very similar to online banking as it exists today. Of course, if a private key is lost or stolen, there is no customer service department to call and no way to recover one's money.

Cryptocurrencies have become provocative and somewhat glamorous, but their unique and key innovation is *how* the database works. The management of money accounts is determined by a set of regulations (computer code) that determines who is permitted to write to the database. The protocols also specify how those who expend effort to write to the database—essentially, account managers—are to be rewarded for their efforts. Two of the most common protocols associated with this process are called proof-of-work (PoW) and proof-of-state (PoS). The technical explanation is beyond the scope of this article. Suffice it to say that *some form* of gatekeeping is necessary—even if the effort is communal—to prevent garbage from being written to the database. The relevant economic question is whether these protocols, whatever they are, can process payments and manage money accounts more securely, efficiently, and cheaply than conventional centralized finance systems.

Native Token

Recording money balances requires a monetary unit. This unit is sometimes referred to as the native token. From an economic perspective, a cryptocurrency's native token looks like a foreign currency, albeit one whose monetary policy is governed by a computer algorithm rather than the

Figure 1

Bitcoin in U.S. Dollars

NOTE: Gray shaded area indicates U.S. recession.

SOURCE: Coinbase via FRED®, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/graph/?g=R9Gx, accessed July 8, 2022.

Figure 2

Ethereum in U.S. Dollars

NOTE: Gray shaded area indicates U.S. recession.

SOURCE: Coinbase via FRED®, Federal Reserve Bank of St. Louis; https://fred.stlouisfed.org/graph/?g=R9Gs, accessed July 8, 2022.

policymakers of that country. Much of the excitement associated with cryptocurrencies seems to stem from the prospect of making money through capital gains via currency appreciation relative to the U.S. dollar (USD). (To see how the prices of bitcoin and ethereum, another cryptocurrency, have changed since 2017, see the FRED® graphs in this article: Figures 1 and 2.) It seems to have less to do with the promise of the underlying record-keeping technology stressed by Nakamoto's white paper. To be sure, the price of a financial security can be related to its underlying fundamentals. It is not, however, entirely clear what these fundamentals are for cryptocurrency or how they might generate continued capital gains for investors beyond the initial rapid adoption phase. Moreover, while the supply of a given cryptocurrency such as Bitcoin may be capped, the supply of close substitutes (from the perspective of investors, not users) is potentially infinite. Thus, while the total market capitalization of cryptocurrencies may continue to grow, this growth may come more from newly created cryptocurrencies and not from growth in the per-unit price of any given cryptocurrency, such as Bitcoin.[9]

In any case, conceptually, there is a distinction to be made between the promise of a cryptocurrency's underlying technology and the market price of its native token. Bitcoin (BTC) as a payments system could, in principle, function just as well at any given BTC/USD exchange rate.

Cryptocurrency Applications

Cryptocurrencies designed to serve as money and payments systems have continued to struggle in their quest for adoption as an everyday medium of exchange. Their main benefit to this point—at least for early adopters—has been as a long-term store of value. But their exchange rate volatility makes them highly unsuitable as domestic payment instruments, given that prices and debt contracts are denominated in units of domestic currency. While year-over-year returns can be extraordinary, it is not uncommon for a cryptocurrency to lose most of its value over a relatively short period of time. How a cryptocurrency might perform as a domestic payments system when it is also the unit of account remains to be seen. El Salvador recently adopted bitcoin as its legal tender, and people will be watching this experiment closely.[10]

A use case touted early in Bitcoin history was its potential to serve as a vehicle currency for international remittances. One of the attractive attributes of Bitcoin is that anyone with access to the internet can access the Bitcoin payments system freely and without permission. For example, a Salvadoran working in the United States can convert his or her USD into BTC at an online exchange and send BTC to a relative in El Salvador in minutes for (usually) a relatively low fee, compared with sending money through conventional channels.

As with any tool, bitcoin may be used for good or ill purposes. Because BTC is a permissionless bearer instrument (like physical cash), it may become a popular way to finance illegal activities, terrorist organizations, and money laundering operations. Recently, it has been used in ransomware attacks, in which nefarious agents blackmail hapless victims and demand payment in bitcoin, thereby bypassing the banking system.

