

Lael Brainard: Distributed ledger technology – implications for payments, clearing, and settlement

Speech by Ms Lael Brainard, Member of the Board of Governors of the Federal Reserve System, at the Institute of International Finance Annual Meeting Panel on Blockchain, Washington DC, 7 October 2016.

* * *

We recognize the potential of distributed ledger technology, or blockchain, to transform the way financial market participants transfer, store, and maintain ownership records of digitized assets. The genuinely innovative aspect of distributed ledger technology combines a number of core elements that can be used to support the transfer process and distributed recordkeeping for digital assets and digital representations of assets. These elements include peer-to-peer networking and distributed data records, which provide broadly shared access to a single ledger across participants in the system, so that all participants maintain a shared, accurate history of all transactions in the system. In addition, cryptography provides a secure way to initiate a valid transaction as well as to securely transmit and store data. And consensus algorithms provide a process for transactions to be confirmed and added to the single ledger, which is an important feature when more than one participant has permission to propose updates to the ledger. We are paying close attention to distributed ledger technology, or blockchain, recognizing this may represent the most significant development in many years in payments, clearing, and settlement.¹

The Federal Reserve Board has established a working group that is engaged in a 360-degree analysis of financial innovation across the broad range of our responsibilities, drawing on engagement with industry stakeholders and on expertise from across the Federal Reserve System, including in supervision, consumer protection, financial stability and information technology. One important area of oversight is the payments system, where technology changes are viewed through the prism of our responsibilities for promoting the safety and efficiency of the payments and settlements systems; supervising financial institutions engaged in payments, clearing and settlement; and safeguarding financial stability. We want to maintain public confidence in the payments system, while supporting innovation that provides broadly shared benefits to the public over time, including through the reduction of unnecessary frictions, costs, and delays.

Illustrative Use Cases

Let me briefly mention a few of the use cases that we have explored in our discussions with industry stakeholders in order to illustrate the potential of distributed ledger technologies to improve payments, clearing, and settlement, as well as the considerations that are important to us in our assessment of benefits and risks.

In cross-border payments and trade finance, significantly faster processing and reduced costs relative to the long and opaque intermediation chains associated with current methods of correspondent banking are promising potential benefits of the technology. Reducing intermediation steps in cross-border payments may help decrease time, costs, and counterparty risks and may materially diminish opacity, for instance by enabling small businesses or households remitting payments across borders to see the associated transfer costs and processing times up front. In trade finance, where document-intensive processes are not fully automated, distributed ledger technology may be able to reduce significant costs and speed up processing associated with issuing and tracking letters of credit and associated documents. To see the full potential of this technology realized for cross-border payments, it will be important to identify and track identities associated with the transactions, which in itself may be facilitated by the use of distributed ledgers, depending on their design.

In securities markets, the industry is exploring activities ranging from the issuance of securities on a distributed ledger, to the clearing and settlement of trades, to tracking and administering corporate actions. For securities clearing and settlement in particular, the potential shift to one master record shared “simultaneously” among users of a distributed ledger-based system could be compelling. Sharing one immutable record may have the potential to reduce or even eliminate the need for the reconciliation of multiple records linked to a single trade among and between dealers and other organizations. In concept, such technology could lead to greater transparency, reduced costs, and faster settlement. Likewise, distributed ledgers may improve collateral management by improving the tracking of ownership and transactions. Nonetheless, as is frequently true in the complex arena of payments, clearing, and settlement, we can also expect that practical details covering a host of technical, business, and market issues will have an important role in determining how new technologies ultimately perform.

For commodities and derivatives, there are projects to streamline some of the more antiquated corners of the markets. In markets that are heavily paper-based and lack any central means for coordination, distributed ledger technology could potentially be leveraged to provide coordination that facilitates exchange, clearing, and settlement of obligations.

