FNALITY GLOBAL PAYMENTS

RESILIENCE IN FNALITY GLOBAL PAYMENTS

THE FNALITY TEAM

FEBRUARY 2021

CONTENTS

ABSTRACT

Resilience is the ability to recover from disruptive events; it is a core characteristic of any successful organisation, ecosystem or society. Due to its systemic importance, regulators have put the resilience of the financial sector under particular scrutiny.

This paper describes resilience in the context of Fnality Global Payments' operational model and its underpinning Distributed Ledger Technology (DLT) infrastructure. Settlement is conducted and finalised on a peer-to-peer basis, making the settlement model much simpler and safer by removing the need for intermediaries, and with it associated operational complexity and risk exposures. DLT is a new technological paradigm, but the spectrum of risks to which it is exposed is the same as the risks faced by any centralised system in operation today. What is novel is the method for solving and mitigating these risks.

This paper also addresses organisational resilience. It has been noted by standards and regulatory bodies that having a culture that recognises the importance of security is vital, and that many organisations are finding that a traditional hierarchical structure is no longer fit for this purpose. While for many the solution is to automate processes - which can be efficient but brittle and difficult to re-design - Fnality's solution is to distribute decision making from the top of the organisation to the areas receiving relevant information in real-time, and thus to steer those decisions with collective purpose. Fnality's organisational design entails empowered, decentralised, cross-functional, fully autonomous teams that are aligned through consumer-led value streams in the context of Fnality's overall vision and strategy. They are therefore highly able to solve problems in an efficient, effective and resilient manner.

INTRODUCTION

A key objective of the Fnality Global Payments (FnGP) initiative is to deliver unprecedented levels of payments infrastructure availability and operational resilience. To achieve this, we harness distributed ledger technology (DLT), with its roots in the 'trustless' environment of cryptocurrencies, in the design and development of Fnality Payment Systems (FnPSs). This enables a simpler and more resilient, peer-to-peer settlement model.

We go one step further by also adopting an organisational design that replicates many of the resilience features of DLT and adds a learning and adapting capability. By building organisational resilience and not only operational resilience, FnGP reconciles two goals that often conflict in traditionally run organisations: achieving safety and soundness while maximising efficiency and cost effectiveness. This is what sets FnPSs apart; this is what will drive the future of global finance.

SECTION 1: RESILIENCE IN FINANCIAL MARKET INFRASTRUCTURE

Resilience, the ability to recover from disruptive events, is a core characteristic of any successful organisation, ecosystem or society.

In finance, the concept of operational resilience came to prominence following the September 11 terrorist attacks in 2001. The attacks focused regulatory attention on the interconnectedness of global financial markets and the need for key institutions to be prepared for disasters and crises, in minimising systemic disruptions to the global financial system.

While regulatory reforms in the aftermath of the global financial crisis of 2008 focused on improving financial stability through strengthening standards of prudential regulation and investor protection, more recently, regulators have returned their attention to ensuring that banks and financial market infrastructures (FMIs) appropriately manage the resilience of their business services.

The spotlight on resilience has been driven by three key factors:

- **Cyberattacks and operational errors:** Financial institutions today place significant reliance on complex information technology systems and communication networks in operating their businesses. High profile cyberattacks and operational errors, which have become increasingly prevalent, have underscored the vulnerability of financial institutions and their clients to cybersecurity and other operational risks.

- **Adoption of new technologies create execution risk:** The emergence of new technologies enable innovation (new products / services, new competitors) which can enhance consumer choice and encourage greater automation of operational processes. At the same time, the adoption of change within established business models brings with it a certain amount of execution risk.

- **Increasing market disruption events:** Recent market disruption events, in particular COVID-19, have pushed financial institutions to their limits in terms of the capabilities of their operations to cope with such adverse ‘black swan’ scenarios.

