FNALITY GLOBAL PAYMENTS

THE CHANGING ARCHITECTURE OF FINANCIAL MARKET INFRASTRUCTURES: IMPLICATIONS FOR FINANCIAL STABILITY AND OVERSIGHT

THE FNALITY TEAM

APRIL 2022

CONTENTS

INTRODUCTION

Financial Market Infrastructures (FMIs) are the backbone of post-trade clearing and settlement of financial transactions.[1] As their uninterrupted and smooth functioning is essential for the stability of the financial system, their safety and soundness needs to be ensured at all times. Not surprisingly, FMIs are regulated as tightly as systemically important banks (SIBs). By the nature of their business FMIs are very IT-centric institutions. While technological changes have influenced how FMIs operate in the past, recent innovations such as Blockchain and Distributed Ledger Technology (DLT) are greatly expanding the feasibility set of how FMIs can operate. While it has always been possible to abstract the various functions of an FMI, the rationale and benefit for doing so has not been particularly obvious. The advent of Blockchain and DLT, however, has created a new architecture that allows for a further explicit abstraction of FMI functionality with the benefits of increased redundancy, resilience and transparency. This new level of abstraction is calling into question how FMI overseers have traditionally delineated between 'core' vs. 'other' FMI functions.

Regulators, overseers and standard setting bodies are challenged in keeping pace with these developments. In recent reports they have provided additional guidance on some technology driven innovations in FMIs (for instance, outsourcing to cloud systems (Bank of England 2021) and stablecoin arrangements (CPMI-IOSCO 2021). In this paper we propose a flexible, general framework that would allow overseers to assess a large number of novel operational FMI arrangements that have emerged or are about to emerge.

RECENT TECHNOLOGICAL DEVELOPMENTS

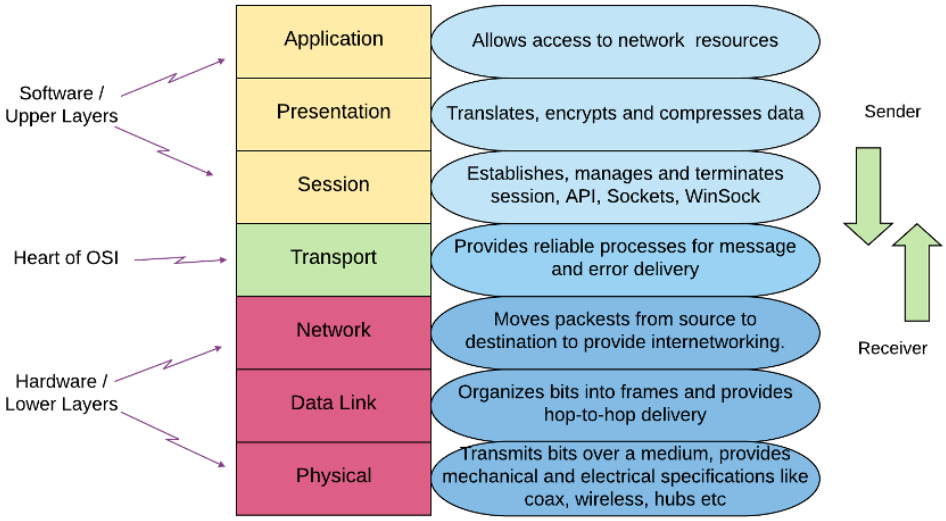
Technological advancement is not just about new technology *per se*. Computer technology has been used in finance for more than 60 years, and the fundamental nature of that technology has not changed; computers still process calculations that transform given inputs into given outputs. The limits of information technology methods, particularly the client-server model, *embedded account intermediation* (i.e. the use of trusted third-party financial institutions to act as settlement middlemen between two counterparties such as commercial banks, investment banks, and fund managers) as the standard business process model for financial markets. A typical FMI business model is for the operator to set the rules for participation and operation, and act as the 'systemic risk manager' for the system, while outsourcing to one or two infrastructure providers who operate the relevant hardware and/or software that constitutes the infrastructure of the system. In these models, hardware or software updates or migrations involve material change programmes that can create large risks to the business, both in terms of change risk as well as resource diversion.

What has changed is the possibilities of how tasks or jobs can be carried out. In other words, account intermediation is no longer the only possible business process. This change has been enabled by the ongoing abstraction and commoditisation of various operational 'layers' necessary to create holistic information technology systems.

For some time now, the computing world has optimised the delivery of technology products and services by creating what are described as '*abstraction layers*'. The basic idea is to create independence between various subsystems in order to make the development of a technology service 'tractable'.

