For release on delivery
7:00 p.m. EDT [4:00 p.m. PDT Local Time]
May 15, 2018

Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning?

Remarks by

Lael Brainard

Member

Board of Governors of the Federal Reserve System

at the

Decoding Digital Currency Conference
Sponsored by the Federal Reserve Bank of San Francisco

San Francisco, California

May 15, 2018

It is a pleasure to be here today. What better place to discuss digital currencies than in San Francisco, home to so many technology innovators working on new ways to disrupt various aspects of our daily lives? [1]

Because of the transformative potential of digital currency and distributed ledger technologies, the Federal Reserve is actively monitoring digital innovations in the financial system. We have been keenly evaluating developments in fintech and digital currencies through a multidisciplinary lens, combining information technology and policy analysis to study their potential implications for payments policy, supervision and regulation, financial stability, monetary policy, and the provision of financial services. This work draws from expertise throughout the Federal Reserve System and benefits from engagement with our colleagues internationally.

Cryptocurrencies

The past decade has seen a wave of important new developments in digital technologies for payments, clearing, and settlement. Cryptocurrencies represent the leading edge of this digital wave. And it was the advent a decade ago of Bitcoin, the first cryptocurrency, that first gave shape to the vision of a decentralized digital currency.

At the heart of any cryptocurrency is the creation of a new type of asset--the unit of the cryptocurrency itself--that is distinct from any traditional form of money used in routine transactions, such as U.S. currency or checking accounts in commercial banks. A typical cryptocurrency would not be a liability of any individual or institution. There is no trusted institution standing behind it. This is in stark contrast to U.S. currency and reserve balances,

[1] I am grateful to David Mills of the Federal Reserve Board for his assistance in preparing this text. The remarks represent my own views, which do not necessarily represent those of the Federal Reserve Board or the Federal Open Market Committee.

which are liabilities of the Federal Reserve Banks, and deposit accounts, which are liabilities of a bank or another regulated depository institution backed by federal insurance up to a specific level. And while a typical cryptocurrency may be used in payments, it is not legal tender, in contrast to U.S. currency.

A typical cryptocurrency relies on the use of distributed ledger technology, which provides a new way to keep ownership records and transfer ownership from one user to another, often with little to no information about the identity of the owner. For instance, Bitcoin relies on the blockchain, which is run by anonymous computers all over the world linked together through a ledger of anonymized transactions. Digital currencies use automation via computer processing power, networking via the internet, and cryptography to transfer value from one person to another. What is innovative is that the computer code behind these transactions uses automated checks and balances to validate the sender and receiver, and whether there is enough value in the sender's account to make the payment. Traditionally, this validation would be done by banks and payment networks. Instead, with a cryptocurrency, this validation could be done by anyone with enough computing power and resources to participate. Importantly, this technology is not owned or managed by any entity--regulated or not--that would be responsible for its maintenance, security, and reliability. Rather, its maintenance, security, and reliability are handled by a decentralized developer community, which often lacks strong governance.

This combination of a new asset, which is not a liability of any individual or institution, and a new recordkeeping and transfer technology, which is not maintained by any single individual or institution, illustrates the powerful capabilities of today's technologies. But there are also serious challenges. For instance, cryptocurrencies have exhibited periods of extreme volatility. If you purchased Bitcoin in December 2017 at a value of over $19,000, your

electronic claims would be worth close to half that today.[2] Indeed, Bitcoin's value has been known to fluctuate by one-quarter in one day alone. Such extreme fluctuations limit an asset's ability to fulfill two of the classic functions of money: to act as a stable store of value that people can hold and use predictably in the future, and to serve as a meaningful unit of account that can be used to assign a comparable value of goods and services.

In addition to losses, individual investors should be careful to understand the potential for other risks.[3] Cryptocurrencies may raise important investor and consumer protection issues. The lack of strong governance and questions about the applicable legal framework for some cryptocurrencies may make consumers vulnerable to mistakes, thefts, and security breaches without much, or any, recourse. Although the cryptographic technology may be robust to some events, such as the fraudulent double spending of the same units of the cryptocurrency for more than one transaction, the large number of breaches at some cryptocurrency exchanges and wallet providers suggest that significant vulnerabilities may remain with respect to security protections around customers' accounts.[4] These breaches remind us that relying solely on cryptography within the transfer technology is not enough. Ultimately, a more holistic approach to the security of the broader cryptocurrency ecosystem, along with added layers of security on top of cryptography, are likely to be necessary for cryptocurrencies to be widely adopted.