But possibly the most attractive characteristic of Bitcoin is that it operates independently of any government or concentration of power. Bitcoin is a decentralized autonomous organization (DAO). Its laws and regulations exist as open-source computer code living on potentially millions of computers. The blockchain is beyond the (direct) reach of government interference or regulation. There is no physical location for Bitcoin. It is not a registered business. There is no CEO. Bitcoin

has no (conventional) employees. The protocol produces a digital asset, the supply of which is, by design, capped at 21 million BTC. Participation is voluntary and permissionless. Large-value payments can be made across accounts quickly and cheaply. It is not too difficult to imagine how these properties can be attractive to many people.

Policy Considerations of Cryptocurrency

To a central bank, a cryptocurrency looks very much like a foreign currency. From this perspective, there is nothing revolutionary here. Foreign currency is sometimes seen as a threat by governments. This is not the case for the United States, since the U.S. dollar remains the world's reserve currency, but many other countries often take measures to discourage the domestic use of foreign currency. Citizens may be prohibited, for example, from holding foreign currency or opening accounts in foreign banks. Because cryptocurrencies are freely available and permissionless, it would likely be considerably more difficult to enforce cryptocurrency controls. The cryptocurrency option may also serve to constrain domestic monetary and fiscal policies—in particular, by imposing a more stringent limit on the amount of seigniorage (i.e., the "printing" of more money to finance government spending).

A dominant foreign currency may cause another problem: As it turns out, it is often cheaper to issue debt denominated in a dominant foreign currency. The problem with this activity is that when the domestic currency depreciates, debtors may have trouble repaying, and a financial crisis may ensue. When that dominant foreign currency is the U.S. dollar, the central bank of a foreign country can sometimes find relief by borrowing dollars from the Federal Reserve through a currency-swap line. But if debt instruments are denominated in cryptocurrency, there is no negotiating with the DAO of that cryptocurrency. Because this is the case, domestic regulators might want to regulate the practice of issuing cryptocurrency-denominated debt more stringently if the practice ever became sufficiently widespread to pose significant systemic risk.

UNDERSTANDING DECENTRALIZED FINANCE

Decentralized finance broadly refers to financial activities that are based on a blockchain. Unlike conventional or traditional finance that relies on intermediaries and centralized institutions, DeFi relies on so-called smart contracts. The removal of those intermediaries in transactions between untrusted parties would significantly reduce costs and grant the parties more control over the terms of such agreements. Still, intermediaries oftentimes play meaningful roles beyond verification and enforcement, which means they would not altogether disappear. Here, we examine some of these concepts to explain what DeFi means and implies.[11]

What Are Smart Contracts?

A smart contract is a computer program designed to execute an agreed-upon set of actions. The concept was first introduced in the mid-1990s by Nick Szabo, who proposed vending machines as a primitive example: A vending machine is a mechanism that dispenses a product in exchange for a listed amount of coins (or bills); anyone with a sufficient amount of money can participate in this exchange.[12] Smart contracts allow interested parties to engage in secure financial transactions without the participation of third parties. As we explain below, their application goes beyond conventional financial transactions.

Ethereum is a blockchain with smart contract capability that was released in 2015. In this case, smart contracts are a type of account, with their own balance and the capability to interact with the network. Rather than being controlled by a user, smart contracts run as programmed, with their code and data residing at a specific address on the Ethereum blockchain. Other platforms may implement smart contracts in different ways.[13]

Like cryptocurrencies, smart contracts overcome security and transparency concerns in transactions between untrusted parties, without the need for a trusted third party. In fact, smart contracts aim to do away with intermediaries such as brokers, custodians, and clearinghouses.

Consider a collateralized loan as an example. In traditional finance, a borrower seeks a bank to lend funds or a broker to find potential lenders. The parties then agree on the terms of the loan: interest rate, maturity, type and value of collateral, etc. The borrower's collateral is placed in escrow. If the borrower fulfills the terms of the contract, the collateral is released and full ownership rights are returned. If the borrower defaults, the collateral is used to fulfill the contract (e.g., repay the remaining principal, interest, and penalties). There are many parties involved in this transaction: financial intermediaries, appraisers, loan servicers, asset custodians, and others.

