Benoît Cœuré: The future of financial market infrastructures - spearheading progress without renouncing safety

Speech Mr Benoît Cœuré, Member of the Executive Board of the European Central Bank, at the Central Bank Payments Conference, Singapore, 26 June 2018.

* * *

I wish to thank the organisers for inviting me to speak here today.[1]

It's great to see so many familiar faces and to be back in Singapore, which as an undeniably cosmopolitan city is a particularly suitable backdrop for talks on the multifaceted nature of today's global market infrastructures.

The message I would like to convey in my remarks this morning is simple: while I share the excitement around distributed ledgers, blockchain and digitalisation more broadly, and while I believe that, like in the past, central banks should not shy away from potentially disruptive technological innovations, we should be mindful of the potential financial stability consequences and we should start by first picking the low hanging fruit and upgrading our current payment systems.

In fact, I believe that an incremental modernisation of our existing retail and wholesale payment systems may well succeed in bringing about many of the benefits promised by the current crop of immature technologies.

The challenges of digital innovation

Let me start with the challenges first.

There is no doubt that the fourth industrial revolution is dramatically changing the way we communicate, the way we shop, the way we learn and, quite frankly, great parts of the way we live our lives. Artificial intelligence and exponential increases in computing power are forcing firms to re-examine how they do business.

The financial services industry is no exception. Digitalisation has already left bustling stock exchange floors in demise. High-frequency trading is increasingly shaping market dynamics. And in the future, thousands of financial analysts may be replaced with robo-advisors.

The financial industry is often the industry spearheading technological change. Distributed ledger technologies (DLT) are a case in point. They have applications well beyond finance. The diamond industry, for example, is using digital ledgers to track and record their assets. But it is the financial sector, and payments in particular, where progress is arguably moving fastest.

Financial institutions and market infrastructures worldwide are exploring DLT for payments and post-trading.[2]

The World Food Program uses a blockchain-based system to handle payments for food aid in Jordan.[3]

Central banks, as both overseers and operators of payment systems, and as sole issuers of banknotes, cannot afford to ignore these disruptive trends.

The central banking community, and the Bank for International Settlements' Committee on Payments and Market Infrastructures (CPMI), which I chair, and the Markets Committee chaired by Jacqueline Loh, are keeping a close eye on how promising technologies, such as DLT, may serve the wider public.[4]

This is not just a philosophical discussion. Although cash still reigns supreme in the vast majority of countries, it may be sidelined sooner rather than later.

If cash were to disappear, trust in the currency, a key public good, would be dependent on the creditworthiness of private entities. With bitcoin and other crypto assets we have seen large and unpredictable price swings and outright cyber heists that may expose people to the risk of losing their savings; this demands that central banks take these risks seriously.

Were central banks to issue their own digital currencies, people would be able to hold a central bank liability comparable to cash, without the risks associated with commercial money.

However, as things stand today, the possible adverse financial stability implications of introducing central bank digital currencies call for the greatest caution[5], while the underlying DLT that would enable these digital tokens to be introduced are still immature, costly to maintain and possibly prone to vulnerabilities.

For example, current crypto assets still fail to ensure clear and legally certain settlement finality[6], which is a necessary condition for a safe and efficient payment system, as emphasised by the Principles for Financial Market Infrastructures (PFMI) issued by the CPMI and the International Organization of Securities Commissions (IOSCO).

In fact, the predecessors of the CPMI under the chairmanships of Hans Meyer and Wayne Angell spent the better part of a decade getting finality right for interbank payment systems.[7]

Up until the 1990s, the risk that net settlement positions could be unwound meant that the failure of a single bank could lead to a cascade of failures.[8]

This systemic risk was one of the main motivations for introducing real-time gross settlement (RTGS) systems around the world. In other words, one has to wonder if uncertainty of finality is a price worth paying for any payment system.

Given these prevailing flaws, I believe central banks should pursue a two-track strategy.

First, they should continue to study new technologies closely and experiment and engage with the industry, whether fintech or techfin.