Some cryptocurrencies also appear quite vulnerable to money-laundering (BSA/AML, or Bank Secrecy Act/anti-money-laundering) concerns. Since many cryptocurrencies store in their

---

[2] See, for example, https://www.coinbase.com/charts.

[3] Lael Brainard, "An Update on the Federal Reserve's Financial Stability Agenda" (speech delivered at the Center for Global Economy and Business, Stern School of Business, New York University, New York, NY, April 3, 2018), https://www.federalreserve.gov/newsevents/speech/brainard20180403a.htm.

[4] For example, Coincheck, a Tokyo-based cryptocurrency exchange was hacked in 2018. See https://www.wsj.com/articles/cryptocurrency-worth-530-million-missing-from-japanese-exchange-1516988190. A similar attack occurred back in 2014 to another Tokyo-based cryptocurrency exchange, Mt. Gox. See https://www.wsj.com/articles/mt-gox-to-hold-news-conference-1393579356.

ledger little to no information about the identity of owners of the cryptocurrency, this essentially mimics a bearer instrument--that is, an instrument whereby the holder of the instrument is presumed to be its owner. Further, cryptocurrencies are easy to transfer across borders. Indeed, a cryptocurrency that mimics a bearer instrument and provides significant anonymity in transactions, including across borders, could raise significant concerns regarding the potential to facilitate illicit activities and associated money laundering. For example, electronic instruments can be easily transferred and stored in large amounts, and peer-to-peer transactions outside of the United States could be very hard to prevent and detect. Such instruments appear to have proven susceptible for use to convey payments to illicit actors--for example, to pay ransoms.

Overall, however, the still relatively small scale of cryptocurrencies in relation to our broader financial system and relatively limited connections to our banking sector suggest that they do not currently pose a threat to financial stability.[5] Of course, if cryptocurrencies were to achieve wide-scale use, or their impact were greatly magnified through leverage, the effects could be broader. In particular, adverse developments and shifts in sentiment could cause a global rush to exit this market. As we have seen in other speculative activity in the past, rush-for-the-exits behavior can aggravate price fluctuations, create trading difficulties, and even induce market breakdowns. Thus, we will continue to monitor cryptocurrencies as they evolve, with particular vigilance for any signs of growing materiality to the broader financial system.

Central Bank Digital Currencies

Given some of the inherent issues and challenges that cryptocurrencies pose for investor and consumer protection and the prevention of money laundering, some have advocated that central banks should create their own digital forms of currency as more stable and reliable

[5] See https://g20.org/sites/default/files/media/communique_-_fmcbg_march_2018.pdf.

alternatives to cryptocurrencies. After all, a central bank digital currency could overcome the volatility risks associated with an unbacked asset with no intrinsic value by substituting a digital instrument that is the direct liability of the central bank. Moreover, advocates suggest a central bank would be able to develop a transfer mechanism that has robust governance.

Even though central bank digital currencies may at first glance appear to address a number of challenges associated with the current crop of cryptocurrencies, this appeal may not withstand closer scrutiny.[6] First, there are serious technical and operational challenges that would need to be overcome, such as the risk of creating a global target for cyberattacks or a ready means of money laundering. For starters, with regard to money laundering risks, unless there is the technological capability for effective identity authentication, a central bank digital currency would provide no improvement over physical notes and could be worse than current noncash funds transfer systems, especially for a digital currency that could circulate worldwide. In addition, putting a central bank currency in digital form could make it a very attractive target for cyberattacks by giving threat actors a prominent platform on which to focus their efforts. Any implementation would need to adequately deal with a variety of cyber threats--especially for a reserve currency like the U.S. dollar.

Second, the issuance of central bank digital currency could have implications for retail banking beyond payments. If a successful central bank digital currency were to become widely used, it could become a substitute for retail banking deposits. This could restrict banks' ability to make loans for productive economic activities and have broader macroeconomic consequences. Moreover, the parallel coexistence of central bank digital currency with retail banking deposits

[6] See, for example, the recent joint Committee on Payments and Market Infrastructures and Markets Committee report "Central Bank Digital Currencies," March 2018, https://www.bis.org/cpmi/publ/d174.pdf. A Fed-issued digital currency might have implications for the rates and terms of funding for U.S. financial institutions and even the U.S. government as well as the transmission of monetary policy that I will not discuss here.

could raise the risk of runs on the banking system in times of stress and so have adverse implications for financial stability.