In a smart contract, the entire agreement is specified as part of the computer program and is stored on a blockchain. The program contains the terms of the loan, as well as the specific actions it will take based on compliance (e.g., the transfer of collateral ownership in the event of default). Since the blockchain handles the faithful execution of the contract, there is no need to involve any parties beyond the borrower and lender.

Asset Tokenization

The example above illustrates an important wrinkle: It may not be possible for all the elements and actions of a contract to be handled by the blockchain—particularly when it comes to collateral. If collateral is not available as an asset in the native protocol (i.e., the specific blockchain where the smart contracts exist), then, as in traditional finance, the contract necessitates a third party to provide escrow services. Naturally, this exposes the contract to counterparty risk. One solution to this problem is asset tokenization.

Asset tokenization consists of converting the ownership of an asset into digital tokens, each representing a portion of the property. If the asset exists in physical form (e.g., a house), then tokenization allows the asset to exist in a blockchain and be used for various purposes (e.g., as collateral). An important issue is how to enforce property rights stored in the blockchain for assets that exist in the physical world. This is an ongoing challenge for DeFi and one that may never be fully resolved.

Tokens also have a variety of nonfinancial applications. For example, they may grant owners voting rights to an organization. This allows for the decentralized control of institutions within a blockchain, as we describe below. Another popular application is the creation of nonfungible tokens (NFTs), which provide ownership of a digital image created and "signed" by an artist. Although the image could in principle be replicated countless times, there is only one version that is verifiably authentic. The NFT serves as a certificate of authenticity in the same way that artists' signatures ensure paintings are originals and not copies. The advantage of an NFT is the security provided by the blockchain—signatures can be forged, whereas the authenticity of the NFT is validated by a decentralized communal consensus algorithm.

Decentralized Autonomous Organizations

Smart contracts could transform the way we organize and control institutions. Applications may range from investment funds to corporations and perhaps even the provision of public goods and services.

A DAO (decentralized autonomous organization) is an organization represented by a computer code, with rules and transactions maintained on a blockchain. Therefore, DAOs are governed by smart contracts. A popular example is MakerDAO, the issuer of the stablecoin Dai, whose stakeholders use tokens to help govern decisions over protocol changes.

The concept of governance refers to the rules that balance the interests of different stakeholders of an institution. For example, a corporation's stakeholders may include shareholders, managers, creditors, customers, employees, the government, and the general public, among others. The board of directors typically plays the critical role in corporate governance. One of the main issues corporate governance is designed to mitigate is agency problems: when managers do not act in the best interest of shareholders. But governance extends beyond regulating internal matters and may, for example, manage the role of a corporation inside a community or relative to the environment.

DAOs may be created for ongoing projects, such as a DeFi entity, or for specific and limited purposes, such as public works. Because they offer an alternative governance model by encoding rules in a smart contract, they replace the traditional top-down structure with a decentralized consensus-based model. Two prominent examples—the decentralized exchange Uniswap and the borrowing and lending platform Aave—started out in the traditional way, by having their respective development teams in charge of day-to-day operations and development decisions. They eventually issued their own tokens, which distributed governance to the wider community. With varying details, holders of governance tokens may submit development proposals and vote on them.

Centralized and Decentralized Exchanges

Currently, the most popular way in which cryptoassets are traded is through a centralized exchange (CEX), which works like a traditional bank or a broker: A client opens an account by providing personal identifiable information and depositing funds. With an account, the client can trade cryptoassets at listed prices in the exchange. The client does not own these assets, however, as the exchange acts as a custodian. Hence, clients' trades are recorded on the exchange's database rather than on a blockchain. Binance and Coinbase are CEXs that offer accessibility to users. However, since they stand between users and blockchains, they need to overcome the same trust and security issues as traditional intermediaries.

Decentralized exchanges (DEXs), on the other hand, rely on smart contracts to enable trading among individuals on a P2P basis, without intermediaries. Traders using DEXs keep custody of their funds and interact directly with smart contracts on a blockchain.

