Decentralised financial technologies

Report on financial stability, regulatory and governance implications

6 June 2019

The Financial Stability Board (FSB) is established to coordinate at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations under the FSB's Articles of Association.

Contacting the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert

Follow the FSB on Twitter: @FinStbBoard

E-mail the FSB at: fsb@fsb.org

Table of Contents

Page

Decentralised financial technologies

Executive summary

Many types of financial service providers are incorporating new technologies that could decentralise the financial system. The decentralisation of financial services refers to the elimination – or reduction in the role – of one or more intermediaries or centralised processes that have traditionally been involved in the provision of financial services. In some instances it refers to the decentralisation of risk-taking away from traditional intermediaries. This already takes place through capital markets, but could be extended more widely, including to the provision of credit and insurance. In other cases it can also involve the decentralisation of decision-making and record-keeping.

It is impossible to predict with certainty the future scope or degree of decentralisation in the financial system. Applications that decentralise along all three of these dimensions (risk-taking, decision-making, and record-keeping) have yet to achieve economically significant scale. That said, technologies that facilitate decentralisation along one or two of these dimensions may, over time, have a noticeable economic impact. There are already examples emerging of decentralisation in payments and settlement, capital markets, trade finance and lending.

The application of decentralised financial technologies – and the more decentralised financial system to which they may give rise – could benefit financial stability. It may also lead to greater competition and diversity in the financial system and reduce the systemic importance of some existing entities.[1] At the same time, the use of decentralised technologies may entail risks to financial stability.[2] These include the emergence of concentrations in the ownership and operation of key infrastructure and technology, as well as a possible greater degree of procyclicality in decentralised risk-taking. New uncertainties concerning the determination of legal liability and consumer protection may also affect public trust in the financial system. Recovery and resolution of decentralised structures may be more difficult.

These issues may pose challenges for financial regulatory and supervisory frameworks, particularly those that currently focus on centralised financial institutions. A more decentralised financial system may reinforce the importance of an activity-based approach to regulation, particularly where it delivers financial services that are difficult to link to specific entities and/or jurisdictions. Certain technologies may also challenge the technology-neutral approach to regulation taken by some authorities. These concerns could continue to be the subject of further consideration by authorities. Regulators may also wish to engage in further dialogue with a wider group of stakeholders, including in the technology sector, that have had limited interaction with financial regulators to date. This should help avoid the emergence of unforeseen complications in the design of decentralised financial technologies at a later stage.

---

1 See FSB (2019), "FinTech and market structure in financial services: Market developments and potential financial stability implications", February, pp. 1, 4 and 17 for a discussion of the impact of technology on competition and financial stability.

2 The FSB has previously concluded that FinTech in general, and crypto-assets – which are one application of DLT – do not currently pose risks to global financial stability. See FSB (2017a), "Financial Stability Implications from FinTech: regulatory and supervisory issues that merit authorities' attention", June; FSB (2018a), "Crypto-asset markets: potential channels for future financial stability implications", October. Both reports state that there is the potential for financial stability implications in the future depending on the scale of adoption of such innovations and other factors.

This report considers several forms of decentralisation in financial services and identifies technologies that are decentralising – or may in the future decentralise – financial activities. It makes a preliminary assessment of which financial services are beginning to, and may in the future, incorporate such technologies. The FSB's work in this area responds to a proposal made by the Japanese G20 Presidency, which was approved at the October 2018 FSB Plenary meeting.

1. Introduction

Financial technology (FinTech)[3] is changing many facets of finance. These include retail and wholesale payments, financial market infrastructures, investment management, insurance, credit provision and capital raising. Global investment in FinTech rose to a record US$112 billion in 2018.[4] Nascent technologies such as distributed ledgers, cloud services, big data, and artificial intelligence (AI) are being tested for a wide variety of financial operations, to make them faster, more robust and less costly.[5] Their impact on financial services could be broad, and their applications include the settlement of interbank payments and the verification and reconciliation of trade finance invoices. They may also play a role in executing, enforcing and verifying the performance of contracts.[6]

This report focuses on applications of technologies that may reduce or eliminate the need for one or more intermediaries or centralised processes *in the provision of financial services*.[7] These are termed *decentralised financial technologies*. Such technology can facilitate a move away from single entities that grant access to and validate transactions, towards the decentralisation of information recording (e.g. via distributed ledgers) as well as the process by which it is updated (e.g. consensus mechanisms). Technology is also facilitating the decentralisation of risk-taking and decision-making. For example, peer-to-peer (P2P) lending and insurance are, in places, shifting credit and other risks away from a single entity (e.g. a bank or an insurer) to individual savers (or pools thereof).[8] Entities that use these technologies

---

3 FSB (2017a). FinTech is defined as technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services.

4 KPMG (2019), "The Pulse of FinTech 2018", February; CB Insights (2019), "FinTech trends to watch in 2019", January.

5 Distributed ledgers are defined as a collection of data that is spread across multiple nodes and whose consistency is enforced by means of a distributed ledger technology. "Distributed" refers here to having multiple locations for data. This is related to, but not identical with the concept of decentralisation of record-keeping (see Section 2.1). See Annex 2 for definitions.

6 The report draws on some examples from specific private firms involved in FinTech. These examples are not exhaustive and do not constitute an endorsement by the FSB for any firm, product or service. Similarly, they do not imply any conclusion about the status of any product or service described under applicable law. Rather, such examples are included for purposes of illustration of new and emerging business models in the markets studied.

7 This disintermediation of established financial institutions and infrastructures is distinct from the more general impact technology is having on the structure of the financial system (e.g. through changes in cost structures, barriers to entry and competition). These issues have been considered in other FSB work on market structure so will not be considered here; see FSB (2019).

8 See IAIS (2017), "FinTech developments in the insurance industry", February.

may have no clear location or multiple locations across jurisdictions, some of which may change over time (e.g. via the flexible configurations of servers).[9]

The *technologies* underlying such applications may themselves be decentralised. Such technologies – for example distributed ledger technology (DLT), which can store information in a decentralised manner – are the focus of this report. But technologies that underlie decentralised provision of financial services need not, themselves, be decentralised. For example, cloud computing or technology based on AI and machine learning may be provided in a *centralised* manner, but still be used to provide *de*centralised financial services through online platforms.[10]

Bearing this distinction in mind, this report identifies specific technologies that enable the decentralisation of financial activity and assesses which financial services are beginning to see various forms of decentralisation. It also makes a preliminary assessment of the implications of these technologies for financial stability, and some issues this might raise for financial supervision and regulation.

This report responds to a request initiated by the Japanese G20 Presidency. To inform its preparation, a workstream of the FSB's Financial Innovation Network (FIN) held a series of discussions with the public and private sectors, relevant organisations and academics. These took place through conference calls and a workshop hosted by the Organisation for Economic Cooperation and Development (OECD) on 25 February.

2. Implications for the structure of the financial system and financial stability

2.1 Forms of decentralisation in financial services

There are a number of different types of decentralisation in financial services. These vary in the degree to which they affect different segments of financial services, but generally take three broad forms:

- Decentralisation of decision-making. This involves a move away from a single trusted financial intermediary or infrastructure towards systems in which a broad set of users is able to make decisions about whether and how to undertake financial transactions.
- Decentralisation of risk-taking. This involves the shift away from the retention of risk (e.g. credit and liquidity risk) on the balance sheets of individual traditional financial intermediaries towards more direct matching of individual users and providers of financial services.
- Decentralisation of record-keeping. This involves a move away from centrally held data and records, towards systems in which the ability to store and access data is

[9] It is important to note that in some cases, these organisations will still play some form of intermediary role, though it may differ from that played by currently established intermediaries.