A related development is the potential coupling of distributed ledger protocols with self-execution and possibly self-enforcement of contractual clauses, using so-called “smart contracts.” To take a familiar example, for a corporate bond with a specified par value, tenor, and coupon payment stream, a smart contract would automatically execute payments on the specified schedule to the assigned owner over the life of the bond. Although the idea of automating certain aspects of contracts is not new, and banks do some of this today, the potential introduction of smart contracts does raise several issues for consideration. For example, what is the legal status of a smart contract, which is written in code? Would consumers and businesses rely on smart contracts to perform certain services traditionally done by their banks or other intermediaries? Could the widespread automated interaction of multiple counterparties lead to any unwanted dynamics for financial markets? These and other considerations will be important factors in determining the extent of the application of smart contracts.

Regardless of the application, much of the industry is at a “proof of concept” stage of development. These proofs of concept are often simple, experimental uses of the technology on a small scale that help stakeholders understand the potential and limitations of the technology for a specific purpose, which in turn typically lead to refinements and more developed proofs of concept. As such, many potential applications are in their infancy, and the industry may still be several years away from an application that is ready to be fully implemented. Even so, the industry seems to be making announcements daily on new proofs of concept and progress that may lead to pilots, so that timeline could accelerate. In some cases, there have been announcements the technology will be used within the next year or two in actual production environments. The initial relatively simple proofs of concept must be followed by much more complex demonstrations in real-world situations before these technologies can be safely deployed in today’s highly interconnected, synchronized, and far-reaching financial markets.

Although many private and inward-facing projects are being explored, the industry has also recognized the need to collaborate at early stages of development. An important positive development is that industry participants are actively engaging with each other to look for common approaches. Some groups are creating standards that facilitate common platforms to enable greater interoperability of often proprietary applications that are built on them and interoperate through application program interfaces, or APIs.

In coming months and years, innovators, investors, and financial practitioners will no doubt make important strides in addressing key challenges such as adopting common standards, achieving interoperability between and among legacy systems and evolving distributed ledgers, improving scalability and computational throughput, and improving cryptographic security. These are

positive developments that we will monitor closely.

Managing Risks

All of this activity demonstrates that we are in a very innovative period. The industry is eager to get on with adopting the various possibilities that distributed ledger technology may bring. However, established players and, increasingly, new entrants understand that there are important guardrails that have been carefully developed over many years in the arena of payments, clearing, and settlement. The safety and soundness of financial institutions, safety and efficiency of the payment system, and broader financial stability are critical to a healthy financial environment that fosters innovation with broad public benefits over the long run. We expect the private sector to bear important responsibility for developing and deploying new financial technologies in a safe and sound manner, even as we all seek an innovative and efficient payment system over the long run. The deployment of any new financial technology must be undertaken with a thorough understanding and management of risks.

Like many new financial technologies, distributed ledgers could ameliorate or exacerbate traditional financial risks. What matters to us as policymakers and regulators is not only whether the migration to a new technological platform increases or reduces risks, but also whether risks are rendered more or less opaque, and how they are distributed among and between financial intermediaries and end users. In the payments, clearing, and settlement arena, some important risk areas for consideration include settlement, operations, and cybersecurity, as well as money laundering and terrorist financing. In managing risks, important considerations include system resiliency and governance as well as the role of licensing in ensuring proper oversight.

In securities settlements, for example, a difference in timing between the delivery of securities and the delivery of funds introduces settlement risk between counterparties and other institutions involved in this process. To the extent that distributed ledger technologies are designed to supplant the traditional reliance on trusted intermediaries to ensure settlement, they will need to reliably demonstrate their ability to mitigate or even eliminate settlement risk, especially in cases where the delivery of the securities and the associated payment take place on different platforms.

Traditional payment, clearing, and settlement are subject to operational risk, and it is critically important that new technologies operate reliably, securely, and with integrity. The daily operation of markets and their clearing and settlement functions are built on trust and confidence. Market participants trust that clearing and settlement functions and institutions will work properly every day. Confidence has built over time that when market participants trade, accurate and timely clearing and settlement will follow.

