

Innovation, technology, and the payments system

Jerome Powell looks at where technological innovation is driving change in the payments system and the role of the authorities in keeping money safe

New technology and innovative businesses increasingly affect our daily financial lives. Mobile devices, high-speed data communication, and online commerce are creating expectations that convenient, secure, real-time payment and banking capabilities should be available whenever and wherever they are needed. At the same time, disruptive new technologies suggest that traditional financial service providers must innovate and adapt or be left behind.

Against this backdrop of technological change and heightened expectations, it is worth remembering our broad public policy objectives, which are driven by the fundamental importance of the payments system in our society. I will lay out those objectives as we see them at the Federal Reserve, and focus in particular on their application in three specific areas where technological innovation is driving change: creating a real-time retail payments system, using distributed ledger technology to develop new clearing and settlement services, and the issuance of digital currencies by central banks.

Public policy objectives for the payments system

We trust financial intermediaries to hold and transfer funds in a safe and secure manner to meet the needs of commerce. The payments system provides financial institutions and their customers a variety of ways to transfer funds, but the goal is essentially the same in all cases: to move money from one individual or business to another in a reliable, secure, low-cost, and convenient manner.

The Federal Reserve and other central banks have adopted broad public policy objectives to guide the development and oversight of the payments system. At the Fed, we have identified efficiency and safety as our most fundamental objectives, as set forth in our [Policy on Payment System Risk](#)¹.

An efficient payments system provides the infrastructure needed to transfer money in low-cost and convenient ways. Efficient systems are innovative in improving the quality of services in response to changing technology and

changing demand. Efficient systems are also broadly accessible through means that are convenient for consumers, businesses, and financial institutions around the country. Safe payment systems are built from proven technology and operate reliably and with integrity. Safe systems address a range of well-known risks, including legal, operational, security, and financial risks. Information security and privacy have become particularly important in recent years. Overall, the payments system must be innovative, while also addressing risks, supporting financial stability, and maintaining public confidence.

Faster and more secure retail payment systems

The development of real-time retail payments has been gaining momentum globally. The UK has had a system in place since 2008. Australia is actively developing a new nationwide system. The European Central Bank, the Bank of Japan, and several other central banks have also been acting as catalysts to promote real-time payments initiatives.

We live in a time of extraordinary technological change. We should be open to the new ideas and innovations that will drive economic growth and improvements in our financial system

The broad emergence of real-time systems throughout the world reflects the growing demand for such systems, and the need for the payments system to keep up with [evolving technology](#)².

In the United States, our traditional bank-centric payments system, sometimes operating on decades-old infrastructure, has adjusted slowly to the evolving demands for greater speed and safety. Innovators have built new systems and services that ride on top of the old rails but with mixed results, and over time, our system has grown more fragmented. Our payments system is large and diverse, with a wide array of financial institutions, systems, and service providers; it will take coordinated action to make fundamental and successful nationwide improvements. The Federal Reserve has often helped address problems of this nature by convening stakeholders in the payments system and encouraging them to identify key issues and to work together to make fundamental improvements.

With this in mind, the Federal Reserve has in recent years been working with a wide range of stakeholders to improve the speed, efficiency, and safety of the US payments system. Significant dialogue and public responses to a consultation paper in 2013 indicated that stakeholders would welcome a broad initiative to work for change. In response, in 2015, the Federal Reserve launched several initiatives including a Faster Payments Task Force and a Secure Payments Task Force.

I spoke about the payments security initiative on another [occasion](#)³. The Secure Payments Task Force has been advancing important work, including outlining ways for the industry to improve payment identity management practices, crafting guidance on standardizing fraud and risk data, and developing a framework for protecting sensitive payment data. You can expect to see the results of these efforts later this year.

In this article I will focus on the [Faster Payments Task Force](#). In forming the task force, we committed to an inclusive and transparent approach that would ensure representation of diverse stakeholder interests. The group is com-

prised of over 300 representatives from financial institutions, technology companies, consumer advocates, and others⁴. The role of the task force is to identify and assess alternative approaches for implementing safe, ubiquitous, faster payment capabilities in the United States.

To support that mission, the task force developed a framework, called the *Faster Payments Effectiveness Criteria*, to provide guidance to the wider payments community on the desired attributes of a future payments system. The framework identified 36 'effectiveness criteria' that a faster payments system should meet, covering six broad areas: ubiquity, efficiency, safety and security, speed, legal framework, and governance. Task force members and others have widely embraced the effectiveness criteria. Our hope is that the criteria will serve as a lasting blueprint for payments service providers in designing innovative future products.

The task force also established a process through which its members could submit proposals for faster payments capabilities and have them assessed against the effectiveness criteria by a qualified independent assessment team. The task force encouraged members to submit proposals reflecting both products under development and conceptual designs. There was overwhelming enthusiasm around the process, and the task force ultimately completed reviews of 19 faster payments proposals. Collectively, the proposals represent a broad range of creative and innovative ways to deliver real-time payments. Some are based on current designs and established technology. Others leverage the latest innovative ideas and technologies.