[10] Decentralised technologies are an aspect of FinTech that has been the subject of previous work by the FSB. See CGFS and FSB (2017), "FinTech credit: market structure, business models and financial stability implications", May; FSB (2017b), "AI and machine learning in financial services: market developments and financial stability implications", November; and FSB (2018a, 2019) on crypto-assets, and FinTech and market structure.

extended across broader consortia of users. Verification of such data and records may also be more distributed, for example via consensus mechanisms.

Applications displaying all three forms of decentralisation – that is, full decentralisation of decision-making, risk-taking and record-keeping – seem unlikely to achieve an economically significant scale in the near term. Instead, the majority of existing applications instead retain forms of centralisation across one or two of these dimensions. This is for a range of reasons, most notably those around scalability (e.g. of "proof-of-work" consensus mechanisms)[11] and limits to the degree to which some underlying technologies can currently establish adequate trust, maintain accountability and handle disputes to the same extent as centralised bodies.[12] Nonetheless, there is the potential for greater decentralisation along each of these dimensions in the future.

2.2 Current examples of technologies that enable financial decentralisation

For this report, the FSB has focussed on two technologies that are currently enabling financial services to be provided in a more decentralised manner:

- Distributed ledger technology (DLT) enables the decentralisation of record-keeping. It does so by removing the need for a central ledger in which to record financial transactions. Various levels of decentralisation of record-keeping are possible. These vary from "permissionless" or public systems that are open to all users, to "permissioned" or private systems where a more limited consortium of users are able to read and/or write to a ledger.[13]
- Online peer-to-peer (P2P), or user-matching, platforms allow users (e.g. creditors and borrowers) to interact directly and decentralise their risk-taking and decision making, yet avoid the sort of search costs that might otherwise be incurred in the absence of a centralised intermediary (e.g. bank or insurance company). As a consequence, lending activities may migrate away from financial intermediaries.

In some cases, decentralised technologies are supported by existing and forthcoming ancillary technologies such as the analysis of big data and AI, 5G cellular communications, the Internet of Things (IoT) and edge computing.[14] These technologies vary in the degree to which they themselves are decentralised. But they can nonetheless lower the cost of, and barriers to entry around, functions traditionally carried out by financial intermediaries (e.g. the processing and communication of data).[15] They can therefore catalyse the decentralisation of financial activity.

---

[11] "Proof-of-work" is a mechanism typically used in permissionless DLT networks to validate changes on a ledger. It involves calculations that are hard for those requesting a change in a ledger to perform but easy for other participants to verify.

[12] These and other similar issues are discussed in Raphael Auer (2019), "Beyond the doomsday economics of "proof-of-work in cryptocurrencies", BIS Working Paper No 765.

[13] The Bitcoin and Ethereum blockchains are examples of the former; Ripple is an example of the latter. These examples are not exhaustive and do not constitute an endorsement by the FSB or its members for any firm, product, or service.

[14] Edge computing refers to computation that is physically close to where data are being used or generated, for instance close to physical sensors or devices in the IoT. See glossary in Annex 4.

[15] For a discussion of how digital technologies lower economic costs in specific areas, see Avi Goldfarb and Catherine Tucker (2019), "Digital Economics", *Journal of Economic Literature* 57(1), 3-43.

The large-scale adoption of some technologies – including those that are, in some respects, highly decentralised – may also involve maintaining some degree of centralisation. For example, DLT systems being developed for use in financial services vary in the extent to which they seek to distribute data and decentralise control over their modification. But a number of current successful applications in financial services involve permissioned systems that have verifiable controls in place to manage operational and other risks.

2.3 Which financial services are likely to be affected?

The extent of decentralisation is likely to evolve over time and in parallel with, or in reaction to, other developments in financial services.[16] The rate at which new technologies are adopted will depend on the efficiency gains offered by decentralised structures. It is too early to say how large any such gains may be, though they will likely vary significantly across applications.

In general, however, decentralised technologies might be less likely to be adopted where financial services are reliant on intermediaries to provide large-scale maturity or liquidity transformation or make use of private information to overcome information asymmetries.[17] Conversely, their adoption may be more likely when existing methods for delivering financial services incorporate a lower degree of intermediation or are more costly.

Some examples of financial services using decentralised technologies are:

- **Payments and settlements.** Service providers in this sector have already begun to incorporate decentralised technologies. For example, foreign exchange platforms that directly match end-users have begun to complement – and in some places replace – traditional interbank payment systems for retail cross-border payments. If decentralised payment and settlement systems achieve scale, this may result in decentralisation of record-keeping.
- **Trade finance.** This area may benefit from technologies that allow verification of information to take place in a decentralised manner. This is due to a lack of established infrastructure or trusted intermediaries through which to verify information between stakeholders. DLT might enable participants from different sectors – for example finance and freight shipping – to interact and share information in a more easily verifiable and decentralised manner.
- **Capital markets.** The tokenisation of securities – that is, the digital representation of traditional assets using DLT – has the potential to further decentralise capital markets. Smart contracts might become more widely applied and provide an opportunity to further automate certain financial services such as settlement and custody, which are activities that are currently undertaken by traditional financial intermediaries.[18]

---

[16] See FSB (2017a), pp. 16, 21-22.

[17] For a broader discussion on the factors influencing the adoption of blockchain, see Christian Catalini and Joshua S. Gans (2016), "Some Simple Economics of the Blockchain", NBER working paper No. 22952, and Matt Higginson, Marie-Claude Nadeau and Kausik Rajgopal (2019), "Blockchain's Occam Problem", McKinsey and Company Insight, January.

[18] Smart contracts are algorithms (typically operating in a DLT environment) that automate the performance of contracts. In some contexts the term may also mean a contract which is partly instantiated by computer code. See example ISDA and Linklaters (2017), "Whitepaper Smart Contracts and Distributed Ledger – A Legal Perspective". See also David Yermack (2017), "Corporate Governance and Blockchains," *Review of Finance* 21(1): 7–31.

- **Lending.** Online lending platforms (and other similar technologies) make lending decisions without relying on conventional financial intermediaries. Such platforms typically carry out credit scoring directly on a granular basis, sometimes making use of novel sources of data on borrowers (such as social networks).

These examples are discussed further in the case studies in Annex 1.

2.4 Potential benefits and risks for financial stability

The application of decentralised financial technologies may reduce some of the financial stability risks associated with traditional financial institutions and intermediaries. For example, the growth and/or dispersion of financial service providers could increase diversity in the financial system and reduce the concentration of service providers. Some decentralised technologies could reduce the reliance on existing intermediaries to channel short-term funding into lending, thereby reducing solvency and liquidity risks arising across their balance sheets.

The degree to which these financial stability benefits are realised is likely to depend on how decentralised technologies affect the structure of financial services and the financial system more generally. The potential implications for financial stability may depend on (i) the degree of decentralisation to which these technologies gives rise; and (ii) the prevalence of their application in the financial services industry.

The use of decentralised financial technologies may also affect the nature and significance of operational risks. On the one hand, decentralised systems may – if appropriately secure – be more resilient to cyber risk than highly centralised systems, particularly in terms of the integrity of their record-keeping and service availability. This is due to how they disperse the recording of information, rather than concentrating it within a single node or system.[19] On the other hand, although the mechanisms through which many DLT systems record and agree information are highly decentralised, participants typically use identical technology and/or computer code. Advances in quantum computing could also threaten the cryptographic underpinnings of DLT.[20] This may increase vulnerabilities to operational and cyber risks.