One way to implement a DEX is to apply the methods from traditional finance and rely on order books. These order books consist of lists of buy and sell orders for a specific security that display the amounts being offered or bid on at each price point. CEXs also work in this way. The difference with DEXs is that the list and transactions are handled by smart contracts. Order books can be "on-chain" or "off-chain," depending on whether the entire operation is handled on the blockchain. In the case of off-chain order books, typically only the final transaction is settled on the blockchain.

Order-book DEXs may suffer from slow execution and a lack of liquidity. That is, buyers and sellers may not find adequate counterparties, and individual transactions may affect prices too much. DEX aggregators alleviate this problem by collecting the liquidity of various DEXs, which increases the depth of both sides of the market and minimizes slippage (i.e., the difference between the intended and executed price of an order).

An automated market maker (AMM) is another way to solve the liquidity problem in DEXs. Market makers are also derived from traditional finance, where they play a central role in ensuring adequate liquidity in securities markets. AMMs create liquidity pools by rewarding users who "deposit" assets in the smart contract, which then can be used for trades. When a trader proposes an exchange of two assets, the AMM provides an instant quote based on the relative availability (i.e., liquidity) of each asset. When the liquidity pools are sufficiently large, trades are easy to fulfill and slippage is minimized. AMMs are currently the dominant form of DEXs, because they resolve the liquidity problem better than alternative mechanisms and thus provide speedier and cheaper transactions.

What Are Stablecoins?

As we described earlier, cryptocurrencies are subject to extreme exchange rate volatility, which makes them highly unsuitable as payment instruments. A stablecoin is a cryptocurrency that ties its value to an asset outside of its control, such as the U.S. dollar.[14] To accomplish this, the stablecoin must effectively convince its liability holders that its liabilities can be redeemed on demand (or on short notice) for U.S. dollars at par (or at some other fixed exchange rate). The purpose of this structure is to render stablecoin liabilities more attractive as payment instruments. Pegging to the U.S. dollar is attractive to people living in the U.S. because the U.S. dollar is the unit of account. Those outside the U.S. may be attracted to the product because the U.S. dollar is the world's reserve currency. This structure serves to increase demand for the stablecoin. But why would someone want to make U.S. dollar payments using a stablecoin instead of a regular bank account?

The answer ultimately rests on which product offers its clients the services they desire at a price they find attractive. A stablecoin is likely to be attractive at the wholesale level, where firms would be able to make USD payments at each point in an international supply chain without the need for conventional banking arrangements. Stablecoins market themselves as leveraging blockchain technology to deliver safer and more efficient account management and payment processing services. These efficiency gains can then be passed along to customers in the form of lower fees. A more cynical view ascribes these purported lower costs to regulatory arbitrage (i.e., sidestepping certain costs by relocating the transaction outside of the regulatory environment), rather than technological improvements in database management.

Financial Stability Concerns

U.S. dollar-based stablecoins are similar to money market funds that peg the price of their liabilities to the U.S. dollar. They also look very much like banks *without deposit insurance*. As the financial crisis of 2007-09 showed, even money market funds are subject to runs when the quality of their assets is questioned. Unless a U.S. dollar-based stablecoin is backed fully by U.S. dollar reserves (it needs an account at the Federal Reserve for this) or by U.S. dollar bills (the maximum denomination is $100, so this seems unlikely), it is potentially prone to a bank run. If a stablecoin

cannot dispose of its assets at fair or normal prices, it may fail to raise the U.S. dollars it needs to meet its par redemption promise in the face of a wave of redemptions. In such an event, the stablecoin would turn out to be not so stable.