In the case of the ECB, we have already established a DLT infrastructure within the EU central bank community, which currently serves, first and foremost, as a learning tool. We have also teamed up with the Bank of Japan on the Stella project – a series of studies on the potential use of DLT for financial market infrastructures.[9]

Remaining on top of technological developments also means that, in the CPMI, we need to constantly take the pulse of our existing international standards. But so far, it is fair to say that the PFMI have proven flexible enough to accommodate technological change, be it through complementary guidance – on cyber for example – or through high-level strategies, such as on wholesale payments fraud, as I will explain later.

The second part of the strategy central banks should pursue entails drawing on less-disruptive existing technologies to make our current payment systems, which are convenient and have earned public trust, more efficient and safer.

At the current juncture, this essentially means doing three things:

1. making retail payment systems instant and available 24/7;
2. modernising our RTGS systems; and
3. enhancing cyber resilience.

Let me briefly touch upon each of these three issues, starting with retail payment systems.

Making retail payment systems instant and available 24/7

Today an increasing number of non-bank payment service providers are entering the domestic payments business, sometimes offering faster payments than the banks they are competing with.

Instant payment solutions can significantly increase the speed of retail payments.[10]

With instant payments, funds are settled with finality and are available for use by the recipient within seconds, 24 hours a day, seven days a week, 365 days a year.

Since bitcoin transactions take, on average, about 15 minutes to validate, and even bitcoin enthusiasts acknowledge that this type of settlement cannot be considered reasonably irrevocable before at least one hour has passed, instant payments may render large parts of the alleged benefits of crypto assets redundant.

Instant payment solutions have been implemented, or are in the process of being developed, in many countries across the world. Here in Singapore, the launch of FAST ("Fast and Secure Transfers") has resulted in a fundamental renewal of the payments infrastructure, with significant benefits for both merchants and customers.[11]

Later this year, the ECB will launch the TARGET Instant Payment Settlement (TIPS) service. In a currency union, instant payment solutions are not just about fostering innovation and improving customer convenience. They are also about promoting further financial integration among Member States.

Indeed, in the euro area, where different legal frameworks and customer habits prevail, there is always a risk of new fragmentation arising from the development of national or closed-loop solutions which are not interoperable. To counter this risk, the European payments industry is now launching a truly pan-European instant payments scheme.

TIPS therefore not only has the potential to help better prepare incumbents for the challenges arising from digital giants, such as Alibaba, Apple and Google, who are integrating payment services into their ecosystems, it also has the potential to be a catalyst for spurring progress in two old failings of our current system: cross-border retail payments and financial inclusion.[12]

Cross-border payments not only allow shoppers to easily buy goods online from overseas, but also allow foreign workers to send money home, supporting financial inclusion and development. However, these payment channels are generally much slower, less transparent and far more expensive than domestic ones.

Improvements here are the best way of rising to the challenges arising from currently unsafe crypto assets. I believe this should be a key priority for international action.

Modernising real-time gross settlement systems

This brings me to my second point, the modernisation of our RTGS systems. Their names imply that these systems are already fast. They settle transactions between financial market infrastructures, central banks and credit institutions in real time.

But these systems are often built on legacy technologies, sometimes dating back to the 1980s, and have been created to meet local needs for participants.

Since then, however, the financial system has become truly global, with banks increasingly

operating across borders and time zones through participation in multiple payment systems. A key element of many RTGS system modernisation projects is therefore implementing a messaging standard that works across the globe.

Of course, migrating from a legacy payment standard incurs costs. So, as with any other technological upgrade, it is important that a critical mass moves towards the new standard.

The Eurosystem is leading by example here.

We are implementing the ISO 20022 standard and offering multi-currency functionalities in our infrastructures. In the near future, both payment and securities settlement services will also undergo a technical and functional consolidation. Specifically, we will roll out a new RTGS system with enhanced functionalities and optimised liquidity management for the participants. The new service is scheduled to go live in November 2021.