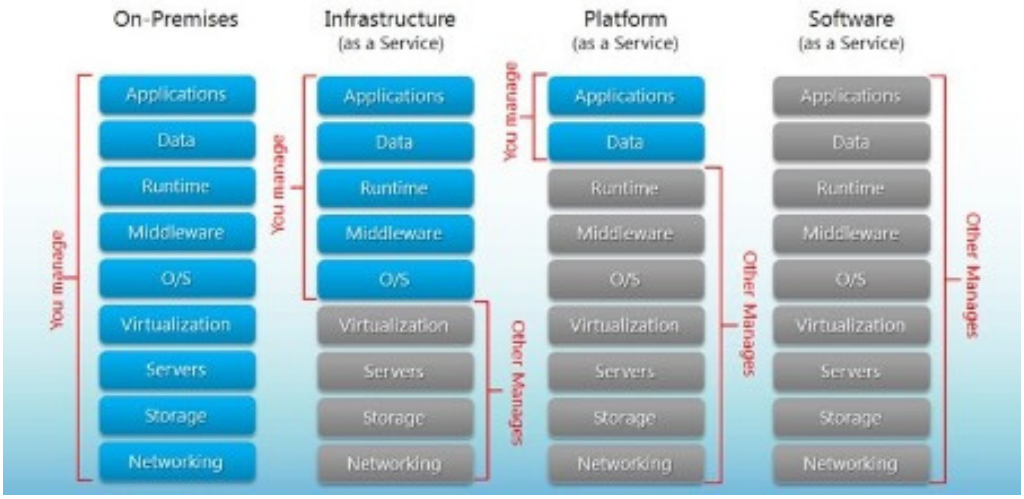
Critically, however, these subsystems must execute various easily recognisable design patterns that can be layered on one another to provide the relevant service. In other words, the layers start to become standardised which creates more usage, in turn driving investment and reliability, in turn driving usage; the flywheel effect made famous by Jim Collins.

The OSI model (Open Systems Interconnection model) for the internet is a well-known example. In this model, there are 7 layers as shown below:



Without this model, every time we wanted to connect one computer to another, we would have to build each of the lower layers from scratch and agree on the standards for the upper layers. This would impose an enormous cost on networking.In fact, the sheer scale of the internet today would simply not be possible without this abstraction layering. What is more, these abstraction layers allow for more reuse, saving costs, and create more composability, enabling a wider set of problems to be solved in a more targeted manner.

This layering concept has been applied to many aspects of computing. The most recent incarnation of the thinking is in Cloud, where one often hears about 'Something-as-a- Service'. What this means is that one can 'rent' the number of services one needs from a cloud provider, rather than having to build or purchase them independently and then host them. The below graphic shows the different versions that are available (ref):



The management and provision of these layered services by specialists contribute to enhanced performance, scalability and, most relevant to FMIs, availability. It is conceptually easy to think about these services as utilities, such as electricity or water where the mass provision is generally much more reliable than self-provision due to specialisation and concentration of resourcing. However, as is well understood in financial markets, reliance on a single provider (single point of failure) can result in spillover risks: while day-to-day service and reliability are massively enhanced, anything that does go wrong can create a much wider impact without proper risk controls and back-up/secondary provider arrangements in place.

This type of layered thinking has migrated from computing into physical products as well. Today, when a car manufacturer builds multiple models, they usually have many common or shared components in the various types. For example, Porsche and Volkswagen share components like chassis and engines and many other features using a modular platform called MQB. This approach extends the layer abstraction into modular product levels where lower-level modules can be used to support multiple higher-level modules. From a mathematical perspective, this dependence takes the form of a directed acyclic graph. The lowest layer products are the most commoditised, e.g bolts, whilst the higher-level products can be more differentiated, e.g. chassis. And the composability released by this thinking means the final car can be highly customised, whilst still using these standard components. It also means that problems or features in one component - such as defeat devices - can spill over to many car models. Any such issues ultimately damage the reputation of the manufacturer and the means by which it has selected and audited the lower-level components. Or put differently, it is always the manufacturer's responsibility to ensure the car as a whole is compliant with all regulatory requirements.

Each of these layers can be architected in different ways, depending on the fundamental design goals. The main goals for the internet were to connect various types of communication networks and, since it was developed initially for military purposes, survive any and multiple elements of the system failing for periods of time. The design goal was solved by ensuring that the system is decentralised, i.e. it has no single point of failure. The world of finance, however, had a different design goal for communication that emphasised the standardisation of financial messaging developing a private, centralised internet called SWIFT.

Several papers have discussed the layering concept in Financial markets using Blockchain technology (e.g. Roy and Schär). The main area they focus on is the settlement layer (also called the payment and exchange layer), which can now be provided by either a trusted third party or by a network. The benefits of a network providing the settlement function are composability, resilience and transparency. As Ronald Reagan famously said to Gorbachev "Trust but verify". On a blockchain, 'everyone' gets to verify! For regulated FMIs, however, an important qualification applies. Only a known and trusted set of entities will be allowed to provide verification services (CPMI-IOSCO (2021)).

