THE INVESTMENT ASSOCIATION

CMS law·tax·future

The Investment Association

Tokenised funds series Paper 5 - Operational & Cyber Resilience Implications

October 2022

The Investment Association in partnership with CMS

Tokenised Funds – Operational & Cyber Resilience

About this paper

This is the fifth paper in the IA tokenised funds series in collaboration with CMS. In this paper we explore the implications for firms running tokenised funds from an operational and cyber resilience perspective. The previous papers are available here.

1. Operational Resilience – Regulatory Framework

As modern businesses increasingly embrace change and conduct activities digitally, firms are continually presented with new risks. This is especially true in the financial services industry, with increased investor uptake of digital platforms, emerging new technologies and complex regulatory requirements. Adding in the context of increased industry discussions of tokenised funds, it is therefore necessary for firms to consider new operational and cyber risks as well as preparing strategies to limit damage and recover swiftly from incidents.

A regulatory priority for a long time, the Financial Conduct Authority ("**FCA**"), Prudential Regulation Authority ("**PRA**") and the Bank of England collaboratively introduced a policy framework in March 2021[1] to increase resilience within financial institutions and financial market infrastructure through supplementing pre-existing requirements[2]. Defining operational resilience as the "ability of firms and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions" [3], the regulators' intention was to protect both the UK financial sector and wider UK economy from the impact of inevitable operational disruptions, acknowledging the increasing complexity of technological issues and increasing risk of hostile cyber-attacks. The total elimination of risks posed by cyberattacks, service outages and data breaches is not possible, so the focus from the regulators is on limiting the potential consumer and economic harm caused by these risks rather than proposing a 'zero failure' regime. This was noted by Megan Butler, FCA Executive Director of Supervision (Investment) who stated that "operational resilience is not about protecting the reputation of your firms or the reputation of the industry as a whole. It is about preventing operational incidents from impacting consumers, financial markets and UK financial system"[4].

In a Statement of Policy on operational resilience,[5] the PRA expanded on this by stating that firms should be able to:

1. Prevent disruption occurring to the extent practicable;
2. Adapt systems and processes to continue to provide services and functions in the event of an incident;
3. Return to normal running promptly when a disruption is over; and
4. Learn and evolve from incidents and near misses.

The FCA and PRA have aligned their approach and generally require the same of firms. Firms must identify and define their important business services and establish testable resilience standards which are tested against.

---

[1] PRA PS6/21 'Operational resilience: Impact tolerances for important business services' (bankofengland.co.uk) and FCA 2021 PS21/3: Building operational resilience: Feedback to CP19/32 and final rules (fca.org.uk)
[2] Existing regulatory framework includes Principle 3 of the FCA's Principles for Businesses, SYSC and the PSRs 2017 and EMRs 2011
[3] FCA paper: CP19/32: Building operational resilience: impact tolerances for important business services and feedback to DP18/04 (fca.org.uk)
PRA paper: CP29/19 'Operational resilience: Impact tolerances for important business services' (bankofengland.co.uk)
[4] The view from the regulator on Operational Resilience | FCA
[5] Operational resilience | Bank of England

Firms must therefore demonstrate the ability to evaluate the impact of unexpected disruption caused by operational and technological risks which are relevant to individuals, firms and wider financial markets which depend on the provision of vital products and services. To do this, the FCA and PRA propose that firms:

- Identify which business services could harm consumers or the wider market if they were disrupted;
- Establish impact tolerances for vital business services and conduct tests to assess whether it is possible to remain within these impact tolerances when faced with potential disruptions;
- Conduct a 'mapping' exercise to identify individuals, technology and operational processes which are critical to a firm's service offering;
- Identify the potential to recover from risks effectively, noting where additional investment is needed; and
- Set up effective communication (internally and externally) in the event of service disruption.

The new rules and guidance came into force on the 31 March 2022. By then, firms must have:

- Identified important business services;
- Set their impact tolerances for the maximum disruption tolerable;
- Conducted mapping and testing to the required level of sophistication; and
- Identified vulnerabilities.

Firms have until 31 March 2025 to perform mapping and testing which demonstrate that they can remain within impact tolerances for every identified important business service[6].

It is important to recognise that the UK regulators hold firms responsible, and ultimately accountable, for their operational resilience, regardless of whether or not they rely upon third parties to support the delivery of their important business services. At the same time, the UK regulators recognise that there is increasing reliance by firms on third-party services to support their operations and that no single firm can adequately monitor or manage the systemic risks that certain third parties pose to the regulators' objectives, including UK financial stability, market integrity and consumer protection, stemming from concentration in the provision of some third-party services.