Cross-border interoperability is just one area where progress can be made. Extending access to our RTGS system to regulated non-bank payment service providers is another avenue that promises to make our current systems fit for the future.

Fintechs are challenging the traditional way payments are made. Some of them offer valuable and safe services to customers. Wider access by these new non-bank payment service providers to central bank payment systems can spur further digital innovation and enhance financial stability by increasing the amount of final settlements conducted in risk-free central bank money. And it would once more reduce the appeal of crypto assets that, if not adequately regulated, may endanger financial stability should they become more widely used over time.

So, overall, there are good reasons to continue to work on improving our current market infrastructures. By embracing innovation and modern technologies, and by promoting inclusion and common standards, I am confident that we will be able to meet the growing expectations that consumers and stakeholders have of the evolving role of today's payment systems.

Enhancing cyber resilience

One of these expectations also relates to safety. As we are extending operating hours, allowing for more access and increasing interoperability, there will be larger "attack surface" in the system. The most efficient and fastest systems are useless if they are not bulletproof, if they can be hacked easily or if they expose consumers to disproportionate risks.

This brings me to the third point I mentioned at the beginning of my remarks – the need to make our current systems safer against the rising number of cyberattacks.

Cyber incidents are becoming much more frequent and increasingly sophisticated – to the point that they now pose a critical threat to market infrastructures and the entire financial ecosystem. This is why the modernisation of our systems must go hand-in-hand with increasing their cyber resilience.

Failure to adequately protect against cyberattacks may have far-reaching repercussions. Take wholesale payment systems as an example. A breakdown of these systems, even if only temporarily, would threaten financial stability, endanger the provision of liquidity by central banks and jeopardise the implementation of monetary policy.

This is also why G7 finance ministers and central bank governors recently took part in a simulation of the day after a major cyber incident in the financial sector. This exercise showed that a major cyber incident would require an internationally coordinated response, and highlighted areas where the G7 Cyber Expert Group could help address potential coordination issues, including areas beyond the traditional reach of regulators, such as third-party providers.[13]

In short, wholesale payment systems are for financial markets what electricity is for households. Anyone who has read Ted Koppel's illuminating *Lights Out* will understand what I mean.[14]

To help protect our systems, the CPMI and IOSCO published guidance on cyber resilience for financial market infrastructures (FMIs) already back in June 2016.[15]

The guidance offers recommendations for measures that FMIs should take to anticipate, withstand, contain and rapidly recover from cyberattacks.

On top of this, last month the CPMI issued a strategy for reducing the risk of wholesale payments fraud.[16]

The strategy aims to galvanise wholesale payment systems, network messaging providers, banks, overseers and supervisors to work together in strengthening the security of the financial ecosystem and its endpoints, all of which are being increasingly exploited by adversaries.

CPMI member central banks are committed to acting as a catalyst for effective and coherent operationalisation of the strategy within and across jurisdictions and systems. We will monitor progress throughout this year and next to determine the need for further action.

At the ECB, we have recently accelerated our efforts to put these initiatives into practice and to strengthen our cyber resilience more broadly. More specifically, earlier this year we did four things:

- We introduced the cyber resilience oversight expectations, which set out detailed best practices to operationalise the CPMI-IOSCO guidance. These expectations are now being finalised following a public consultation.
- We established the Euro Cyber Resilience Board for pan-European Financial Infrastructures, a forum that brings together high-level FMI representatives, service providers and authorities with the aim of raising awareness of common cyber challenges and acting as a catalyst for joint initiatives and solutions.[17]
- Our third initiative was introducing a European Framework for Threat Intelligence-Based Ethical Red Teaming (TIBER-EU), which supports FMIs and other financial entities in conducting the highest level of cyber resilience testing in a multi-jurisdiction and multi-authority context.[18]
- And finally, we adopted the aforementioned CPMI wholesale payments security strategy as the competent authority for two wholesale payment systems in the euro area – TARGET2 and EURO1.