LAYERS IN SETTLEMENT SYSTEMS: AN ILLUSTRATION

Both Payment Systems and Securities Settlement Systems facilitate the transfer of ownership of securities or funds (money). To do this, the Settlement Systems must have a:

- System Operator
- Settlement Asset
- Settlement Asset Supplier
- Account Operator
- Record Keeper
- Settlement Agent.

It should be noted that some systems may have an Account Operator to operate an account at a bank or CSD.

System Operator: Determines 'The Rules' of the system and ensures access is open to the relevant identified participants. This is the key role from a governance perspective of the FMI; the System Operator is accountable to regulators for the overall operation of the FMI, managing all the associated risks and overseeing all the third parties who perform various roles in the system.

Settlement Asset: For systems that facilitate exchange of value, such as payment systems ('money settlement') or securities settlement systems ('securities settlement'), the system must have a settlement asset in which the counterparties can willingly and legally settle. The Settlement Asset must maintain belief in its ability to be used to discharge obligations.

Settlement Asset Supplier: For systems that facilitate the exchange of value, there must be a supplier who is accountable to the System Operator and the system participants for the supply of the Settlement Asset in the system. This role also communicates with the Record Keepers to enable them to perform their role.

Account Operator: If the Settlement Asset Supplier relies on a Central Bank or Central Securities Depository (CSD) with control over the Assets that "back" the Settlement Asset to discharge its own liability to system participants, then an Account Operator role may additionally be assumed by the Settlement Asset Supplier. This role is to communicate with the Central Bank or the CSD with respect to inflows or outflows of Assets that 'back' the Settlement Asset.

Record Keeper: This role provides the operational processes, whether manual or automated via technology, to enable the FMI to record the changes in the 'state' of ownership of the Settlement Asset. It is purely an administrative role for which it is accountable to the System Operator.

Settlement Agent: This role controls changes from one 'state' to another, allowing only those changes that are permissible under the rules of the system. In the case of a settlement system, the Settlement Agent ensures there is no double spend and/or the synchronisation conditions for PvP and DvP are met. (As the CPMI Glossary notes a settlement agent sometimes differs from the operator or settlement institution of the system). It is accountable to the System Operator for performing this role and communicates with the Record Keepers for this purpose.

REGULATION OF FMIS

The relevant international regulatory standards for FMIs are the 2012 CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI). The PFMI define an FMI as '*a multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling, or recording payments, securities, derivatives, or other financial transactions. FMIs typically establish a set of common rules and procedures for all participants, a technical infrastructure, and a specialised risk-management framework appropriate to the risks they incur*'.

While the addressee of the PFMI is generically referred to as 'the FMI', it is clear that the addressee is a legal entity incorporated in a jurisdiction and owned by shareholders. In the layers introduced above, this addressee is the System Operator. The governance arrangements of this entity need to be documented, be underpinned by adequate policies and allow for clear and direct lines of responsibility and accountability. For instance, the System Operator needs to have a Board of Directors, Board Committees and senior executives.

Operators of FMIs have traditionally outsourced important services to other FMIs or third-party service providers, in particular in operations. For instance, System Operators have often outsourced the provision, operations and maintenance of the system's infrastructure to a third party, while retaining overall responsibility for its performance and resilience.

According to the PFMI an FMI needs to govern the relationship with 'service providers' adequately and remains accountable.[2] These service providers usually take the form of separate companies and businesses, but many of the same issues arise between different departments within the FMI operator or even just different groups of people (PFMI 3.17.20). Thus, the FMI '*should ensure that those (outsourced) operations meet the same requirements they would need to meet if they were provided internally*'. Also, an FMI should have robust arrangements for the *selection and substitution* of such providers, timely access to all necessary information, and the proper controls and monitoring tools. For particularly important services providers, like the global messaging system SWIFT, regulators have coined the term 'critical service providers' (CSPs). The oversight expectations for CSPs are part of the PFMI (Annex F). In 2014, CPMI and IOSCO published the corresponding assessment criteria for CSPs.