For this reason, in addition to the operational resilience regime for firms, the UK is following in the footsteps of Europe with plans to oversee third parties designated as "critical third parties" or "CTPs" by HM Treasury. The Financial Services and Markets Bill (FSM Bill), which was put before Parliament on 20 July 2022, sets out a proposed statutory framework for managing systemic risks posed by CTPs and the UK regulators subsequently released a discussion paper (DP) on 21 July 2022 which sets out how the supervisory authorities could use their proposed powers in the FSM Bill to assess and strengthen the resilience of services provided by CTPs to firms, thereby reducing the risk of systemic disruption.

The UK regulators have emphasised that the measures proposed across the DP would seek to complement, and not replace, firms' own responsibilities to manage potential risks to their operational resilience, including as a result of the impact of the failure or disruption of a third party, thus reinforcing the message that firms' ability to understand and plan for their dependencies on third parties forms a critical piece of the operational resilience puzzle.

The IA has identified a number of important business services and we have released a paper detailing our findings[7]. Subsequently, the IA has published further member guidance on governance, impact tolerances, scenario testing and self-assessment documents[8].

---

[6] https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience
[7] https://www.theia.org/sites/default/files/2020-06/Important Business Services - Member Guidance Jun20.pdf
[8] https://www.theia.org/operational-resilience

CMS recently commissioned a technology risk survey of over 500 international businesses. The survey respondents from the financial services sector expressed a high degree of confidence in their ability to manage the risks associated with both current and future technologies. Over 90% of respondents were confident that the executives in the business had a good understanding of the risks and a similar proportion considered that their in-house legal teams had the requisite levels of knowledge and expertise to manage risks. However, the survey data also suggests that this confidence does not translate into effective risk management, with a large proportion of the respondents failing to maintain standard risk management policies, such as an incident response plan to manage a cyber breach, a crisis plan for technology failure or maintaining a regulatory risk register.

2. Operational resilience implications for tokenised funds

As discussed in our first paper in this series, tokenised funds are subject to the same regulatory regime as traditional funds due to the FCA's "technology neutral" approach. Tokenised funds would therefore face similar regulatory risks and requirements as any traditional fund. However, due to the unique nature of tokenised funds there are several additional operational resilience implications. This includes issues relating to novelty, general risks and benefits associated with blockchain technology, considerations around blockchain integrity and potential issues associated with blockchain intermediaries.

a) Novelty and lack of real-world examples

Tokenisation, and tokenised funds in particular, are relatively new developments. This makes tokenised funds an exciting concept with a range of anticipated benefits, however it also means that many of the potential operational risks are primarily theoretical. This could make adherence to the new operational resilience regulatory framework challenging, as firms will need to establish impact tolerances and conduct mapping exercises to establish what exact risks are presented and how best to recover from and mitigate them. In this fast-evolving area, technology often outstrips regulation so any future tokenised funds would need to quickly assess potential cyber threats posed by the new operational model.

Recognising the need to test innovative new market propositions before they are implemented on a broad scale, the FCA operates a Regulatory Sandbox. It is open to authorised and unauthorised firms that would require UK authorisation, as well as technology companies looking to provide innovative solutions for financial services[9]. This Regulatory Sandbox could provide an opportunity to pilot tokenised fund technology with FCA approval before rolling it out on a wider basis, allowing for some of the theoretical implications to be tested in practice in a limited manner under the regulator's supervision.

July 2018's Cohort 4[10], April 2019's Cohort 5[11] and July 2020's Cohort 6[12] of the Regulatory Sandbox featured organisations utilising blockchain and tokenisation. The FCA's focus for the latest Cohort, Cohort 7 was fraud and scam detection, vulnerable customer resilience and SME finance access. This is relevant but indirectly so to tokenised funds in the UK.

International examples are also rare. The Spanish financial supervisory bodies (Spanish Central, Comisión Nacional del Mercado de Valores and Directorate General of Insurance and Pension Funds) have announced a cohort of the Spanish equivalent of the FCA's Regulatory Sandbox. "Issuance and Custody of Tokenised Investment Fund Shares" was one of the projects, focusing on applying blockchain technology to the issuing of shares and the management of investment funds[13].