All of these efforts are multilateral and predicated on strong cross-country collaboration. Some of our initiatives are pan-European, but others, such as TIBER-EU, are entity-agnostic, meaning that they can – and will – be used to harmonise processes not only for FMIs and other financial entities within Europe but also beyond.

Conclusion

Let me conclude.

The multilateral efforts I have just described reflect the growing recognition by both industry participants and regulators that we should see the global payment system for what it really is: an essential global public good whose integrity is increasingly being challenged by malicious cyberattacks and fraud attempts by individuals. In the future, it may also be challenged by adverse spillovers of otherwise well-intended government actions meant to protect data privacy and national security. Such spillovers may create new fault lines across the system.

To better understand these spillovers and to guard against fragmentation, we need strong multilateral cooperation more than ever. Let's work together to make our payment systems faster, cheaper and safer – and let's shield them from the sound and fury of politics.

Thank you.

---

[1] I would like to thank Elin Amundsen, Takeshi Shirakami and Morten Bech for their contributions to this speech. I remain solely responsible for the opinions contained herein.

[2] See Committee on Payments and Market Infrastructures (2017), *Distributed ledger technology in payment, clearing and settlement. An analytical framework*, Bank for International Settlements, February.

[3] See Bank for International Settlements (2018), *Cryptocurrencies: looking beyond the hype*, Annual Economic Report, Chapter V, June.

[4] See Committee on Payments and Market Infrastructures and Markets Committee (2018), *Central bank digital currencies*, Bank for International Settlements, March; and Cœuré, B. and Loh, J. (2018), "Bitcoin not the answer to a cashless society", op-ed published in the Financial Times, 13 March.

[5] See Committee on Payments and Market Infrastructures and Markets Committee (2018), op. cit.

[6] See also Bank for International Settlements (2018), op. cit.

[7] See, for example, Group of Experts on Payment Systems of the central banks of the Group of Ten countries (1989), *Report on netting schemes (Angell Report)*, Bank for International Settlements, February; and Committee on Interbank Netting Schemes of the central banks of the Group of Ten countries (1990), *Report of the Committee on Interbank Netting Schemes of the central banks of the Group of Ten countries (Lamfalussy Report)*, Bank for International Settlements, November.

[8] This could happen, for example, due to "zero hour rules", a provision in the insolvency law of some countries whereby the transactions conducted by an insolvent institution after midnight on the date the institution is declared insolvent are automatically ineffective by operation of law.

[9] See ECB and Bank of Japan (2017), "Payment systems: liquidity saving mechanisms in a distributed ledger environment", a joint research project of the European Central Bank and the Bank of Japan – STELLA, September.

[10] See also Committee on Payments and Market Infrastructures (2016), *Fast payments – Enhancing the speed and availability of retail payments*, November.

[11] See Menon, R. (2016), "An Electronic Payments Society", keynote address at the Sim Kee Boon Institute Conference on FinTech and Financial Inclusion, 19 August.

[12] See Committee on Payments and Market Infrastructures (2018), *Cross-border retail payments*, February. The report sets out a holistic view of cross-border retail payments to analyse the market and identify issues and challenges. Also see Committee on Payments and Market Infrastructures and the World Bank Group (2016), *Payment aspects of financial inclusion*, April. This report outlines guiding principles to help central banks and other stakeholders achieve effective financial access and broader financial inclusion.

[13] See G7 Cyber Expert Group (2017), "Fundamental elements for effective assessment of cybersecurity in the financial sector", 20 October.

[14] Koppel, T. (2015), *Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath*, Broadway Books.

[15] See Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions (2016), *Guidance on cyber resilience for financial market infrastructures*, June.

[16] See Committee on Payments and Market Infrastructures (2018), *Reducing the risk of wholesale payments fraud related to endpoint security*, May.

[17] See Cœuré, B. (2018), "A Euro Cyber Resilience Board for pan-European Financial Infrastructures", introductory remarks at the first meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt, 9 March.

[18] See ECB (2018), *TIBER-EU FRAMEWORK – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming*, May.