For those service providers that are deemed to be of critical importance to the functioning of the infrastructure, '*an FMI should identify the risks from its critical service providers and utilities and take appropriate actions to manage these dependencies through appropriate contractual and organisational arrangements*'. It is also the duty of the FMI to ensure that the relevant authorities are '*informed about the performance of these critical service providers and utilities*'. To that end, the FMI can contractually provide for direct contact between the critical service provider and the relevant authority, '*contractually ensure that the relevant authority can obtain specific reports from the critical service provider, or the FMI may provide full information to the authority*' (PFMI 3.17.21). The authorities may also establish 'expectations' that critical service providers should meet (PFMI Annex F). It should be noted that in some cases the authorities may have direct supervisory powers over a critical service provider, but the FMI retains its primary role in monitoring, managing and mitigating risks that their service providers pose to their systems. In other cases, the authorities may not have direct supervisory power over a critical service provider. Thus, they have to monitor adherence to the 'expectations' exclusively through their statutory powers over the FMI or the system operator as the accountable entity.

Can the PFMI be applied to next generation FMI architectures?

The PFMI - including the oversight expectations for CSPs - were published in 2012. Back then, it was inconceivable that FMIs would ever rely on blockchain or distributed ledger technology or even cloud technology. Similarly, it was difficult to foresee that layers of an FMI could be separated and essentially all layers could be outsourced and be provided by a diverse group of service providers offering commoditised products. Hence, an obvious question is whether the PFMI are still fit for purpose in a world of 'layered FMIs'.

Using the FMI layers introduced above it is possible for FMIs to become very lean organisations. In essence, an FMI can consist just of the top layer ('system operator') which provides the rule book for how participants access and use the shared infrastructure, the overall governance arrangement and comprehensive risk management. The other layers would be provided by third parties or other FMIs. It can be expected that there will be several providers per layer offering commoditised products or services. In other words, the dependence on any single service providers will be reduced markedly. This will lower overall operating costs while increasing redundancy and resilience.

Due to the increased importance of these providers, FMIs and their overseers need to pay closer attention to these arrangements, in particular the contracts governing the relationship. This will be particularly true where a given layer or commoditised product or service is critical to the FMI's payment and clearing processes. The risk appetite and operational resilience impact tolerances set by an FMI's Board for each layer and product/service will need to be credibly met by such third parties. This is where clear roles and responsibilities in both 'business as usual' and times of crises, and the maintenance of standards, including regular stress testing, will be needed to ensure the robustness of arrangements.

The PFMI seem to be able to accommodate these developments. Principle III requires the FMI to have 'comprehensive risk management' in place. More precisely, 'an FMI should have effective risk management tools to manage all relevant risks, including the legal, credit, liquidity, general business, and operational risks that it bears from and poses to other entities' (3.3.7).

However, in a discussion paper, the FSB (2020) lists the challenges associated with increased outsourcing of financial institutions, arguably without having FMIs in mind. The report indicates that contractual obligations of third-parties to grant access to information to supervisory and resolution authorities 'can be challenging to negotiate and exercise, particularly in a multi-jurisdictional context'.

In line with the observation by the FSB, today's approach of indirect oversight of important service providers is inefficient in a world in which a service provider serves several FMIs. Such a service provider will need to provide all kinds of information to the FMIs and their overseers without any mechanism for cross-border or cross-FMI coordination.

Against this background, two remedial measures stand out. First, important service providers should be able to receive an international license (or 'passport') which relieves their need to provide information to multiple overseers individually. In essence, this approach would be similar to the well-known co-operative oversight approach outlined in Responsibility E of the PFMI. A prominent example is the co-operative oversight of SWIFT. SWIFT serves the global banking and payments community, and is overseen by the National Bank of Belgium (lead) in cooperation with the central banks of G10 countries.

Second, increased distribution, meaning multiple simultaneous providers replicating important third-party services cost-effectively due to commodification and eliminating single-points-of-failure, means that each individual provider is less important than in previous FMI architectures. Let SWIFT again serve as an illustration. Due to the fact that there are essentially no alternatives to the SWIFT network for global payment messaging, the regulatory standards applied to SWIFT obviously need to be extremely demanding. But if there are several service providers that are easily substitutable, the regulatory bar on the individual provider can be set lower. Thus, if a distributed system can evidence that the set of third-party providers and the controls and processes around substitution/redundancy meet operational resilience impact tolerances as well as other standards, the regulatory demands on individual third-party providers should be less challenging.

FOOTNOTES

1 - They include systemically important payment systems, central counterparties (CCPs), central securities depositories (CSDs), securities settlement systems (SSS) and trade repositories (TRs).

2 - Existing regulatory regimes for FMIs make very limited provision for oversight of individual conduct within these entities as most supervisory and enforcement powers are focused on the legal entity. The Bank of England proposes to fill this gap with an extension of its “Senior Managers and Certification Regime” to FMIs (Bank of England 2021b)

CONTACT US

WOULD YOU LIKE TO LEARN MORE?

FNALITY.ORG

Fnality International
Rise London
41 Luke St
London
EC2A 4DP

Email: enquiries@fnality.org