If the adverse consequences of a stablecoin run were limited to the owners of stablecoins, then standard consumer protection legislation would be sufficient. But regulators also are concerned about the possibility of systemic risk. Consider, for example, the commercial paper market, where firms regularly borrow money on a short-term basis to fund operating expenses. Then consider a stablecoin (or any money market fund) with large holdings of commercial paper. A stablecoin run in this case may compel a fire sale of commercial paper to raise the funds needed to meet the wave of redemptions. This fire sale would likely have adverse economic consequences for firms that make regular use of the commercial paper market: As commercial paper prices decline, the value of commercial paper as collateral falls, and firms may find it more difficult to borrow the funds they normally access with ease. If the fire sale spills over into other securities markets, credit conditions may tighten significantly and lead to the usual woes experienced in an economic recession (missed payments, worker layoffs, etc.). These events are sufficiently difficult for a central bank to handle when the entities involved are domestic money market funds. The problem is compounded if the stablecoin is an unregulated "offshore" DAO. Will offshore stablecoins that are "too big to fail" be able to take advantage of the implicit insurance provided by central bank lender-of-last-resort operations? If so, this would be an example of how the private benefits of DeFi arise from regulatory arbitrage and not from an inherent technological advantage. This possibility presents a significant challenge for national and international regulators.

On the other hand, it may be possible for stablecoins to be rendered "run-proof" by employing smart contracts to design more resilient financial structures. For example, real-time communal monitoring of balance sheet positions is a possibility—a feature that could shine light on what are traditionally opaque financial structures.[15] Furthermore, because redemption policies can potentially manifest themselves as computer code, their design can be made more elaborate (state-contingent) and credible (contractual terms that can be credibly executed and not reversed). These features can potentially render stablecoins run-proof in a manner that is not possible with conventional banking arrangements.

Regulators and Stablecoins

The regulatory concerns with stablecoins are similar to age-old concerns with the banking industry. Banks are in the business of creating money and do so by issuing deposit liabilities that promise a fixed (par) exchange rate against U.S. dollar bills and dollar credits held in Federal Reserve accounts. Lower-yielding liabilities are used to acquire higher-yielding assets. Because commercial banks normally hold only a very small fraction of their assets in the form of reserves, they are called fractional reserve banks. Since the introduction of federal deposit insurance, retail-level bank runs have been practically nonexistent. Banks also have access to the Federal Reserve's emergency lending facilities. These privileges are matched by a set of regulatory constraints on bank balance sheets (both assets and liabilities) and other business practices.

Some stablecoin issuers would undoubtedly like to base their business models on those of banks or prime institutional money market funds. The motivation is clear: Issuing low-cost liabilities to finance high-yielding assets can be a profitable business. (Until, of course, something goes wrong.

Then, regulators and policymakers face blame for permitting such structures to exist in the first place.) This business model naturally involves non-negligible risk and could make for a potentially unstable stablecoin. As stablecoins with these properties interact with off-chain financial activity, they introduce risks that may spill over to other markets and, therefore, prompt some form of regulation.

Other stablecoin issuers are likely to focus on delivering payment services, which can be accomplished by holding only safe assets. These stablecoins would be more akin to government money market funds. Stablecoins that submit to government regulations may be permitted to hold only the safest of securities (e.g., U.S. Treasury securities). If they could, they might even hold only interest-bearing reserves, thereby becoming "narrow banks." The business model in these cases would be based on generating profits through transaction-processing fees and/or net interest margins enhanced by what stablecoin users would hope to be a wafer-thin capital requirement.

THE MAKEUP OF A CENTRAL BANK DIGITAL CURRENCY

The Board of Governors of the Federal Reserve System (BOG), in its recent paper "Money and Payments: The U.S. Dollar in the Age of Digital Transformation," defines a central bank digital currency (CBDC) as a "digital liability of the Federal Reserve that is widely available to the general public" (BOG, 2022, p. 3). This essentially means allowing the general public to open personal bank accounts at the central bank. How might a CBDC work?

Today, only financial institutions defined as depository institutions by the Federal Reserve Act and a select number of other agencies (including the federal government) are permitted to have accounts at the Federal Reserve. These accounts are called reserve accounts. The money balances that depository institutions hold in their reserve accounts are called bank reserves. The money account held by the federal government at the Federal Reserve is called the Treasury General Account. In a sense, a CBDC already exists, but only at the wholesale level and only for a small group of agencies. The question is whether to make it more broadly accessible and, if so, how.