SECTION 2: OPERATIONAL RESILIENCE IN FNALITY GLOBAL PAYMENTS

Lael Brainard, member of the Board of Governors of the Federal Reserve System, noted that the biggest benefit of Distributed Ledger Technology (DLT) for payments, clearing and settlement may be resiliency:

"Distributed ledger technology may enable a network to continue to operate even if some of the nodes on the network are compromised because of the ability of the other nodes in the network to pick up the slack and continue processing transactions."[1]

If one of the main advantages of DLT is its resilience, and the resilience comes from having many alternative redundant services, operated by different stakeholders, implemented in diverse technologies, performing the tasks necessary for the system to function, it is important not to lose these benefits by introducing Single Points of Failure (SPoFs) and Single Points of Trust (SPoTs).

However, DLT enables an even more fundamental change which enhances resiliency: a simplification of the settlement model.

Simplifying the Settlement Model

Settlement in financial markets today is heavily intermediated.This intermediated model arose to allow traders and their customers to transact over distance and time. Banks were trusted by their clients and other banks to intermediate trade between Amsterdam and Venice and kept accounts using double-entry book-keeping. Since the 1960’s, developments in information technology enable book-keeping to be automated, but the underlying intermediated settlement model remained: both because it was easier to automate an existing model and because the double-spend problem of transferring value digitally was not solved. This has resulted in a complex chain of intermediaries where the risk of operational failure exists in each individual banking institution, the FMIs that provide clearing and settlement services, and in the flow of information between them.

Now that cryptocurrencies like Bitcoin have shown that value can be transferred digitally without the need for an intermediary, the question is whether we should revert to the settlement model that existed before intermediation: a peer-to-peer model. Fundamentally, this model is simpler than the intermediated model and simplicity has the benefit of increasing resilience. The Fnality Global Payments model proposes to implement this peer-to-peer capability, removing the need for intermediaries and with it the associated operational complexity and exposure risk.

DLT Model of Resilience and Reliability

Once the settlement model is changed from intermediated to peer-to-peer, Fnality Global Payments proposes to use decentralised technology. There are three primary reasons for why decentralisation, as proposed in the public blockchain space, will ultimately result in greater resilience:

- **Fault Tolerance:** The distributed nature of DLT is intrinsically resistant to faults by having no single point of failure. The FnGP model has a network of nodes that can continue normal operation even with multiple concurrent failures. Fault tolerance is further enhanced by diversity of the nodes not only in terms of location, as is often found in traditional FMI, but also in other areas not normally practical for traditional FMI such as operating system, software implementation, and system operator.

- **Attack Resistance:** A traditional FMI relies on keeping threats out and operation is typically severely compromised once security is breached. The FnGP private DLT model in contrast can continue normal operation even in the presence of malicious colluding nodes, provided that less than a third of validator nodes are compromised. The FnGP model combines state-of-the-art cryptography and security mechanisms to protect the network with having no single point of trust. This combines the security protection of a traditional FMI with the inherent attack resistance demonstrated by public blockchain cryptocurrencies.

- **Collusion Resistance:** The final weakness of traditional FMI is the possibility of collusion. The DLT model of FnGP involves the transparent and independent validation, execution, and storage of transactions by diverse peers on the network. In addition to the operational resilience outlined above, the ledger is innately resistant to tampering and unauthorised transactions due to requiring a consensus of over two thirds of validator nodes.

- When this is combined with diverse participants, with diverse goals, who are accountable for the correct operation of their nodes, this provides innate collusion resistance. This is further combined with real-time transparency of market operation that allows immediate detection of compromised operation combined with continuous regulatory oversight.

DLT is a new technological paradigm, but the spectrum of risks to which it is exposed is the same as the risks faced by any centralised system in operation today. What is novel is the method for solving and mitigating them. An example that highlights this point concerns system uptime.

The distributed nature of DLT eliminates SPoFs and through that can achieve far higher availability than that of the individual nodes. While cloud providers such as AWS and GCP provide instance uptime SLA of 99.5%, for illustration and to consider other factors lets assume any individual node is functioning correctly and connected to the network just 99% of the time. In the case of a FnPS running with a validator node set of 15 nodes, the network can tolerate the loss or compromise of 4 these nodes yet still guarantee correct operation. If individual nodes have independent availability of 99%, this translates to overall FnPS availability of 99.9999% (calculated using the binomial probability distribution). Availability does not rely on traditional approaches of extreme engineering with high costs and diminishing returns, instead it arises naturally from the distributed design of transaction execution and storage.