Overall, decentralised financial technologies may raise the following risks to financial stability:

- **New forms of concentration risks** may arise in what might appear to be decentralised systems. In addition to using similar technology, many activities in larger DLT systems (e.g. ownership of the assets, control over source code, operation of the infrastructure, crypto-assets mining and code development) remain concentrated in a relatively small set of persons (e.g. software developers) or entities.

- **Greater procyclicality** could emerge, particularly in the supply of credit. For example, P2P matching platforms may exhibit larger and sharper swings in their provision of credit than existing financial institutions. This may apply particularly

---

[19] A node can be defined as the basic computing unit of a network. In the context of DLT, a node refers to a computer participating in the operation of a DLT arrangement. See CPMI (2017), "Distributed ledger technology in payment, clearing and settlement: An analytical framework", February, p. 2.

[20] See Divesh Aggarwal, Gavin K. Brennen, Troy Lee, Miklos Santha, Marco Tomamichel (2017), "Quantum attacks on Bitcoin, and how to protect against them", *Ledger,* [S.l.] v.3, Oct 2018, arXiv:1710.10377. Responding to such threats may require action that may be difficult to coordinate.

where lending decisions are automated and/or rely on novel data or models whose performance remains untested in a downturn (see case study 4 in Annex 1).[21]

- **Diffused or unclear responsibility and accountability** may arise where the allocation of liability in a more decentralised financial system may be unclear. Such legal risk may be particularly problematic in systems that are permissionless or where participants remain anonymous, and around liabilities arising from smart contracts.[22]
- **Recovery and resolution challenges** may arise, particularly where current approaches to the recovery and resolution of financial institutions are reliant on centralised record-keeping and claims on market participants whose identity and location is known.
- **Other operational and legal risks** may also arise, particularly in permissionless systems that involve large networks of anonymous users. Technologies such as DLT that rely on algorithms (e.g. proof-of-work) to achieve consensus might be vulnerable to adversarial dynamics in which certain actors seek to 'verify' fraudulent transactions.[23] This might also frustrate the process of agreeing settlement finality in the case of decentralised payment and settlement systems.

If the cumulative effects of – and interaction between – these risks were to cause market participants to lose confidence in financial markets, this may also increase risks to financial stability. They may allow the build-up of risks in parts of the system that cannot easily be monitored. There may also be a risk of regulatory arbitrage if financial services that are provided in a decentralised manner may not be (or may only partially be) subject to regulation, particularly where this differs between jurisdictions.

Decentralised financial services might also be less responsive to certain official sector interventions that have previously been used to remedy threats to financial stability. For example, liquidity facilities offered by central banks – including those offered as part of their role as lender-of-last-resort – have traditionally been granted to regulated financial institutions operating through traditional centralised structures, rather than decentralised technologies. Greater use of decentralised financial technologies might reduce the efficacy of these or other services provided by central banks. It might also prompt their redesign in order to make them interoperable with decentralised financial technologies.[24]

3. Issues concerning financial regulation and governance

Significant use of decentralised financial technologies may have implications for the effectiveness and enforceability of current regulatory frameworks, particularly where the execution of supervisory and oversight mandates focuses on the presence of centralised decision-making entities (e.g. financial intermediaries). A more decentralised financial system

21 See CGFS and FSB (2017).

22 See for example, Lexology (2018), "A Foreboding View of Smart Contract Developer Liability", November.

23 One such mechanism for doing so is a "51% attack" in which an actor assembles sufficient computing power on a network to give the appearance having verified a fraudulent transaction via proof-of-work.

24 See, for example, discussion in Bank of England (2018), "Real-time Gross Settlement (RTGS) Renewal", September.

may reinforce the importance of an activity-based approach to regulation, particularly where it delivers financial services that are difficult to link to specific entities and/or jurisdictions.

Some of these issues may also prompt further consideration of the governance arrangements around decentralised financial technology, which could have implications for financial regulation, supervision and stability. Such arrangements generally provide processes to set objectives and determine means for achieving and monitoring performance against them.[25]

As such, this section of the report considers issues related to the governance of technological development, and the activities of businesses (both incumbent and innovators) and users of technology, which could have implications for financial regulation and financial stability. Annex 2 explores some of the challenges to governance raised by these technologies.

3.1 Potential implications for public policy

Decentralised financial technologies have a range of potential implications for public policy. In particular they could:

- **Be used to avoid regulation or engage in misconduct**: decentralised financial technologies have the potential to anonymise users and to enable them to offer financial services that, while coming under the purview of regulatory authorities, may lessen the effectiveness of current financial regulation and facilitate misconduct.[26]
- **Raise issues around enforcement**: regulatory enforcement following misconduct or data breaches may be more difficult with decentralised decision-making or record-keeping across multiple players.
- **Increase jurisdictional uncertainty:** the use of decentralised financial technologies could increase the degree to which financial services are provided across borders. Such technologies may also increase the ease and speed with which providers of financial services are able to change their locations, including in response to actions of authorities. Some crypto-asset trading platforms have, for example, moved their headquarters between jurisdictions in response to regulatory actions.[27]

Decentralised financial technologies may also mean that financial activities can be executed without a clear geographic location. For example, decentralised autonomous organisations may in the future use autonomous systems to control access to assets and resources, without relying on individuals located in a given jurisdictions.[28] This may challenge authorities' enforcement of relevant jurisdictions' laws and regulations.

There are also factors that may mitigate the potential effects of such cross-border migration of activities. For instance, even though a trading platform may move its operations outside a jurisdiction, any offers or sales of securities to residents of that jurisdiction are typically still

[25] See CPMI and IOSCO (2012), "Principles for financial market infrastructures", Principle 2.

[26] For an example related to P2P lending, see Fabio Braggion, Alberto Manconi and Haikun Zhu (2018), "Can Technology Undermine Macroprudential Regulation? Evidence from Peer-to-Peer Credit in China", January.

[27] Andrea Tan (2018), "Another Giant Crypto Exchange Is Moving to Tiny Malta", Bloomberg, April.

[28] See Aaron Wright and Primavera De Filippi (2018), *Blockchain and the Law*, Cambridge, MA and London: Harvard University Press, Ch. 9.

subject to the laws of the jurisdiction. In many cases, individuals remain responsible for the operation or deployment of software and for key functions within organisations providing certain aspects of decentralised technologies, or within consortia facilitating their deployment; this, too, could present a means by which authorities could regulate activities.[29] Finally, cross-border cooperation is already taking place with regard to supervision and some enforcement actions including on deployments of decentralised financial technologies.[30]

3.2 Areas of further assessment

As part of the G20 discussion, authorities may wish to consider the implications of decentralised financial technologies for:

- **Financial regulation and regulatory approaches:** for example, by considering the appropriateness, applicability and effectiveness of current financial regulations for financial businesses and activities based on decentralised financial technologies, and exploring ways to address potential regulatory gaps and financial stability concerns. Some jurisdictions may consider new ways of administering or enforcing regulation. This might include embedding restrictions in computer code, the implications of which have yet to be explored under legal theory.[31]
- **Financial supervision:** for example, by assessing how decentralised financial technologies could lead to gaps or overlaps in supervisory systems, and updating or modifying data reporting processes accordingly (such as with respect to supervising activities on distributed ledgers).

  New data could also provide supervisors with greater and timelier insights into potential systemic risks, through the real-time tracking of asset ownership and shifting of associated risks. That said, acquiring and analysing such data may prove to be resource intensive for both market participants and regulators.[32]
- **The proportional and consistent application of regulation of decentralised financial technologies**: for example, by continuing to regulate decentralised financial technologies in a manner proportional to the risks they pose. In places, the application of decentralised financial technologies may present challenges to the technology-neutral approach to regulation taken by some authorities.