As explained above, the general public already has access to a digital currency in the form of digital deposit liabilities issued by depository institutions. Most households and businesses have checking accounts with private banks. The general public also has access to a central bank liability in the form of physical currency (cash). While banks are obligated to redeem their deposit liabilities for cash on demand, deposits are not legally central bank or government liabilities. To put it another way, CBDC is (or would presumably be made) legal tender, while bank deposits represent claims to legal tender.

Federal Deposit Insurance

Bank accounts in the United States are presently insured up to $250,000 by the Federal Deposit Insurance Corp. From a political-economic point of view, bank deposits at the retail level are a de facto government liability. Moreover, given the role of the Federal Reserve as lender of last resort, one could make a case that large-value bank deposits are also a de facto government liability. To the extent this is so, the legal status of CBDC versus bank money may not be important as far as the ultimate safety of money accounts is concerned.

The Question of Counterparty Risk

Safety is only one of the many concerns surrounding money and payments. There is also the question of how counterparty risk may affect access to funds. For example, even if money in a bank account is insured, access to those funds may be delayed if a bank is suddenly subject to financial stress. This type of risk may be one reason corporate cash managers often turn to the repo market, where deposits are typically collateralized with Treasury securities that can be readily liquidated in the event deposited cash is not returned on time. If there is no restriction on the size of CBDC accounts, the product would effectively provide fully insured money accounts for corporations with no counterparty risk. Such a product, if operated effectively, could very well disintermediate (i.e., eliminate) parts of the money market.

Potential for Efficiency Gains

There is also the question of how a CBDC might improve the overall efficiency of the payments system. This is a difficult question to answer. Proponents often compare a well-designed CBDC with the payments system as it exists today in the United States, which has not caught up to developments in other jurisdictions, including in many developing economies. The U.S. payments system, however, is evolving rapidly to a point that may make CBDC a less attractive proposition. For example, The Clearing House now offers a 24/7 real-time payment services platform.[16] The Federal Reserve's FedNow platform will provide a similar service (BOG, 2021).

There may be no single best way to organize a payments system. A payments system is all about processing payment requests and debiting/crediting money accounts. Conceptually, bookkeeping is very simple, even if the actual implementation and operation of a payments system are immensely challenging endeavors. Any arrangement would need mechanisms that guard against fraud. Messaging must be made fast and secure. Institutions (or DAOs) must be trusted to manage the ledgers containing money accounts and related information. Property rights over data ownership would need to be specified and enforced. Some have advocated strongly for a CBDC (e.g., Crawford, Menand, and Ricks, 2021). Others seem less enthusiastic (e.g., White, 2020; Selgin, 2021; and Waller, 2021). In principle, a private, public, or private-public arrangement could be made to work well.

Like most central banks, the Federal Reserve is designed to facilitate payments at the wholesale level. It performs a vital function and overall performs it well. Traditionally, servicing the needs of a large and demanding retail sector in the United States is left to the private sector. A CBDC could be designed to respect this division of labor in one of two ways:

1. Permit free entry into the business of "narrow banking." This would entail granting Fed master accounts to qualified firms with the requirement that they hold only reserves (and possibly U.S. Treasury bills) as assets. In this arrangement, digital currency remains a private liability (though fully backed by reserves).
2. Grant households and firms direct access to CBDC and delegate the responsibility of processing payments at the retail level to private firms. This latter arrangement is the one described in the aforementioned BOG (2022) report on CBDC.

CONCLUSION

The ability to write history is a tremendous power. Who should be entrusted with such power? And how should privileges be restricted to ensure honesty, accuracy, and (where needed) privacy?

All sorts of individual and group histories play an important role in coordinating economic activity, including credit histories, work histories, performance histories, educational attainment histories, and regulatory compliance histories. In this article, we have focused primarily on payment histories in the context of cryptocurrency—including the fact that histories can be fabricated and that individuals and organizations may be tempted to misrepresent their own histories for private gain at the expense of the broader community. Even relatively well-functioning societies must devote considerable resources to reconciling conflicting claims of past behavior, given the absence of reliable databases that contain those histories.[17]

Much of our everyday economic activity occurs outside any formal record-keeping, and societies have relied on *informal* communal record-keeping to incentivize individual and organizational behavior. Paper and electronic receipts issued for most commercial exchanges are more formal but are often incomplete and easily fabricated. More important records—for physical property, bank accounts, financial assets, licenses, certificates of education, etc.—are managed by trusted authorities.