Finally, there is no compelling demonstrated need for a Fed-issued digital currency. Most consumers and businesses in the U.S. already make retail payments electronically using debit and credit cards, payment applications, and the automated clearinghouse network. Moreover, people are finding easy ways to make digital payments directly to other people through a variety of mobile apps. New private-sector real-time payments solutions are beginning to gain acceptance in the United States. And the Faster Payments Task Force has laid out a roadmap embraced by a variety of stakeholders for a fast, ubiquitous, and secure payments system to be in place in the United States in the next few years.[7] In short, a multiplicity of mechanisms are likely to be available for American consumers to make payments electronically in real time. As such, it is not obvious what additional value a Fed-issued digital currency would provide over and above these options.

Wholesale Digital Settlement Tokens

It is important for the Fed and other central banks to continue to research these issues as technology evolves, exploring the technical and economic possibilities and limitations of central-bank-issued digital currencies. Even though the case for a digital currency for general use may not be compelling, opportunities for more targeted and restricted use may nonetheless prove to have value. The private sector has been exploring a variety of ways of deploying the underlying technologies of digital assets that are native to a particular wholesale platform, to help to

[7]See https://fedpaymentsimprovement.org/faster-payments/path-to-faster-payments/.

facilitate finality of settlement. Such wholesale digital settlement tokens could potentially reduce the time and costs required for wholesale financial transactions. This is being discussed, for instance, for the use cases of interbank payments, securities settlements, and cross-border transactions, where the introduction of a digital token native to a platform may facilitate certain types of settlement.

Likewise, it is possible at some point in the future that a limited central bank digital instrument that serves as a settlement asset for wholesale payment and settlement activity may hold some promise. Several central banks have been studying this issue, and we have been actively watching these developments.[8] We are also interested in work that decouples the underlying distributed ledger technology from cryptocurrencies and attempts to build on the benefits of the technology, a topic to which I now turn.

Distributed Ledger Technology

Even if cryptocurrencies prove to have a very limited role in the future, the technology behind them is likely to live on and offer improvements in the way we transfer and record more traditional financial assets. Distributed ledger technology could also facilitate other applications that could improve the way we share information, validate possessions, and handle logistics.

Recall that distributed ledger technology is the mechanism for recordkeeping and transfer of ownership that underpins cryptocurrencies. Over the past few years, the financial industry has conducted a great deal of research and development on how to adapt the more promising aspects of distributed ledger technology for use with more traditional financial assets. The industry has moved a number of these projects through a series of phases, often developing more incremental changes at first in order to gain confidence in the technology before tackling large projects with

[8] For example, see Bank of Canada's Project Jasper, https://www.bankofcanada.ca/research/digital-currencies-and-fintech/fintech-experiments-and-projects/.

significant operational impacts. The industry is making steady progress and some projects could be live in some form this year.

Many of the use cases focus on the areas of post-trade clearing and settlement of securities transactions, cross-border payments solutions, and trade finance. The common thread running through these use cases is the presence of operational "pain points" that generate inefficiencies and delays for users. For example, post-trade reconciliation of securities transactions can be a time-consuming and resource-intensive process that involves numerous parties, operational steps, and message flows across the counterparties and their various agents involved in the transactions. Distributed ledger technology has the potential to provide synchronized, real-time views for those counterparties and agents that can speed up the process and reduce errors.

For cross-border transactions, the process for sending payments via the existing correspondent banking network can add time and money. Distributed ledger technology could potentially lower the costs and time it takes funds to reach the recipient through more direct connections, reducing the number of intermediaries required to effect the transaction.

The financial industry has been working on versions of distributed ledger technology that help address a number of concerns, including the loose governance around the maintenance, security, and reliability of the technology for cryptocurrencies. Most projects are organized either as partnerships between technology and financial services firms or through consortia of technology firms, financial firms, and other interested parties. To some degree, these alliances may provide prototype governance arrangements for future technology deployments in financial services. In addition, there are exchanges and clearinghouses that are actively exploring the use of distributed ledger technology, which represent the more traditional model of multilateral

organization in the financial markets. Although the governance arrangements may need to evolve over time, one thing that is clear is that strong governance arrangements will be required to provide the coordinated operational and financial risk management for the critical clearing and settlement operations that underpin our financial markets.

In addition, the industry continues to make progress on the ability of distributed ledger technology to handle the very large volumes of transactions that take place both in financial markets and in retail payments every day. As I highlighted in 2016, this technical challenge of achieving the necessary scale and through put is an important hurdle.[9] Much of this challenge has been tied to the time it takes to achieve "consensus" on a distributed ledger. Consensus is the process by which new transactions are broadcast to all the participants, or nodes, in the network and each node accepts those new transactions as valid additions to the ledger. The initial consensus method used by Bitcoin, called "proof of work," is designed to deal with the lack of information and trust among the users of the network by providing tools and incentives to overcome this problem. But it is a highly resource-intensive process that limits the number of transactions that can be processed each second. The proof of work consensus model represents a tradeoff between operational efficiency and scalability, on the one hand, and the ability to operate without sufficient trust or information about the entities in the network, on the other hand.