Decentralised financial technologies are likely to continue to evolve rapidly. Early liaison between regulators and a wider group of stakeholders might help ensure that regulatory and other public policy objectives are considered in the initial design of technical protocols and applications. This should help limit the emergence of unforeseen complications at a later stage.

---

29 Wright and De Filippi (2018), p. 155.

30 For example, see SEC (2017), "*SEC Emergency Action Halts ICO Scam*", December.

31 See Aaron Wright and Primavera De Filippi (2017), "Decentralised Blockchain Technology and the Rise of Lex Cryptographia", July; and De Filippi and Wright (2018).

32 For example, changes in the share of trading activity of a particular jurisdiction can serve as an early signal that the trading activity may flow to other jurisdictions, which could potentially have both financial stability and regulatory implications; see Monetary Authority of Singapore, (2018), "Financial Stability Review".

In particular, decentralised financial technologies could see greater provision and use by entities that have had limited interaction with financial regulators to date. Authorities may therefore wish to enhance their dialogue and cooperation with a wider group of stakeholders, including software developers, the engineering community, as well as businesses, academia, and other relevant stakeholders such as investors, consumers and users. This would help to assess the opportunities and risks of decentralised financial technologies. It would also enable supervisors to continue to address emerging issues promptly and use supervisory resources effectively while at the same time remaining open to the benefits of financial innovation.

Annex 3 gives some examples of multi-stakeholder approaches to governance that might be relevant to the governance of decentralised financial technologies.

Annex 1: Case studies

Case study 1 – Cross-border payments and settlements

Description of innovation

Cross-border payments are typically slower, costlier and more opaque than domestic payments. A single payment transaction often involves a significant number of parties, and typically settles through decentralised and complex correspondent banking networks that face well-known challenges around cost and customer due diligence.[33] Inefficiencies also arise from operations across different currencies, message formats, time zones and laws.[34]

A number of initiatives are using DLT in an effort to address some of the current challenges in correspondent banking and to develop alternative means of transferring funds across borders.[35] Such DLT applications vary in their degree of decentralisation. Permissioned (or restricted) DLT systems can retain record-keeping in a single entity, much as is the case with traditional payments. Some such "closed loop" systems are designed to internalise the market and liquidity risks of foreign exchange (FX) transactions, and maintain a single ledger with proprietary message formats. Other configurations decentralise decision-making, risk-taking and/or record-keeping. Table 1 below highlights some of the different configurations that systems based on DLT may take.

Potential economic and financial stability implications

Initiatives that use DLT in cross-border payments typically harness its ability to reduce complexity and cost, improve the speed of reconciliation, and strengthen transaction transparency. Whereas risk management, record-keeping and decision-making in traditional cross-border payments take place in a loose (relatively decentralised) network of correspondent banks, initiatives using DLT increase speed and efficiency by automating reconciliation, reducing operational costs or increasing the availability of "know-your-customer" (KYC) data.[36]

There remain, however, uncertainties around operational and security aspects of DLT, as well as questions concerning settlement finality, legal underpinnings and governance arrangements.[37] A potential lack of interoperability of some DLT payment systems with existing processes and infrastructures might also decrease overall financial efficiency.

Some initiatives (including those initiated by major commercial banks) also reportedly make use of systems based on DLT to create either a "bridging currency" for foreign exchange or to generate – and then allow customers to transfer – tokens sometimes representing assets that are

---

[33] CPMI (2016), "Correspondent banking", July. See also FSB (2018b), "FSB action plan to assess and address the decline in correspondent banking: Progress report to G20 Summit of November 2018", November.

[34] CPMI (2018), "Cross-border retail payments", February.

[35] Dong He, Ross Leckow, Vikram Haksar, Tommaso Mancini Griffoli, Nigel Jenkinson, Mikari Kashima, Tanai Khiaonarong, Celine Rochon and Hervé Tourpe (2017), "Fintech and Financial Services: Initial Considerations", *IMF Staff Discussion Note 17.*

[36] Capgemini (2019), "Will Blockchain enable digital nirvana for supply chain management?", January.

[37] CPMI (2017).

held in custody. Some regulatory sandboxes report positive outcomes in speed and transparency as well as cost reduction of payments made using this method, but also report significant issues concerning the volatility, liquidity and availability of the bridging crypto-assets used.[38] Moreover, consumers' direct use of crypto-assets for cross-border payments could undermine anti-money-laundering (AML) or combating-the-financing-of-terrorism (CFT) efforts. As such, current use is minimal or concentrated in niche groups.[39] There has also been a recent proliferation in stablecoins (digital tokens backed by fiat currency deposits or commodities, or supported by decentralised algorithms).[40] However, use of such coins might create commingling, fraud or wrong-way risk in case of bankruptcy of the operator, as those coins tend to be issued by the operator itself or by a related party.

Potential legal/regulatory considerations

Important legal considerations for any arrangement using DLT to make cross-border payments include: (i) the clarity and enforceability of the legal basis for any payment (including settlement finality); (ii) potential conflicts of laws between jurisdictions; and (iii) the clarity of the rights and obligations of the participants.[41] Additional consumer and investor protection issues could arise where DLT is used to create a crypto-asset or digital token, including those concerning the legal status of crypto-assets that do not represent a claim on any legal entity or individual.[42]

Furthermore, some new arrangements for cross-border payments in certain jurisdictions may not be subject to the same regulatory, supervisory and oversight requirements as traditional payment service providers.[43] Technology and governing rulesets should be transparent to the authorities that would supervise or oversee DLT solutions, and, for a cross-border arrangement, this could require the cooperation of multiple authorities.

Potential governance considerations

The governance of arrangements that use DLT to share information and maintain ledgers may require careful planning at the outset. Change and incident management – as well as enforcement decisions – pose particular challenges, particularly in more decentralised and/or permissionless systems. Broad governance considerations include: (i) arrangements to support sound decision making, risk management, incident and emergency response as well as management oversight; (ii) identification of the different stakeholders and their responsibilities (e.g. multiple entities could maintain a ledger or its underlying software); and (iii) the clarity of decision making mechanisms.

---

[38] FCA (2017), "Regulatory sandbox lessons learned report", October.

[39] Christian Barontini and Henry Holden (2019), "Proceeding with caution – a survey on central bank digital currency", *BIS Papers No 101*, January.

[40] See Blockchain.com (2019), "The state of stablecoins", February; CCAF (2018), "2nd Global Crypto-asset Benchmarking Study", December.

[41] CPMI (2017).

[42] Work is currently underway at the CPMI. See FSB (2018c), "Crypto-assets – Report to the G20 on work by the FSB and standard-setting bodies", July.

[43] CPMI (2018).

Potential configurations of DLT arrangements

Table 1

<table>
<tr><th>Description of arrangement</th><th>One entity maintains and updates the ledger (for example, a typical FMI)</th><th>Only approved entities can use the service; entities can be assigned distinct restricted roles</th><th>Only approved entities can use the service; entities can play any role</th><th>Any entity can use the service and play any role</th></tr>
<tr><td>Operation of the arrangement</td><td>Single entity</td><td colspan="3">Multiple entities</td></tr>
<tr><td>Access to the arrangement</td><td colspan="3">Restricted</td><td>Unrestricted</td></tr>
<tr><td>Technical roles of nodes</td><td colspan="2">Differentiated</td><td colspan="2">Not differentiated</td></tr>
<tr><td>Validation and consensus</td><td>Within a single entity</td><td>Within a single entity or across multiple entities</td><td colspan="2">Across multiple entities</td></tr>
</table>

Source: CPMI (2017).