These traditional forms of record-keeping are likely to be challenged by blockchain technology, which provides a very different model of information management and communication. Competitive pressures compel organizations and institutional arrangements to evolve in response to technological advances in data storage and communications. Consider, for example, how the telegraph, telephone, computer, and internet have transformed the way people interact and organize themselves. Advances in blockchain technology are likely to generate even more dramatic changes, though what these may be remains highly uncertain. ■

NOTES

[1] See Federal Reserve Bank of St. Louis (2014) for a video and presentation from the event.

[2] See, for example, the Federal Reserve Bank of St. Louis "Cryptocurrencies and Fintech" theme page: https://research.stlouisfed.org/publications/cryptocurrencies-and-fintech/.

[3] See also Andolfatto (2018), "Block, Cryptocurrencies and Central Bank," the keynote presentation from a later St. Louis Fed lecture series.

[4] For an accessible introduction to the technology, see Schär and Berentsen (2020).

[5] See Kocherlakota (1998).

[6] Relatively minor patches to the code to fix bugs or otherwise improve performance have been implemented. But certain key parameters, like the one that governs the cap on the supply of bitcoin, are likely impervious to change.

[7] Beyond viewing the balances, one can also view the transaction histories of every monetary unit in the account (i.e., its movement from account to account over time since it was created).

[8] It is important to note that many cryptocurrency users hold their funds via third parties to whom they relinquish control of their private keys. If an intermediary is hacked and burgled, one's cryptocurrency holdings may be stolen. This has nothing to do with security flaws in the cryptocurrency itself—but with the security flaws of the intermediary.

[9] Andolfatto and Spewak (2019).

[10] Legal tender is an object that creditors cannot legally refuse as payment for debt. While deposits are claims to legal tender (they can be converted into cash on demand), they also constitute claims against all bank assets in the event of bankruptcy.

[11] For a more extensive review, see Schär (2021); also see an analysis by Feenan et al. (2021).

[12] See Szabo (1994 and 1997). The key idea is that contractual terms, once agreed upon, are not renegotiable and are therefore automatically executed in the future. In economic theory, so-called Arrow-Debreu securities have the same property.

[13] For example, Hyperledger allows for confidential transactions, whereas Ethereum, a public network, does not. Bitcoin is also able to handle a variety of smart contracts.

[14] Some stablecoins stabilize their value by pegging to the U.S. dollar, backed with non-U.S. dollar assets; Dai, for example, pegs its value to a senior tranche of other cryptoassets. See Feist (2021).

[15] The opacity of financial structures is not necessary to explain bank runs. For example, the canonical model of bank runs assumes the existence of transparent balance sheets. See Diamond and Dybvig (1983).

[16] See https://www.theclearinghouse.org/payment-systems/rtp.

[17] The U.S. Chamber of Commerce Institute for Legal Reform (2018) found the cost of litigation in the United States amounted to $429 billion, or 2.3 percent of U.S. gross domestic product, in 2016. Over 40 percent of this cost was used to pay legal, insurance, and administrative costs. These costs constitute a lower bound, as most disputes are reconciled outside the legal system.

REFERENCES

Andolfatto, David. "Blockchain, Cryptocurrencies and Central Banks." Keynote presentation at the Federal Reserve Bank of St. Louis Dialog with the Fed (lecture series), August 28, 2018; https://www.stlouisfed.org/dialogue-with-the-fed/blockchain.

Andolfatto, David and Martin, Fernando M. *2022 Annual Report: The Blockchain Revolution: Decoding Digital Currencies*. Federal Reserve Bank of St. Louis, 2021; https://www.stlouisfed.org/annual-report/2021/essay.

Andolfatto, David and Spewak, Andrew. "Whither the Price of Bitcoin?" Federal Reserve Bank of St. Louis, *Economic Synopses*, 2019, No. 1; https://doi.org/10.20955/es.2019.1.