In 2017, the task force has been working on a final report. [Part 1 of the report](#) - the background and motivation for pursuing faster payments - was published in January⁵. Part 2 will include the proposals themselves and their assessments, along with task force recommendations for moving the US payments system forward in implementing faster payments. Part 2 will be released around the middle of this year. Until then, the proposals remain confidential to the task force.

The role of the task force is not to select one or more proposals for implementation, but rather to assess the proposals against the task force criteria. It will be the job of the financial industry to take these proposals forward as they see fit. I strongly encourage the industry and other stakeholders to continue the work of bringing ubiquitous real-time payments systems and services to the US market. It will be important that we keep end users in mind as the new real-time environment evolves, emphasizing inclusion, safety and trust, and consumer education and protections. End users will ultimately determine the success of new payment services and the future direction of faster payments in this country.

Distributed ledger technologies

Let's turn to another type of new technology that may have important implications for the payments and financial systems: distributed ledger technology, or DLT. Bitcoin helped bring this technology to public attention. Using blockchain technology - which employs a form of DLT - and an open architecture, Bitcoin allows for the transfer of value (bitcoins) between participants connected to its ecosystem without reliance on banks or other trusted intermediaries. This feature has led some to predict that DLT will in the long run render parts of the banking and payments system obsolete, as the intermediation of funds through the banking system will become unnecessary.

Faced with these dramatic predictions, we have seen banks and market infrastructures collaborate with technology firms to explore the use and further development of DLT. In 2016, there was widespread experimentation. Efforts by financial institutions often focused on evaluating the technology, identifying potential uses, and conducting proofs of concept.

Prominent examples included the use of distributed ledgers to store transactional data and records in tamper-proof ways, as well as the use of the technology as a primary means to hold and transfer money or assets. By the end of 2016, a few major US clearing organizations had announced plans to use distributed ledger technology in limited ways.

As we have followed developments over the past year, a few lessons have come into [better focus](#)⁶. First, in contrast to Bitcoin's open architecture, work by the financial industry has focused on the development of 'permissioned' systems, which establish criteria to determine who is permitted access to particular systems, ledgers, functions, or information. In the near term, this approach seems more likely than fully open systems to provide the needed governance and management to address operational, security, and financial risks. Indeed, access is typically permissioned in situations that require the protection of systems and information in the financial and other industries.

Even in permissioned systems, some key issues will remain, including whether finality of settlement is to be determined by a central trusted party or by a majority of participants, and whether participants are able to view information on other parties' transactions. Some argue that movement away from open systems undermines the potential efficiency and the spirit of DLT. At least for now, in payment, clearing, and settlement, safety and confidence must also weigh in the balance.

Second, firms are still grappling with the business case for upgrading and streamlining payment, clearing, settlement, and related functions with DLT. Promoters of DLT offer a vision of streamlined processes that lead to faster processing, reduced reconciliation, and lower long-run operating costs. Some argue that in certain markets, faster and more predictable processing will also reduce the capital and liquidity costs of operations. But upgrades are often costly, lengthy, and risky, particularly if the technology is still being proven, as is the case for DLT. Network effects can also affect adoption, since multiple firms may all need to adopt a particular implementation of DLT in order to justify its use in a specific market.

Third, technical issues remain. Practical issues such as whether a particular version of DLT will work for the intended purpose are still being explored. Issues of reliability, scalability, and security remain very important. Beyond these issues, standardization and interoperability across different versions of DLT will need to be addressed to allow tech-

nology integration and avoid market fragmentation. In general, industry members and technology providers recognize these important issues and have taken initial steps to address problems. It will be important to keep these challenges firmly in mind as we move beyond experimentation and into the development and deployment of new products and processes.

Fourth, governance and risk management will be critical. For individual firms or clearing houses that adopt DLT as an internal technology upgrade, the governance and risk-management processes are likely to be internalized within existing organizations and be akin to other technology upgrades. However, if new networks of bilateral payment, clearing, and settlement are established, the new technology may involve tightly coupled protocols and operations.

The safety of the overall design will depend on a highly interdependent framework. If automated risk management, smart contracts, and similar tools are deployed across a network, cascades of rapid and hard-to-control obligations and liquidity flows could propagate across a network and the financial system in response to events. This interdependence will likely call for creative organizational thinking to address the need for governance and strong risk management.

Finally, the legal foundations supporting DLT will need attention. Deployments of DLT will involve firms, perhaps in different jurisdictions, with systems that record and transfer information and assets under existing legal frameworks. Which bodies of law apply to the particular firms, assets, and activities will determine the associated rights and responsibilities when transfers are made, cleared, and settled.

For example, whether and how banking, payments, securities, or commodities laws apply in a given context are likely to be important in designing systems and services and understanding their properties. And, as with any new technology, things may go wrong. We will need a thorough analysis of how DLT fits into current legal frameworks

and what gaps need to be filled by contractual agreements or new laws and regulations. A robust legal basis that provides certainty across relevant jurisdictions is essential for building strong governance, risk management, and operations.

Digital currencies issued by central banks to the general public

My last topic is the potential use of DLT or other technologies by central banks to issue a digital currency to the general public. In a sense, the idea of a digital currency is merely a 21st century analog of paper currency. While this is a fascinating idea, there are significant policy issues that need to be [analyzed](#)⁷.