Case study 2 – Capital markets (tokenisation)

Description of innovation

Tokenisation can be defined as the representation of traditional assets – e.g. financial instruments, a basket of collateral or real assets – on DLT.[44,45] Well-publicised examples of tokenisation include the recent issuance of "bond-i" on DLT by the World Bank,[46] a project to tokenise high quality collateral from Deutsche Börse,[47] and the reported tokenisation of a property in Manhattan.[48] This case study focuses only on tokenisation activities that represent traditional financial securities ("tokenised securities") [49] or interests in assets.

Ownership of tokenised securities can be recorded on a blockchain that uses a smart contract to set the terms of the tokenised security or asset. Smart contracts use computer protocols to execute, verify, and constrain the performance of a contract. In doing so, they can automate decision-making, by allowing self-executing computer code to take actions at specified times and/or based on reference to the occurrence (or non-occurrence) of an action or event.[50] Where tokenisation is used as part of the process of raising capital, it can decentralise such activity away from traditional financial intermediaries.

Potential economic and financial stability implications

Potential benefits

As with other online offerings of securities, tokenisation can allow companies to issue securities that could be traded with a broad investor base without the involvement of a traditional financial intermediary. This could shorten – and increase the transparency of – custody chains that are typically involved in traditional securities holdings.[51, 52] Online offerings of tokenised securities

---

44 There are a number of initiatives currently aiming at tokenising cash, including through so-called stablecoins. This case study does not consider the implications of these initiatives, many of which extend beyond use in capital markets.

45 Other examples of the application of decentralised financial technologies in capital markets include the tokenisation of securities – that is, the issuance of tokens that are securities but do not represent rights in an entity, and in that context the use of 'smart contracts' to set forth the rights of the token holders.

46 In 2018, the World Bank proceeded to issue short-term bonds worth AUD 110m using a private permissioned DLT as Proof of Concept. See World Bank (2018), "World Bank Prices First Global Blockchain Bond, Raising A$110 Million", August.

47 In January 2019, Deutsche Börse announced that the technical and regulatory set up of the solution, which aims to facilitate the efficient management of high quality collateral, was close to final.

48 In October 2018, it was reported that a Manhattan development worth over US$ 30m became the first property to be tokenised on Ethereum blockchain. See Rachel Wolfson (2018), "A First For Manhattan: $30M Real Estate Property Tokenized With Blockchain", Forbes.

49 Tokenised securities should not to be confused with security tokens, although the two are both subject to securities laws or regulatory jurisdictions. Tokenised securities are in essence securities, which happen to be represented on DLT. Security tokens are primarily digital tokens, which may have certain attributes of a security. Tokenised securities are likely to qualify as securities in the legal sense and hence to fall within the scope of existing financial securities rules, which may not be the case of security tokens in some jurisdictions. See https://www.coindesk.com/security-tokens-vs-tokenized-securities-its-more-than-semantics.

50 CFTC (2018), "A primer on smart contracts", CFTC Release number 7847-18.

51 Long custody chains generally increase the risk that investors may be unable to access their own securities - at least temporarily - due to operational issues or financial distress of a sub-custodian. That could possibly lead to - potentially systemic - liquidity problems for market participants.

52 Thomas Droll, Natalia Podlich and Michael Wedow (2016), "Out of sight, out of mind? On the risk of sub-custodian structures", *Journal of Banking and Finance* 68: 47-56.

may increase firms' access to funding and create additional investment opportunities for investors. They could also enhance the liquidity of certain assets (e.g. unlisted SME shares or physical assets), by making them fractionalised[53] and thus more easily tradable. Tokenisation could also increase speed with which transactions settle and streamline cumbersome back-office processes. This could also reduce counterparty and operational risks.

Potential negative implications

The use of DLT could in some cases entail new forms of concentration and cyber risks (see Section 2.4). For example, new forms of concentration risks could arise in relation to so-called "miners" or "validating nodes", on which the completion of transactions on DLT is dependent. Where DLT is used as the sole means of recording changes in ownership,[54] the integrity of tokenised securities (and companies whose securities are represented by such tokens) could be compromised were such validating nodes to cease operating or change their operations materially. This risk might arise through how mining activities are currently highly concentrated in the case of public DLTs,[55] and through how private DLTs tend to rely on a small number of validating nodes. Similarly, where tokenised securities are traded on secondary market trading platforms, concentration risk could stem from custodial wallet providers or other centralised trading platforms that hold private keys on behalf of their clients and have been subject to cyber incidents.[56,57] Market integrity issues could also arise in relation to the transparency that is embedded in DLT and the role of miners or validating nodes and a potential lack of settlement finality (where the risk of "forking" in ledgers could create uncertainty over the status of the ledger as a record).

If tokenisation were adopted more broadly, it is possible that it might create an appearance of liquidity in assets that are inherently illiquid. This may also have negative implications for financial stability. In particular, risks could arise where there is a liquidity mismatch between the token and the underlying asset, or where investors have limited understanding of products packaged into a token. For example, the tokenisation of real estate (were it to become widespread over a large geographic area) might threaten investor confidence in certain areas were investors to overestimate the degree to which the underlying assets could be sold at (or close to) prevailing market prices during periods of stress.

---

[53] This means that they are able to be issued as fractional interests representing less than one unit of the underlying asset.

[54] While ownership records of traditional securities may involve DLT, in many cases, the transferability of the securities and the recording of ownership may remain independent of (or recorded alongside) DLT ownership records.

[55] Reports indicate that the five largest mining pools control c.60% of Bitcoin's hash rate, see Blockchain, "Hashrate Distribution An estimation of hashrate distribution amongst the largest mining pools" (accessed 15 April 2019). One pool alone reportedly has a 40% market share on Ethereum. See Gastracker.io, "Top Miners on Ethereum Classic, by avg. hashrate for past 24 hours" (accessed 15 April 2019).

[56] A private key controls the disposition of assets at a given DLT address. Losing a private key is equivalent to losing the right to dispose of assets, hence safekeeping of the private key is of great importance.

[57] Losses as a result of cyber incidents at trading platforms exceed US$ 3.3bn. See Jean-Pierre Landau (2018), "Les crypto-monnaies", July. See also Ciphertrace (2018), "Cryptocurrency Anti-Money Laundering Report", Q3. These incidents could increase as tokenisation and smart contracts become more widespread. At the same time, awareness of these risks and in turn, use of more secure private key storage mechanisms (e.g. cold wallets and seed phrases), is also likely to increase over time. Already, centralised crypto-exchanges keep an average of 87% of the clients' funds in cold storage, see Garrick Hileman and Michel Rauchs (2017), "Global Cryptocurrency Benchmarking Study", Cambridge Centre for Alternative Finance.

Potential legal/regulatory considerations

It is important that regulators continue to assess the degree to which current rules provide adequate safeguards in the case of tokenisation. Issuers of tokenised securities should also properly consider applicable regulation. This could include issues around: (i) settlement and settlement finality and the role of miners and validating nodes (which may fall outside of existing regulations); (ii) the safekeeping of private keys and the interactions with the existing custody/safekeeping rules; and (iii) the security of the underlying DLT protocol and codes, including in relation to smart contracts. To the extent that tokenisation widens the potential investor base for a variety of products, effective application of investor protection rules may similarly require careful consideration.

Tokenisation may also raise other specific legal issues, depending on its precise form. These might include the role and liabilities of the party originating the tokenisation and the existence of a legal claim on the underlying asset for investors.

Potential governance considerations

The shift towards smart contracts and self-executing code could also create specific governance and accountability issues. These include the question of whether – and to what extent – software developers, system operators or users can be held responsible if contracts do not function as intended.