This calculation does not include failures in, for example, planned maintenance or catastrophic events like entire region failures, or non-independent failures like faulty smart contracts. However, it illustrates the order of magnitude of superior performance achievable compared to the performance of centralised FMIs. It is also likely to be substantially less expensive to operate as it can be run on commoditised cloud services.

Centralised systems also use this notion of redundancy. Principle 17 of the PFMIs requires an FMI to "*set up a secondary site with sufficient resources, capabilities, and functionalities and appropriate staffing arrangements that would not be affected by a wide-scale disruption and would allow the secondary site to take over operations if needed.*" Typically, FMIs have two to three operational sites or data centres with a recovery time objective of 2 hours. Various methodologies exist to enable this fail-over; the speediest can happen within a matter of seconds.

Due to cost pressures, a centralised system usually has very low diversity in terms of its hardware, operating system, hosting and administrator dimensions. This lack of diversity can mean that failure modes are highly correlated giving a false sense of the effectiveness of redundancy as a defence. On the other hand, with a DLT based system underpinned by a common protocol but which has a firm emphasis on diversity in respect of the above dimensions, the difficulty and/or cost of attacking a sufficient number of the DLT system's diverse features so as to impact the system is very high. To guard against the possibility that all validators inadvertently centralise risk, Fnality has developed a Diversity Index to measure the heterogeneity of the nodes. The Diversity Index includes elements such as software clients, operating systems, hardware and locations. Monitoring this index will provide a robust method of demonstrating continued resilience and the validators will have incentives to ensure they remain different.

In order to maintain parity or 1 to 1 convertibility between fiat money (funds held at the central bank) and the funds balances in the Fnality Payment System, there is an operational link between the Fnality Payment systems and the Central Bank Account (RTGS system). This link is sometimes thought of as a single-point-of-failure because one cannot fund or defund the Fnality Payment System without it. However, the fundamental process of the Fnality Payment System is to enable the making of payments among participants, which can continue regardless of the operation of this link. For this reason, the core of the system can be considered resilient. The link itself will be subject to the same failure modes as centralised systems and can only be improved if either the central bank itself becomes an issuer on the Fnality Payment System or the RTGS system is adapted to enable other advanced cryptographic state exchange methods.

Economic Mechanism Design and Mutual Accountability

A key component of cryptocurrencies are the elements of economics or game theory such as an incentive mechanism which are crucial to the functioning of crypto in a trustless environment. This construction is important and is enabled by the technology, but is not a *feature* of the technology; it is economic mechanism design.

DLT can be used without mechanism design as exemplified in many enterprise proofs-of-concept and much to the disdain of the cryptocurrency community. However, the key function of mechanism design is to improve resilience by creating an economic downside for behaviour that negatively

impacts the equitable functioning of the system versus an economic upside for positive usage. Fnality Payments Systems take note of this, utilising a member-mutual style ownership structure for the validation node operators (VNOs). This member-mutual structure drives a mutual accountability, incentivising the VNOs (who are also participants) to obey the rules for the proper functioning of the system. It is also a very familiar model to capital markets participants having been the standard ownership structure for exchanges until the turn of the 21st century. Fnality could potentially improve the resilience of the system by implementing staking protocols, but has chosen not to implement them in the initial phases.

Truly distributed systems such as Bitcoin or Ethereum have a far lower probability of failure versus any centralised system as demonstrated by their ongoing operation without failure. This has been achieved through a combination of redundancy, facilitated through cryptography, and the innovative use of economic mechanism design. The key for Fnality is to ensure that the design of permissioned DLT does not introduce any SPoFs or SPoTs to ensure redundancy, and maintains the right incentives for the participants.