First, there are meaningful technical challenges. We should have serious reservations about our ability to keep a generally circulating digital currency safe and secure over the long run. A digital currency issued by a central bank would be a global target for cyber attacks, cyber counterfeiting, and cyber theft. The threats could significantly exceed historical experience with paper currency.

A digital currency would also be a prime target as a potential vehicle for global criminal activities, including money laundering. Central banks could face difficult trade-offs between strengthening security and enabling illegal activity. Advanced cryptography could reduce vulnerability to cyber attacks but make it easier to hide illegal activity. To the extent we relax strong cryptography to make it easier for authorities to monitor illegal activity, we could simultaneously weaken security. Growing computer power over time could be used to increase security but could also increase threats.

Second, privacy issues must be seriously considered. Central banks would have to maintain records of digital currency issuance and might need to maintain records of individual transactions in order to authenticate those transactions and to combat cyber risks and illegal activity. In today's environment, commercial banks maintain extensive

records for individual debit and credit card transactions and increasingly monitor patterns of behavior for fraud. Such records in the hands of a central bank or government entity, however, could raise serious privacy concerns by users and might limit public appeal. Again, there may be important trade-offs between privacy and risk.

Any central bank actively considering issuing its own digital currency would need to carefully consider the full range of the payments system and other policy issues, which do seem substantial, as well as the potential societal benefits. To my mind, they should also consider whether the private sector can substantially meet the same needs.

Private-sector products and systems already exist or are being developed that will fulfill demands that central-bank-issued digital currencies might otherwise seek to meet. Prepaid cards grew out of the wave of retail payments innovation in the mid-1990s and are now in widespread use. And as I mentioned earlier, new private-sector-led faster payments initiatives are coming.

In the United States, a faster payments system that operates around the clock and provides the capability to hold and transfer deposits insured by the Federal Deposit Insurance Corporation in real time would go a long way toward providing the low-risk and flexible payment arrangements that paper currency historically provided. Indeed, I would expect private-sector systems to be more forward leaning than central banks in providing new features to the public through faster payments systems as they compete to attract retail customers. A central bank issued digital currency would compete with these and other innovative private-sector products and may stifle innovation over the long run.

Conclusion

We live in a time of extraordinary technological change. We should be open to the new ideas and innovations that will drive economic growth and improvements in our financial system. At the same time, the public rightfully ex-

pects that authorities will do whatever it takes to keep their money safe. Those of us in the public sector will insist on safety and security, while also working to assure that our citizens benefit from payments system innovation. ■

Governor Jerome H Powell is a Member, Board of Governors of the Federal Reserve System

1. See Board of Governors of the Federal Reserve System, "The Federal Reserve Policy on Payment System Risk" (Washington: Board of Governors, 2016).

https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf

See also Board of Governors of the Federal Reserve System, The Federal Reserve System Purposes & Functions, 10th edition (Washington: Board of Governors, 2016),

<https://www.federalreserve.gov/pf/pf.htm>

and Federal Reserve System, "Strategies for Improving the US Payment System" (Washington: Board of Governors and Federal Reserve System, 2015).

<https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf>

2. For a broad discussion of international developments and issues in faster payments, see Committee on Payments and Market Infrastructures, "Fast Payments--Enhancing the Speed and Availability of Retail Payments" (Basel, Switzerland: Bank for International Settlements, November 2016).

<https://www.bis.org/cpmi/publ/d154.pdf>

3. See Jerome H Powell, "Building a Safer Payment System" (speech delivered at the Federal Reserve Bank of Kansas City Conference, "The Puzzle of Payments Security: Fitting the Pieces Together to Protect the Retail Payments System," Kansas City, Missouri, June 25, 2015).

<http://www.federalreserve.gov/newsevents/speech/powell20150625a.htm>

4. Information about the Faster Payments Task Force and the companion Secure Payments Task Force is available at <https://fedpaymentsimprovement.org/>
5. See “The US Path to Faster Payments, Final Report Part One: The Faster Payments Task Force Approach,” Faster Payments Task Force (2017).
<https://fedpaymentsimprovement.org/wp-content/uploads/path-to-faster-payments.pdf>
6. See David Mills, Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, Clinton Chen, Anton Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kargenian, Max Ellithorpe, Wendy Ng, and Maria Baird, “Distributed Ledger Technology in Payments, Clearing, and Settlement,” Finance and Economics Discussion Series 2016-095 (Washington: Board of Governors of the Federal Reserve System, December 2016).
<https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf>
7. Several of these and additional issues relating to the issuance of digital currencies by central banks are touched on briefly in Committee on Payments and Market Infrastructure, “Digital Currencies” (Basel, Switzerland: Bank for International Settlements, November 2015).
<http://www.bis.org/cpmi/publ/d137.pdf>

Based on a speech given at Blockchain: The Future of Finance and Capital Markets? at Yale Law School Center for the Study of Corporate Law Weil, Gotshal & Manges Roundtable at Yale University, New Haven, Conn. March 3, 2017