Case study 3 – Trade finance and insurance

Description of innovation

Trade finance typically requires financial institutions to make credit assessments and perform payments – often through paper-based exchange and validation of documents – across multiple participants. Streamlining such highly fragmented cross-border activity is often hampered by the lack of trust between parties, particularly when they are situated in different jurisdictions. Paper-based processes can also make trade finance prone to fraud, such as that arising from duplicate financing and forged documents.

The private sector, often in partnership with regulators, has proposed a number of DLT applications[58] that aim to decentralise record-keeping and facilitate the more efficient flow of information between parties involved in trade finance.[59] DLT has the potential to reduce the risk of fraud and duplicate financing, as well as improving operational efficiency, by allowing for verification of information by its users rather than by a single trusted party. It also has the potential to increase the speed of transactions and reduce the need for paper reconciliation. The application of DLT to trade finance was in one instance reported to reduce the time take for the exchange of a letter of credit from 5-10 days to 24 hours.[60]

Over US$ 9 trillion in trade finance was processed globally in 2017. Some estimates suggest this leaves a substantial (US$ 1.5 trillion) quantity of potential trade finance transactions that could not be met by traditional technology, and which might be facilitated by the application of DLT.[61, 62]

Potential economic and financial stability implications

Validated information on trade receivables via DLT could allow banks to make more accurate credit assessments. It might also open up new revenue streams for financial institutions by increasing the viability of transactions for which a lack of verifiable information previously made them uneconomic. Smaller companies might be able to secure working capital at lower cost because banks would incur lower costs in verifying their documentation.[63]

Conversely, the application of DLT in this area might also introduce new dependencies on third parties. New forms of concentration risks could arise, as multiple institutions rely on the same

---

[58] See e.g. Monetary Authority of Singapore (2017), "Singapore and Hong Kong launch a joint project on cross-border trade and trade finance platform", November.

[59] Decentralisation of decision making also takes place where smart contracts are also used to settle trade payments automatically based on defined triggering events (see https://www.etradeconnect.net). Although DLT could in theory achieve decentralisation of risk-taking in trade finance (for example through factoring or invoice discounting arrangements sold directly to retail customers), this has yet to be seen in practice.

[60] See HSBC (2018), "HSBC and ING execute groundbreaking live trade finance transaction on R3's Corda Blockchain platform", 14 May.

[61] International Chamber of Commerce (2018), "Global trade – securing future growth", May.

[62] World Economic Forum (2018), "Trade Tech – A New Age for Trade and Supply Chain Finance", September.

[63] For examples of applications providing easier access for SMEs, see Carlo R.W. De Meijer (2018), "We.Trade on Blockchain: Yes We Can!", Finextra. Hong Kong Monetary Authority (2017), "Cross-border Trade Finance", November.

technology provider or data source. This could lead to a single point of failure, at least in the case of permissioned systems.

The information recorded on DLT-based trade finance platforms can also be created or modified by diverse groups of participants many of which are governed by laws other than or in addition to existing financial regulation. A lack of clear and adequate internal controls and governance of technology could create operational, reputational, and other risks for financial institutions. Non-compliance with AML/CFT regulations by any one participant could have a material financial impact and possible reputational consequence on all other participants. It may also be unclear which party is accountable for unexpected errors or fraud if responsibility of maintaining correct information on DLT is diffused. Recovery and resolution may also be challenging given the diversity of participants. Finally, the risk of forged transactions could still arise unless all trade transactions are recorded on the same DLT network (or different networks share and synchronise information in a timely manner).[64]

Potential legal/regulatory considerations

Trade finance transactions using DLT might increase cross-border interconnectedness because they involve participants in different sectors or at different geographic locations. Although this issue is not unique to new decentralised technologies, particular legal and compliance risks could arise around the question of which laws and jurisdictional authority is applied to a given set of transactions. For example, the enforceability of a digitally signed contract may vary across jurisdictions, as might the available tools to resolve disputes. Consensus on the designated location may be more difficult to be reached if the network scales up quickly. The novelty and hence unclear legal value of smart contracts in many jurisdictions could lead to disputes.

Potential governance considerations

The possible absence of a central party to govern a DLT platform and assume liability could pose challenges to the overall governance and management of the network. Most existing cases establish a joint venture between participants to assume the liability of operating the platform and decide on the governance model. Yet given the diversity of participants, reaching consensus on updates to software and protocol standards, admission of new participants, and changes in administration and operational procedures could become more difficult and time consuming.

64 Hong Kong Monetary Authority (2018), "The launch of eTradeConnect and the Collaboration with we.trade", October.

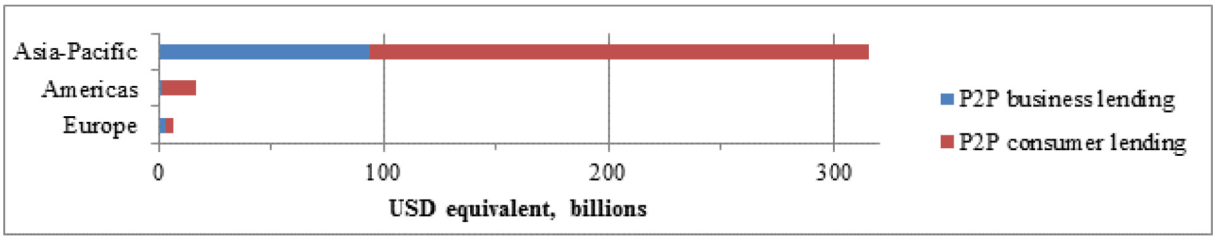
Case study 4 – Peer-to-peer lending

Description of innovation

Peer-to-peer (P2P), or user-matching, lending platforms allow retail investors and institutions to lend directly or indirectly to consumers and businesses. As such, they are a form of FinTech credit.[65] Such platforms can allow borrowers and lenders to interact directly or indirectly yet avoid search costs that might otherwise be incurred in the absence of a centralised intermediary.

Such platforms may facilitate decentralisation of both risk-taking and decision-making. Investors can bear the credit risk of underlying loans, and (at least some simple) platforms allow investors to choose how their funds are invested. Other platforms have more sophisticated business models that incorporate some centralisation of decision-making. They may, for example, structure investments so that multiple investors underpin a single loan, or set prices or select portfolios in such a way that investors can achieve some given target rate of return. Other platforms also work with banks to originate loans themselves. Either way, lending platforms typically retain (centralised) record-keeping and administration responsibilities.

P2P lending platforms have been established in many countries. The largest market is in China, where P2P platforms have become a significant source of funds for small firms and consumers.[66] The chart below illustrates peer-to-peer business and consumer lending volumes in 2017.



Source: Cambridge Centre for Alternative Finance

In many jurisdictions, P2P lending remains a small share of total lending. In the UK, for example, annual growth rates (over 80% in 2015) have recently slowed considerably. In China, volumes have recently declined as a number of platforms have exited the market.[67]

Potential economic and financial stability implications

P2P lending provides an alternative source of financing for households and small businesses. As such, it has the potential to improve access and competition, as well as lower concentration in credit provision. This is particularly the case in jurisdictions where consumer or small business lending is concentrated in a few dominant financial institutions. Barriers to entry are typically lower than for bank-based lending models, meaning that P2P lending platforms may also foster financial inclusion. In the United States, for example, the Department of the Treasury

---

65 For more information on business models, see Committee on the Global Financial System (CGFS) and FSB (2017), "FinTech credit: Market structure, business models and financial stability implications", May.

66 Stijn Claessens, Jon Frost, Grant Turner and Feng Zhu (2018), "Fintech credit markets around the world: size, drivers and policy issues", BIS Quarterly Review, September.