However, it currently remains difficult to anticipate the exact operational risks and opportunities that

[9] https://www.fca.org.uk/firms/innovation/regulatory-sandbox
[10] Regulatory sandbox - cohort 4 | FCA
[11] Regulatory sandbox - cohort 5 | FCA
[12] Regulatory sandbox - cohort 6 | FCA
[13] https://allfunds.com/en/blog/2021/05/14/allfunds-and-renta-4-join-forces-in-spanish-regulatory-sandbox-project-for-the-tokenization-and-custody-of-investment-funds/

tokenised funds present in a real-world setting due to the limited number of fully developed examples. It is therefore helpful to assess the operational and cyber resilience implications of the underlying blockchain technology that distinguish tokenised funds from traditional funds.

b) Blockchain-specific rewards and risks

Distributed ledger technology ("**DLT**"), and specifically blockchain technology (which is a type of DLT), has gained widespread traction across financial services. For instance, the International Swaps and Derivatives Association ("**ISDA**") has piloted the implementation of Common Domain Model ("**CDM**"), a "blueprint for how derivatives are traded and managed across the trade lifecycle"[14] which digitally represents trade events. The ISDA CDM has been introduced to create consistency and ensure that differing firms and platforms increase interoperability, which could lead to wider technological innovation due to the CDM's machine readable nature.

There are numerous advantages to using blockchain technology in financial services, some of which include:

1. **Instant settlements.** Settlements in the traditional financial system can currently take a significant amount of time, with some transactions taking approximately a week to settle. Blockchain technology significantly reduces transaction times, through its capability of settling transactions instantaneously (i.e. within minutes, or even seconds).
2. **Removal of fee-charging intermediaries.** Blockchain makes peer-to-peer transactions possible, which means that there may not necessarily be a need to engage intermediaries (for instance, custodian banks and clearers). This will likely reduce operational costs for financial institutions.
3. **Reduced counterparty risks.** As above, there are likely to be fewer parties involved in any one transaction. Additionally, the instantaneous nature of transaction settlements will remove the risk that a counterparty is not able to meet its obligations.
4. **Increased transparency and detailed audit trail.** The blockchain is effectively a transparent time-stamped ledger, which anyone (or at least authorised persons in a permissioned blockchain) should be able to view.

Notwithstanding its advantages, DLT can present some unique risks. The Joint Committee of the European Supervisory Authorities (including representatives from the European Securities and Markets Authority ("**ESMA**"), the European Insurance and Occupational Pensions Authority and the European Banking Authority ("**EBA**")) issued a report on "Risks and Vulnerabilities in the EU Financial System" in April 2017. The report identified that DLT "anchors cyber threats as a long term but rapidly evolving risk".[15] Another ESMA study published in the same year elaborates on these risks, highlighting that there are potential vulnerabilities in DLT systems surrounding key management and hardware access.[16] As with any outsourcing project, relying on one specific service provider can come with risks.

<u>Risks</u>

As with any new technology, there are of course security risks and issues surrounding blockchain technology. Below is a list of a few such security risks and issues:

1. **51% attacks.** This occurs when a single entity controls the majority of the blockchain's hash rate, which can result in network disruption.[17] This could ultimately exclude some transactions from taking place or lead to some transactions being modified or reversed. These attacks are unlikely but would be a key consideration when evaluating operational resilience.
2. **Vulnerable smart contracts.** Security issues when it comes to vulnerability in smart contracts include scenarios such as incorrect calculation of output token amounts (for instance, incorrect decimals handling and incorrect fee calculation).

[14] https://www.isda.org/a/z8AEE/ISDA-CDM-Factsheet.pdf
[15] Spring Joint Committee Risk Report (JC 2017 09).pdf (europa.eu) (pg 15)
[16] dlt_report_-_esma50-1121423017-285.pdf (europa.eu)
[17] https://academy.binance.com/en/articles/what-is-a-51-percent-attack

3. **Routing attacks.** These types of attacks take place when hackers redirect traffic from internet providers. As with a 51% attack, such attacks could cause the exclusion of some transactions from completing, or even partition a particular blockchain network in half.

Blockchain networks tend to fall under two categories: permissioned and permissionless. Permissionless blockchains are built on open-source technology, which means that anyone in the world has the capacity to access it to view any relevant information, or even be a participant node. Permissioned blockchains, on the other hand, only allow pre-authorised nodes to participate in the network and are generally not built open-source.

The open-sourced nature of permissionless blockchains such as the Bitcoin, Ethereum and Litecoin networks, means that they could theoretically be more susceptible to security risks. However, the bigger the blockchain, the harder it is to carry out an attack on it. Take for example a 51% attack – it would be extremely difficult for anyone, or even a collection of nodes to be able to harness enough computing power to control 51% of any one of these networks. Contrast this with permissioned blockchains, which are significantly more selective when it comes to which nodes are authorised to participate in/have access to the network. Whilst not necessarily aligned with an evangelist's vision of full-scale decentralisation, financial institutions generally work with permissioned blockchains to be able to control its operations more effectively, comply with any relevant regulatory obligations and maintain high levels of cyber-security.

c) Integrity of the blockchain

Blockchain is a nascent technology and remains open to significant refinement. It is therefore not unusual to find defective code within a network, with defective code generally being one of the bigger issues present in blockchain projects.