Fundamentally, however, the financial industry does not operate as a trustless network. Rather, the industry has long specialized in the collection and analysis of information about

[9] Lael Brainard, "The Use of Distributed Ledger Technologies in Payment, Clearing, and Settlement" (speech delivered at the Institute of International Finance Blockchain Roundtable, Washington, DC, April 14, 2016), https://www.federalreserve.gov/newsevents/speech/brainard20160414a.htm; and Lael Brainard, "Distributed Ledger Technology: Implications for Payments, Clearing, and Settlement" (speech delivered at the Institute of International Finance Annual Meeting Panel on Blockchain, Washington, DC, October 7, 2016), https://www.federalreserve.gov/newsevents/speech/brainard20161007a.htm.

customers and counterparties as a core part of banking operations. Even allowing for the inevitable imperfect information that may result, it would seem natural for the financial industry to be able to leverage institutional information and trust in ways that allow for more efficient methods to achieve consensus than proof of work. Consequently, the industry and the academic community have focused a great deal of attention on various consensus methods that can provide greater scalability either by leveraging trust, which relaxes some operational and incentive constraints, or possibly by devising methods without trust that are much less resource intensive. Some of the technology firms working with the financial industry are taking different approaches in this fast-moving arena.

Another important challenge for the industry has been leveraging distributed ledger technology while preserving the confidentiality of transactional information. At its core, distributed ledger technology is a shared ledger across multiple nodes in a network, likely representing multiple firms and legal entities. Ownership records and transactions flows from accounts on such a ledger are typically copied and stored on all the nodes in the network. The financial industry, however, must develop distributed ledgers that adhere to laws, regulations, and policies that protect important information of the parties and their customers. Clearly, a model where every entity on the network can see everyone else's account holdings and transactions history will not satisfy broad industry confidentiality requirements. In addition, stored data that may be protected cryptographically today may not be protected as the technology continues to advance, which adds even more difficulty and urgency to the work on confidentiality.

The industry has been working to develop approaches to preserve confidentiality so that only the authorized parties relevant to a transaction can see the details recorded on the ledger.

Some of these approaches involve encrypting data on the ledger so that the ledgers can still be copied across all the nodes in the network, but an entity cannot look at any element of that ledger except for transactions in which it has been involved. Other approaches include so-called zero-knowledge proofs or ring signatures that allow entities to validate transactions without seeing confidential information. Still others are looking at platforms that connect multiple ledgers rather than having one single ledger that is copied across all nodes in the network. While questions remain about the usefulness and viability of each of these approaches, it is important to underscore that preserving confidentiality is an important area of research.

Finally, perhaps the biggest potential benefit for payments, clearing, and settlement of distributed ledger technology may be resiliency. Distributed ledger technology may enable a network to continue to operate even if some of the nodes on the network are compromised because of the ability of the other nodes in the network to pick up the slack and continue processing transactions. One challenge going forward will be to understand the implications that the confidentiality tools and different approaches to consensus under consideration may have on the resilience of the distributed ledger. Given that resiliency is a key potential benefit of distributed ledger technology over existing platforms, it is critical to understand the trade-offs between resiliency and a consensus method that focuses on operational speed, or between resilience and confidentiality.

Conclusion

It is an exciting time for the financial sector as digital innovations are challenging conventional thinking about currency, money, and payments. Cryptocurrencies are strikingly innovative but also pose challenges associated with speculative dynamics, investor and consumer protections, and money-laundering risks. Although central bank digital currencies may be able

to overcome some of the particular vulnerabilities that cryptocurrencies face, they too have significant challenges related to cybersecurity, money laundering, and the retail financial system. Even so, digital tokens for wholesale payments and some aspects of distributed ledger technology--the key technologies underlying cryptocurrencies--may hold promise for strengthening traditional financial instruments and markets. I have highlighted a few key areas where the technology is advancing to deal with some important policy, business, and operational challenges. The Federal Reserve is dedicated to continuing to monitor industry developments and conduct research in these vital areas. I remain optimistic that the financial sector will find valuable ways to employ distributed ledger technology in the area of payments, clearing, and settlement in coming years.