SECTION 3: ORGANISATIONAL RESILIENCE IN FNALITY GLOBAL PAYMENTS

The CPMI notes that having a culture that recognises the significance of security is important, but there is no mention of the importance of building resilience into the design of FMI organisations as a core principle, rather than simply looking to enhance resilience as a purely technical or operational objective.

Many organisations – ranging from the armed forces, through manufacturing to health – are finding that a traditional hierarchical structure is no longer fit for purpose. The main rationale is that traditional hierarchies have inherent vulnerabilities due to single lines of communication and dependency on relatively few individuals on the higher rungs. They are struggling to cope in a world of dizzying complexity and rapid change. They simply cannot learn and adapt fast enough to remain competitive and resilient.

The current mantra is to automate processes. Automation yields efficiency. Further, the conventional argument is that the fewer processes and the more effective the technology that automates them, the less there should be to go wrong due to manual error and fewer operational vulnerabilities should remain. However, this misses an important point: as markets change, intentional evolutionary change within institutions is both desirable and necessary. Automation can make change riskier and the impact of change more uncertain – in other words, elevating operational risk – because typically, the connections and interdependencies between processes that have been automated cannot be easily seen.

Fnality's organisational design seeks to overcome the bureaucracy of traditional hierarchies and to resolve the apparent trade-off between efficiency and resilience. The solution is to distribute decision making from the top of the organisation to the areas receiving relevant information in real-time, and to steer those decisions with collective purpose. This requires many other elements of the organisation to be designed to reinforce the 'right' decision as has been described in many recent books[2] [3] [4] [5] [6]. The methods used by these organisations can be adopted to make the whole organisation stronger in multiple dimensions including resilience. The typical traditional organisation fails to achieve true resilience because it departmentalises resilience; each department seeks to build bigger and deeper defences. This can work when the nature of potential disruptions is well, or at least somewhat, understood. However, when unexpected problems happen, it struggles to communicate and coordinate across these departmental barriers, amplifying the adverse impact.

The core, fundamental elements of Fnality's organisational design are:

- To co-ordinate and collaborate across the teams we have taken a 'Team-of-Teams' approach as popularised by General Stanley McChrystal. In this model, the whole organisation links the teams together by treating each team as an element of a single bigger team. The Fnality approach utilises two of the key concepts of Team-of-Teams: extreme transparency and empowerment, pushing decision making to the places with the best information.

- To allow for decentralised decision making, Fnality operates a very flat and lean structure with a principle of 'mutual accountability' across our teams. In teams and the collective of teams, this means that employees are accountable to each other – mutually accountable – which is exponentially more robust than individually accountable.

- Teams consist of 7-9 members to optimise communication, collaboration and efficiency. This improves understanding, innovation and response.

- Team members are all T-shaped, meaning they have a core skill set (the vertical trunk of the 'T') and other skills (the horizontal arms of the 'T'), and all teams are cross-skilled, autonomous and aligned to Fnality's strategic consumer objectives. This means they can make decisions on consumer value and have the competencies to build and ship the products.

- Teams can increase capacity and capability by adding virtual ‘Subject Matter Experts’ (SMEs) based on the best fit to the work to be completed. This harnesses cross team collaboration and exposure, allows for capacity balancing, and improves responsiveness.

- The capabilities and capacities are mapped to iterative deliveries of outcomes. This ensures that Fnality is always aligned on scope and can constantly adjust to ensure the right skillsets are available in the right amount for what needs to get done next.

- Enabler leadership is practised to support team success. This reduces command and control risks and individual 'hero' reliance.