With defective code comes erroneous execution, as in the Singaporean case of *Quoine*,[18] where its system mistakenly allowed a trader to sell ether at an inflated price. One of the questions considered in this case was whether the smart contract, being a decentralised and autonomous actor, could somehow be held liable in itself or whether it is prudent to look to a developer's intention when they developed and built a network. Whilst this case delves into some unanswered legal issues, the question of liability is relevant also to tokenised funds. Where code is wrongly executed in tokenised funds, the most likely scenario would be that the fund provider indemnifies its customer and then seeks to recover its losses from the applicable party. In this case, the customer is likely to want an indemnity from the fund provider, and in turn the fund provider may wish to obtain an indemnity from the blockchain developer. Given the questions raised in the case of *Quoine*, it is not unreasonable to think that it may be difficult to obtain the same.

A sensible way to mitigate and manage such risk is to carry out regular audits of blockchain code. This type of audit is effectively a manual review of any code to locate any defects or bugs within it. A key consideration for any firm looking to launch a tokenised fund is therefore to consider the frequency of any blockchain audits within a network.

d) Potential issues associated with blockchain intermediaries and automation

Tokenised funds have the potential to transform the roles of different firms and organisations that would previously be considered essential participants in traditional fund management. Some intermediaries may become obsolete if transactions can be automated. In some ways this could enhance operational resilience by having fewer organisations involved in tokenised fund management, however…

[18] B2C2 Ltd v Quoine Pte Ltd. [2020]

e) Lost keys and inability to remedy

A key concept behind blockchain is decentralisation. Blockchain uses asymmetric cryptography, offering users control and ownership over their information and data. To access the records stored on a particular user, individuals require a private key which must be noted. This puts quite a high degree of responsibility on the individual because if this key is shared with others then their records are at risk. If the key is misplaced or destroyed, then access to the assets is permanently lost. A fund provider may be unable to remedy this, as the decentralised nature of the blockchain would be undermined if human beings could step in to recover lost keys. Additionally, there is an increased risk of hacking associated with keys. If investors took note of their keys on an unencrypted computer system or if security measures were not sufficient, unscrupulous actors could take advantage by hacking and accessing shares.

Having a physical share register, which many traditional funds utilise, would also defeat the purpose of decentralisation. Regulators such as the FCA may ultimately be uncomfortable with the fact that ordinary retail investors may lose any record of or means of access to their shares, which poses some additional operational risk when considering the applications of tokenised funds in practice. Regulators may wish to request some sort of recovery mechanism, which is at odds with the decentralised nature of these funds.

3. Conclusion

Funds and the firms managing them must be aware of the requirements of maintaining operational resilience. It is a topic of general concern as financial institutions of all types continue to digitalise their front and back office. The leading digital and tokenised fund projects are up and running, and so it is an appropriate time for the risk management processes associated with these to clarify that they take account of the work done by regulators and the industry on operational and cyber resilience.

Tokenised funds series

This paper discussed operational and cyber resilience implications for tokenised funds, with other papers in the series covering a range of topics. We are keen to hear from members on what is important to them – contact us with requests and suggestions at john.allan@theia.org

Sam Robinson
Partner
Financial Services Regulation
T +44 20 7524 6836
E sam.robinson@cms-cmno.com

Yasmin Johal
Associate
Financial Services Regulation
T +44 20 7524 2623
E yasmin.johal@cms-cmno.com

Christopher Luck
Partner
Indirect Funds and Real Assets
T +44 20 7524 6294
E chris.luck@cms-cmno.com

Aidan Campbell
Partner
Regulated Funds
T +44 141 304 6112
E aidan.campbell@cms-cmno.com

Charles Kerrigan
Partner
Banking & Finance
T +44 20 7367 3437
E charles.kerrigan@cms-cmno.com

John Finnemore
Partner
Corporate
T +44 20 7524 6432
E john.finnemore@cms-cmno.com

Kushal Gandhi
Partner
Litigation
T +44 20 7367 2664
E kushal.gahdhi@cms-cmno.com

Phil Anderson
Partner
Tax
T +44 20 7524 6048
E phil.anderson@cms-cmno.com

Duncan Turner
Partner
TMIC
T +44 131 200 7669
E duncan.turner@cms-cmno.com

CMS
law·tax·future

THE
INVESTMENT
ASSOCIATION

The Investment Association

Camomile Court, 23 Camomile Street, London, EC3A 7LL

www.theia.org

Policy, Strategy & Innovation

@InvAssoc @The Investment Association