Thus, robust security is an important element of any system. The distributed nature of this new technology, combined with the fact that many connected participants can update the shared ledger, means that end-point security is another critical component of any successful implementation of the technology. Adverse actors that can take over a participant's access to the ledger remains a key security concern, as thefts of cryptographic keys in Bitcoin continue to demonstrate. Thus, advances in cryptography will remain a key priority to enable widespread adoption of distributed ledger technologies, along with systems for securing private keys, the management of access to private keys, and differentiated permissions for participants in the system to read and write to the ledger. Recent episodes have illustrated the importance of having protocols agreed at the outset to determine whether and under what circumstances to reverse transactions once they have been recorded in a distributed master ledger.

Finally, it will be important that users and administrators of distributed ledger technologies can meet their responsibilities to combat money laundering, terrorist financing, and other key law enforcement concerns. Some of the new technologies would potentially allow authorized access to certain data records in a much more efficient manner than has previously been possible. For example, distributed ledgers could be developed to collect personally identifiable information and

country identifiers that enable banks to identify and report on suspicious activity. It will be important that these new technological developments and their implementation perform in a safe and sound manner that is transparent and satisfies regulatory requirements.

While prevention will remain the preferred approach, realistically, resiliency and recovery will also need to be high-priorities. Indeed, many firms have suggested that the distributed data storage concept has the potential to increase the level of resiliency and data integrity. The basic idea is it should be harder to corrupt multiple copies of the same data simultaneously such that digital ledgers could reduce the vulnerability associated with a single point of failure. We must press firms and experts to identify the strengths and vulnerabilities of this concept, even as we all look for ways to make databases more secure and resilient. In an interesting development, some financial institutions have also begun to consider using distributed ledgers to back up critical databases and enable quick recovery from potentially virulent cyberattacks. We will be interested in whether such techniques can make new contributions to cybersecurity.

Overall, the public needs to have confidence that any system employing distributed ledgers will operate properly, particularly in stressed conditions, and know that when adverse scenarios do occur, there will be robust management and governance to respond effectively. Recent events, such as thefts from accounts on distributed ledger platforms, highlight the challenge that distributed ledgers may have when adverse scenarios occur and there is uncertainty around what an appropriate response would be. Such uncertainty around management and governance can raise doubts about the integrity of a system employing distributed ledgers.

Traditionally, financial regulators in the United States have been given licensing authority as a key way of ensuring that responsibility for managing risks is transparently assigned with appropriate oversight. The development of new business models associated with evolving financial technologies has raised questions about the applicability of existing licenses and their adequacy to new business models. For instance, the Monetary Authority of Singapore recently issued a consultation paper that proposes an activity-based payments framework as a way to address the introduction of non-traditional payment providers.² The United States has seen several noteworthy recent developments, including the New York State Department of Financial Services' BitLicense, a distributed ledger company, securing Federal Reserve Bank of New York approval for participation in the National Settlement Service, and, most recently, discussion by the OCC of a limited-purpose charter.

Ongoing Engagement

Because of the notable potential of distributed ledger technology, financial authorities, both domestic and international, will follow these developments with keen interest. At the Federal Reserve, we expect to publish a research paper later this year that summarizes some of the key findings from our industry engagement so far. Going forward, we will continue to deepen our engagement with a range of financial institutions, technologists, multi-stakeholder consortia, and academic experts to refine our understanding of the new technologies, along with their possibilities and limitations, with a particular focus on our responsibilities for the payments system, as well as our oversight of financial market intermediaries. We will also continue to discuss these issues with other central banks and authorities around the world. We will work together to foster socially beneficial innovation, while insisting that risks are thoroughly understood, managed, and controlled.

¹ See www.federalreserve.gov/newsevents/speech/brainard20160414a.htm. Also, see the forthcoming Feds working paper, "Staff Study on Distributed Ledger Technology in Payments, Clearing, and Settlement," 2016.

²

See www.mas.gov.sg/~media/resource/publications/consult_papers/2016/Proposed%20Activity%20Based%20F