67 See Claessens et al. (2018).

has discussed their potential to enhance access to credit, and has made recommendations to eliminate certain regulatory constraints.[68]

P2P lending platforms may be vulnerable to mispricing of risk, particularly as they have generally yet to witness a full financial cycle.[69] Information asymmetry and principal-agent problems that apply between platform providers, issuers and investors may also lead to mispriced risk.[70, 71] Lending platforms are generally subject to indirect network effects, with both issuers and investors benefiting from increased participation.[72] They may therefore have an incentive to underestimate the risk underlying the projects they offer to investors. Greater access to credit may also lead to more procyclical credit provision, including the weakening of lending conditions in an upswing and a reduction in credit extension in times of stress.

Such a potential deterioration in lending standards might be particularly problematic when platforms are not required to retain any risk on their own balance sheet. Some platforms have started to bundle and consolidate loans and sell them on to third parties in the form of asset-backed securities.[73] This might also lead to an increase in interconnectedness and regulatory arbitrage on part of bank lenders. [74]

Where P2P lending platforms are not within the scope of prudential regulation, this may limit the effectiveness of credit-related macroprudential policy measures.[75] There also remain significant data gaps around P2P lending and FinTech credit in general.[76] Analysis of data from one major P2P lending platform in the United States suggests its lending base is comprised predominantly of institutional lenders that rely on the platform to assess the risk of loans. [77]

---

68 U.S. Department of the Treasury (2018), "A Financial System that Creates Economic Opportunities: Nonbank Financials, FinTech, and Innovation", July.

69 For a discussion of the financial cycle, see Stijn Claessens, M. Ayhan Kose, and Marco Terrones (2012), "How do business and financial cycles interact?", *Journal of International Economics* 87(1): 178-90; Moritz Schularick and Alan Taylor (2012), "Credit booms gone bust: Monetary policy, leverage cycles, and financial crises, 1870-2008", *American Economic Review* 102(2): 1029-61.

70 Jensen and Meckling (1976) describe the issue of principal–agent problems as a situation where 'one or more persons (the principal(s)) engage another person (the agent) to perform some service on their behalf which involves delegating some decision making authority to the agent. If both parties to the relationship are utility maximisers, there is good reason to believe that the agent will not always act in the best interests of the principal'. See Michael C. Jensen and William H. Meckling (1976), "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure", *Journal of Financial Economics* 3(4): 305–60.

71 For a discussion of asymmetric information and pricing strategies for crowdfunding platforms, see Paul Belleflamme, Nessrine Omrani and Martin Peitz (2015), "The Economics of Crowdfunding Platforms", *Information Economics and Policy* 33: 11–28.

72 See, for example, Jean-Charles Rochet and Jean Tirole (2003), "Platform Competition in Two-Sided Markets", *Journal of the European Economic Association* 1(4): 990–1029.

73 Eleanor Kirby and Shane Worner (2014), "Crowd-Funding: An Infant Industry Growing Fast", IOSCO Staff Working Paper.

74 Kirby and Worner (2014) note that "investing in uncollateralised loans, via peer-to-peer lending platforms, may be a way for banks and other large institutional investors to circumvent capital requirements or other regulatory requirements".

75 CGFS and FSB (2017); Fabio Braggion, Alberto Manconi and Haikun Zhu (2018), "Can Technology Undermine Macroprudential Regulation? Evidence from Peer-to-Peer Credit in China", January.

76 See FSB (2019), "Global Report on Non-Bank Financial Intermediation 2018", February, pp. 68-72.

77 Tetyana Baluk and Sergei Davydenko (2018), "Reintermediation in FinTech: Evidence from Online Lending", August.

This P2P platform therefore entails little decentralisation: institutional lenders have essentially selected a new centralised decision-making intermediary to replace the role of a loan officer.

Potential legal/regulatory considerations

P2P lending platforms are generally operated by a legal entity that exists within clear jurisdictional boundaries. Although fully decentralised systems could be proposed in the future, including those whose location is unclear, the FSB is not aware of any such systems currently extending credit.

The regulatory frameworks applying to P2P platforms vary by jurisdiction.[78] Regulations introduced to date tend to focus on investor protection, rather than specifically referring to financial stability. The complexity of some P2P business models could, for example, result in harm to investors, at least where the risks involved are not clearly and accurately disclosed. Appropriate investor disclosures can therefore increase the resilience of the P2P lending sector in a downturn, by reducing the likelihood of investors suffering unanticipated losses.[79]

Potential governance considerations

To date, the role of legal entities in operating platforms, regulatory measures applied to such entities and limited cross-border P2P lending mean that such platforms do not raise significant issues in terms of governance of the financial system. This may change in future, if, for example, cross-border supervisory and regulatory cooperation does not keep pace with developments in this sector.

---

[78] See CGFS and FSB (2017); Claessens et al. (2018); FSB (2019).

[79] See, for example, UK Financial Conduct Authority (2018), "Loan-based ('peer-to-peer') and investment-based crowdfunding platforms", Consultation Paper, July.

Annex 2: Clarifying governance issues related to permissionless distributed ledgers

According to the Principles for Financial Market Infrastructures (PFMIs), governance provides the processes through which an organisation sets its objectives, determines the means for achieving those objectives, and monitors performance against them.[80] A number of current successful applications in financial services involve permissioned systems that have verifiable controls in place to manage operational and other risks. Permissionless DLT could, however, shift many roles away from singular legal entities. This may raise new challenges for regulators that have typically approached governance by focussing on traditional financial intermediaries. The rest of this annex explores some of the challenges to good governance raised by permissionless DLT.

New form of governance in permissionless distributed ledger platforms: control embedded in code

Distributed ledgers introduce new processes through which transactions may be executed and verified. They do so by using computer code to execute, verify, and record financial transactions. Such computer code embodies rules that determine who obtains access to the system and related data, and governs how such rules are enforced (for example through smart contracts and defined consensus protocols). Existing permissionless DLT systems have, however, not developed code or other mechanisms to achieve many of the aims that are incorporated within the governance arrangements of financial institutions, FMIs, and other financial intermediaries. For example, existing implementations of permissionless DLT systems typically do not incorporate explicit rules to meet public policy objectives – including, for example, combatting money laundering or ensuring financial stability.

Potential DLT governance issues

For permissionless systems there are at least three potential governance issues.

The first concerns the control of changes to DLT systems, which has particular implications for their scalability. All software systems need to be continuously updated to address bugs, security issues and changes in the operating environment. DLT systems may also require changes to the size of their information blocks and other parameters such as the strength of their encryption. Such updates can in principle change any aspect of the software, including record-keeping and ownership rules.[81] There may therefore be a need for regulators and users to better understand the process governing such rule changes, and how they are prioritised, developed, implemented and controlled.

The second potential issue is that permissionless DLT systems may experience disagreements between participants that could lead to multiple disparate versions of the same system emerging.

---

[80] The PFMI set out principles against which financial market infrastructures (systemically important payment systems, central securities depositories, securities settlement systems, central counterparties, and trade repositories, collectively FMIs) can be assessed. Principle 2 (Governance), states that an FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.

[81] Vili Lehdonvirta and Robleh Ali (2016), "Governance and Regulation", Ch. 3, in UK Government Chief Scientific Adviser (ed.), *Distributed Ledger Technology: Beyond Blockchain.*

This could arise from how such systems have been developed in a manner that lacks central authority and allows virtually any actor to participate in the process of records verification and technological development. Permissionless access may allow actors involved in making decisions to be more opaque and/or to behave opportunistically. Doing so may serve their own interest at the expense of other users or wider stakeholders. Substantive disagreements between decision makers may lead to "hard forks" that have been a feature of some permissionless blockchains.[82] A potential disorderly proliferation of DLTs could also lead to unintended market fragmentation and threaten consumer and investor protection.