- Fnality is ‘Consumer Outcomes’ focussed - everything the teams deliver is aligned to consumer value, both hypothesised and measured, and this is what drives both strategy and delivery. As described in an FCA speech the “*Impact tolerance requires firms to think about services from the perspective of their consumers, as well as the wider UK financial system and financial markets.*”

All of this results in a fit with Conway’s law: empowered, decentralised, cross-functional, fully autonomous teams able to solve problems, aligned through consumer led value streams and the context of Fnality’s overall vision and strategy. Short increments of work allows Fnality to learn before improving each step or process, reducing waste and risk. Multi-skilled teams allow different people to pick up tasks ensuring continuous value delivery. An elimination of dependency on ‘hero’ individuals ensures a continuous spread of capability and increases redundancy. Finally, minimisation of work-in-progress leads to overall higher output allowing Fnality to produce more value, more quickly and to rebound stronger in the event of failure. In fact, tolerance of failure is promoted as an opportunity to constantly expose any weakness of thinking and to rapidly learn.

So, the Fnality organisation has the ability, meaning the capabilities and the capacity, to solve problems when and where they occur immediately, and then propagate those learnings throughout the organisation to improve the overall resilience. Fnality is anti-fragile.

APPENDIX: FNALITY ORGANISATIONAL DESIGN PRINCIPLES

Principle 1: Diversity and redundancy

Fnality organisations are designed such that there is redundancy in products, people (collectively: ‘capabilities’) and organisational governance to compensate the loss or failure of one or more of these elements. To ensure there are no single points of failure in these areas, redundant elements are designed to exhibit diversity in response i.e. react differently to a change or disturbance but achieve the same stable operation outcome.

Principle 2: Mutual Accountability

Fnality organisations use ‘mutual accountability’ as an operating principle to ensure a polycentric governance structure i.e. people mutually achieve an outcome and maintain its integrity such that accountability cuts across hierarchies and structures to introduce a sense of organisational self-regulation.

Principle 3: Transparency through frequent and open communication with no hierarchical boundaries

Fnality organisations operate on a principle of complete transparency in decision making, operations and governance. Strong communication ensures that this transparency is maintained internally with its employees and externally with organisations in the ecosystem. Fnality operates on open-source principles so that competent ecosystem members can critique and contribute to improve the Fnality Payments System into an ever more resilient FMI.

Principle 4: Senses and learns

The culture in Fnality gives employees the capacity to experiment, evaluate and test alternative hypotheses, rapidly learn and adapt. This results in continuous, fast and incremental improvements.

Principle 5: Balances strength and resistance with adaptability to continually improve

Fnality uses the minimum viable approach in everything it does. This builds resilience by maintaining a balance between resistance, i.e. long-term strength, and flexibility. The agile philosophy at Fnality allows the organisation to continually improve and adapt to ensure there is always scope for course correction in the event of change or disruption.

Principle 6: Comes back stronger

Fnality is designed such that it comes back stronger and becomes more resilient in a difficult environment or when things break so that the resilience is evolutionary. The focus is to foster a complex adaptive systems thinking approach and a proactive culture by evaluating beyond design events, formulating attack scenarios and learn from their impact to constantly build resilience.

Principle 7: Continually re-aligns to a shared common goal or vision

Although empowered and mandated to explore alternative paths, the organisation always reverts to an aligned direction through the use of a shared consciousness. This balance of a stable, predictable and consistent direction and desired outcome, combined with multiple pathways to achieve it, builds resilience.

WOULD YOU LIKE TO KNOW MORE?

CONTACT US:

Fnality International c/o WeWork
2 Minster Court
Mincing Lane
London
EC3R 7BB

Email: enquiries@fnality.org

FOOTNOTES & FURTHER READING

[1] - Lael Brainard, Cryptocurrencies, Digital Currencies, and Distributed Ledger Technologies: What Are We Learning?, May 2018

[2] - Stanley McChrystal, Team of Teams: New Rules of Engagement for a Complex World, May 2015

[3] - David Marquet, Turn the Ship Around: A True Story of Turning Followers into Leaders, May 2013

[4] - Frederic Laloux, Reinventing Organizations: A Guide to Creating Organizations Inspired by the Next Stage of Human Consciousness, February 2014

[5] - Gary Hamel, Michele Zanini, Humanocracy: Creating Organizations as Amazing as the People Inside Them, August 2020

[6] - Nick Obolensky, Complex Adaptive Leadership: Embracing Paradox and Uncertainty, August 2010