Board of Governors of the Federal Reserve System. "FedNOW[SM] Service." Last update: April 28, 2021; https://www.federalreserve.gov/paymentsystems/fednow_about.htm.

Board of Governors of the Federal Reserve System. "Money and Payments: The U.S. Dollar in the Age of Digital Transformation." January 2022; https://www.federalreserve.gov/publications/files/money-and-payments-20220120.pdf.

Crawford, John; Menand, Lev and Ricks, Morgan. "FedAccounts: Digital Dollars." *George Washington Law Review*, January 2021, *89*(1), pp. 113-172; https://scholarship.law.columbia.edu/faculty_scholarship/3118/.

Diamond, Douglas and Dybvig, Philip. "Bank Runs, Deposit Insurance, and Liquidity." *Journal of Political Economy*, June 1983, *91*(3), pp. 401-19; http://links.jstor.org/sici?sici=0022-3808%28198306%2991%3A3%3C401%3ABRDIAL%3E2.0.CO%3B2-Z.

Federal Reserve Bank of St. Louis. "Bitcoin and Beyond: The Possibilities and the Pitfalls of Virtual Currencies." Dialog with the Fed (lecture series), March 30, 2014; https://www.stlouisfed.org/dialogue-with-the-fed/the-possibilities-and-the-pitfalls-of-virtual-currencies.

Feenan, Sara; Heller, Daniel; Lipton, Alexander; Morini, Massimo; Ram, Rhomaios; Sams, Robert; Swanson, Tim; Yong, Stanley and Barrero Zalles, Diana. "Decentralized Financial Market Infrastructures: Evolution from Intermediated Structures to Decentralized Structures for Financial Agreements." *Journal of FinTech*, 2021, *1*(2); https://doi.org/10.1142/S2705109921500024.

Feist, Dankrad. "On Supply and Demand for Stablecoins." September 27, 2021; https://dankradfeist.de/ethereum/2021/09/27/stablecoins-supply-demand.html.

Goodwin, Keith. "Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010." Federal Reserve History, July 21, 2010; https://www.federalreservehistory.org/essays/dodd-frank-act.

Kocherlakota, Narayana. "The Technological Role of Fiat Money." Federal Reserve Bank of Minneapolis *Quarterly Review*, Summer 1998; https://doi.org/10.21034/qr.2231.

Schär, Fabian. "Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets." Federal Reserve Bank of St. Louis *Review*, Second Quarter 2021, *103*(2), pp. 153-74; https://doi.org/10.20955/r.103.153-74.

Schär, Fabian and Berentsen, Aleksander. *Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction*. MIT Press, 2020; https://mitpress.mit.edu/books/bitcoin-blockchain-and-cryptoassets.

Selgin, George. "Central Bank Digital Currency as a Potential Source of Financial Instability." Cato Institute *Cato Journal*, Spring/Summer 2021; https://www.cato.org/cato-journal/spring/summer-2021/central-bank-digital-currency-potential-source-financial-instability.

Steelman, Aaron. "Full Employment and Balanced Growth Act of 1978 (Humphrey-Hawkins)." Federal Reserve History, October 1978; https://www.federalreservehistory.org/essays/humphrey-hawkins-act.

Szabo, Nick. "Smart Contracts." 1994; https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

Szabo, Nick. "The Idea of Smart Contracts." Satoshi Nakamoto Institute, 1997; https://nakamotoinstitute.org/the-idea-of-smart-contracts/.

U.S. Chamber of Commerce Institute for Legal Reform. "Cost and Compensation of the U.S. Tort System." October 24, 2018; https://instituteforlegalreform.com/research/costs-and-compensation-of-the-u-s-tort-system/.

Waller, Christopher. "A CBDC: A Solution in Search of Problem." Presented at the American Enterprise Institute, Washington, DC (via webcast), August 2, 2021; https://www.federalreserve.gov/newsevents/speech/waller20210805a.htm.

White, Larry. "Should the U.S. Government Create a Token-Based Digital Dollar?" Alt-M.org, June 19, 2020; https://www.alt-m.org/2020/06/19/should-the-u-s-government-create-a-token-based-digital-dollar/.