Third, there may be a potential need to balance users' desire for privacy (or secrecy) with other concerns, such as investor and/or consumer protection and visibility/auditability of transactions. Therefore the characteristics and available means of audit should be properly discussed.

Suggestions for authorities to consider in relation to the governance of DLT systems

It is important that public authorities consider various dimensions of the governance of permissionless DLT systems, particularly where they may be used to conduct regulated financial activities. This could include greater engagement with a broader group of stakeholders. Such engagement may also help broaden understanding of the purpose and functions of financial regulation, and help spur the development of technological tools for advancing its aims. Given the potential issues above, regulators might wish to deepen their understanding of the dynamics of, and motivation for, the development of technical code such as open source software. An early assessment of the issues of interoperability among distributed ledgers may have significant benefits for competition, concentration, cyber resilience, financial stability and regulation. One possible outcome might be to develop a common approach to standardising and coordinating systems, similar to that developed in the case of the internet (e.g. shared protocols and domain directories).

Second, entities such as virtual asset service providers and wallet providers now facilitate access to some permissionless systems. Rules applied to such entities could mitigate some risks, such as that of money laundering. Recommendations from international standard-setting bodies such as the Financial Action Task Force (FATF) are being revised in light of these challenges and may result in strengthening the governance of DLT systems.[83] That said, a single entity or person in control of such systems may be difficult to identify. Authorities may therefore wish to assess, or continue to assess, the applicability of existing regulations based on the functions or activities performed by entities or persons participating in such a system.

---

[82] A 'hard fork' is a bifurcation in a distributed ledger whereby separate and irreconcilable ledgers are created (usually due to an unresolved disagreement among developers or other actors such as miners associated with a distributed ledger).

[83] FATF (2019), "Mitigating Risks from Virtual Assets".

Annex 3: Examples of international organisations relevant to the governance of technology

There are a number of international organisations active in the governance of technology and related operations. Discussion between relevant regulators and these organisations could provide insights as to how to approach governance issues concerning decentralised financial technologies. These organisations involve cooperation between multiple stakeholders.

In particular, several global collaboration mechanisms have developed to address specific tasks:[84]

- The Internet Engineering Task Force (IETF) is a not-for-profit community that develops open standards of internet-related technologies. The internet has an almost permissionless nature, and as such there is a strong need to ensure its interoperability. The IETF takes an open process approach whereby interested person can participate, know what is being decided and make their voice heard on issues. Its technical work is done in Working Groups that span several specific subject areas. Within Working Groups, participants take an approach called "rough consensus and running codes", which means that they make standards based on their combined engineering judgement and real-world experience in implementing and deploying specifications. Other notable characteristics of IETF are that all participants represent themselves but not the organisations to which they belong.
- The Internet Corporation for Assigned Names and Numbers (ICANN) is a not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the internet secure, stable and interoperable. It is responsible for coordinating the maintenance and procedures of several databases related to the namespaces and numerical spaces of the internet, and ensuring the network's stable and secure operation. Within ICANN, government agencies and international governmental organisations form a Government Advisory Committee (GAC) that provides advice to the ICANN Board. The GAC itself does not participate in the decision making process. The contract regarding certain stewardship functions between ICANN and the National Telecommunications and Information Administration of the United States Department of Commerce ended on 1 October 2016. This initiated the formal transition of ICANN's functions to a global multi-stakeholder community.
- The International Organisation for Standardisation (ISO) is an international standard-setting body with representatives from various national standards organisations. Founded on 23 February 1947, ISO promotes worldwide proprietary, industrial and commercial standards. It is headquartered in Geneva and works in 164 countries. It was one of the first organisations granted general consultative status with the United Nations Economic and Social Council. In particular, ISO Technical Committee (TC) 307 is working to develop a suite of DLT standards on foundations (WG 1), security, privacy and identity (WG 2), smart contracts and their applications (WG 3), Governance (WG 5), use cases (SG 2) and interoperability (SG 7).

[84] This annex does not intend to give example of specific directions financial regulators should pursue, but rather offers examples of multi-stakeholder governance in areas outside of finance.

- The International Telecommunication Union (ITU) is a specialised agency of the United Nations that is responsible for issues concerning information and communication technologies. ITU has been an intergovernmental public-private partnership organisation since its inception. Its membership includes 193 Member States and around 800 public and private sector companies and academic institutions. It also includes international and regional telecommunication entities, known as Sector Members and Associates, which undertake most of the work of each Sector.
- The World Wide Web Consortium (W3C), founded in 1994, is an international community that develops protocols and guidelines to ensure the long-term growth of the World Wide Web. Its standards define key aspects of how this technology functions. Membership of the W3C is open to all types of organisations and individuals, and as of April 2019 comprised of 450 members. It also has a full-time staff, but not a single physical headquarters (instead it is hosted by four other institutions). The W3C has a number of working groups, including a Web Payments Working Group, whose mission is to make payments made via the Web easier and more secure.

Annex 4: Glossary

The following definitions are drawn from existing work by the FSB, Basel Committee on Banking Supervision (BCBS), BIS Committee on the Global Financial System (CGFS), Committee on Payments and Market Infrastructures (CPMI), Financial Action Task Force (FATF), BIS Markets Committee (MC), International Organization of Securities Commissions (IOSCO), and the glossary of the report of the Economic Consultative Committee (ECC) ad hoc group on digital innovation.

- **Artificial intelligence:** the theory and development of computer systems able to perform tasks that traditionally have required human intelligence.
- **Big data:** A generic term that designates the massive volume of data that is generated by the increasing use of digital tools and information systems.
- **Cloud computing:** an innovation that allows for the use of an online network ('cloud') of hosting processors so as to increase the scale and flexibility of computing capacity.
- **Distributed ledger:** a collection of data that is spread across multiple nodes and whose consistency is enforced by means of a distributed ledger technology (see next).
- **Distributed ledger technology (DLT):** a means of recording information through a distributed ledger. These technologies enable nodes in a network to propose, validate, and record state changes (or updates) consistently across the network's nodes – without the need to rely on a central trusted party to obtain reliable data.
- **Edge computing:** computation that is physically close to where data are being used or generated, for instance close to physical sensors or devices in the Internet of Things.
- **FinTech:** technology-enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on the provision of financial services.
- **FinTech credit:** credit activity facilitated by electronic platforms whereby borrowers are obtain funding directly or indirectly from individual or institutional lenders. These entities are commonly referred to as "loan-based crowdfunders", "peer-to-peer (P2P) lenders" (see below) or "marketplace lenders". Such electronic platforms can facilitate a range of credit obligations, including secured and unsecured lending, and non-loan debt funding such as invoice financing.
- **Governance:** processes through which objectives are set, the means through which such objectives are met, and performance against them monitored. In this paper governance refers to both the governance of technological development, the activities of business, and users of technology, all of which could have implications for financial regulation and stability.
- **Hard fork:** a bifurcation in a distributed ledger whereby separate and irreconcilable ledgers are created (usually due to an unresolved disagreement among developers or other actors such as miners associated with a distributed ledger).
- **Internet of Things:** software, sensors and network connectivity embedded in physical devices, buildings, and other items that enable those objects to: (i) collect and exchange data and (ii) send, receive and execute commands.

- **Node:** the basic computing unit of a network. In the context of DLT, a node refers to a computer participating in the operation of a DLT arrangement.
- **Peer-to-peer (P2P) lending:** a type of FinTech credit platform, where individuals or businesses are matched directly or indirectly for lending purposes.
- **Stablecoin:** a crypto-asset designed to maintain a stable value relative to another asset (typically a unit of currency).
- **Tokenisation:** the practice of issuing digital tokens.