Decentralized Financial Market Infrastructures:

Evolution from Intermediated Structures to Decentralized Structures for Financial Agreements

By Sara Feenan, Daniel Heller, Alexander Lipton, Massimo Morini, Rhomaios Ram, Robert Sams, Tim Swanson, Stanley Yong, and Diana Barrero Zalles

Abstract

Financial market infrastructures (FMIs) have evolved as core elements of highly intermediated financial markets partly due to the technological limitations of the time when they were first architected. Organizations and firms were unable to share records without having to entrust a single party to manage them; hence this phenomenon of intermediation has led to significant information silos. Simultaneously, it has driven the structure of business models, as well as regulatory supervision and oversight, in ways that furthered intermediation and also created a misalignment of incentives and risk taking between entities now categorized as systemically important financial institutions (SIFIs) and systemically important financial market infrastructures. Over time, this consolidation has led to highly concentrated FMIs and with it, concentrated risks. Some of these risks go beyond the credit risks of just one or two institutions, becoming instead systemic risks that are continuously monitored by regulatory bodies based on coordinated sets of principles and guidelines including the 2012 Principles for Financial Market Infrastructures from CPMI and IOSCO.

Over the past decade, advances in public key cryptography, hash functions, virtualisation, distributed consensus, multiparty computation, and peer-to-peer networking have led to experimentation around record sharing between erstwhile competitive firms. Over the past five years, a series of independent efforts has chaperoned regulatory requirements into a digital, automated state that enables secure information sharing in full compliance with the law, while simultaneously enabling market participants to mutualise infrastructure that would otherwise be run by a single trusted party. With these developments, many of the services that centralised intermediaries currently provide could potentially be replaced by decentralised infrastructures or *decentralised financial market infrastructure* (dFMI). dFMI also enables a change in business structure, where a re-alignment of incentives can take place such that those firms taking risks can fully bear the consequences of these risks.

Table of Contents

A. Introduction

Decentralized financial market infrastructure (dFMI) is a new concept built on emergent structural truisms of financial markets, namely:

1. Money, credit and financial markets make up an international *system* of inter-connected activities between trading counterparts and various supporting actors.
2. This system is socially useful only if *incentives are aligned* in such a way that risk is assumed proportionally by those who create it and reap its rewards.[1]
3. This system admits the existence of *public goods* provided by entities whose incentives are not primarily financial and whose rewards are reaped exogenously.
4. The infrastructure that implements 1 can either support or undermine 2.

This paper takes the view that today's Financial Market Infrastructure (FMI) falls short on point 3 because of excessive financial intermediation.

The infrastructure of today's financial markets often facilitates misaligned incentives and results in the involuntary socialisation of risk.[2] Hence the current FMI is one where point 1 above has undermined point 2.

The source of excessive intermediation lies in the existing market infrastructures and business models of the key institutions upholding them, particularly for clearing and settlement (C&S) such as central counterparties (CCPs) and central securities depositories (CSDs) which were designed around mainframe (later, client-server) technology architectures. The root cause of this intermediation can be traced to the fact that the business models and market structures we have today are shadows cast by the introduction of electronic data storage and computing models launched in the 1970s (e.g., dematerialisation in securities).[3] Whilst information technology brought essential benefits and efficiencies to a market previously based on paper-based instruments, this also disrupted incentive structures and organisational models that were built up over several centuries of market practice and commercial law.

The purpose of financial intermediation was to provide a means to settle the transfer of financial risk during a trade, initially involving physical assets, across space and time, in an efficient and standardised "trusted" way. As the financial industry expanded and

---

[1] Alternatively, socially *fair*. Public goods, by definition, one does not reap what one has sown. CBDCs are a type of public good. According to Agustín Carstens: After all, the monetary system is a critical public infrastructure that everyone depends on, and should be run in the interests of the public, not those of private stakeholders. When I refer to "central bank public goods", this is what I have in mind. "The future of money and the payment system: what role for central banks?" speech given on December 5, 2019.

[2] Costly Information Intermediation as a Natural Monopoly by Daniel Monte and Roberto Pinheiro

[3] Codified in the Geneva Securities Convention

automated at scale, the end result has been intermediation in the value chain between issuance of financial assets and securities, and the subsequent transfer of value between counterparties.

While CCPs brought significant benefits to the markets, such as transparency and standardisation, they also facilitated incentive misalignments[4]. The risk of a derivative, for example, is no longer borne by the derivative counterparty, but is partly centralised at the CCP, which is often a too-big-to-fail entity whose incentives are not necessarily aligned with those of CCP members. Participants in CCPs, such as banks, take risk onto their balance sheets by giving out loans and mortgages. Clearing members in a CCP provide additional financial resources to cover excess losses incurred by the CCP in unwinding positions of defaulting parties. There is a sense that the risk of catastrophic loss of a single party is borne by all parties.

The dFMI proposal is an attempt to re-imagine how points 1 and 2 above can be achieved as the internet's architecture evolves from client-server to peer-to-peer. Just as IT disrupted *market structure* in the 1970s by creating a heavily tiered and intermediated system, a peer-to-peer internet will disrupt market structure by collapsing trading and settlement into one process.[5] This can be similarly —maybe even more— disruptive to the system that has reigned for the last four and a half decades, where incentives are aligned such that point 1 above supports point 2.

An example of incentive alignment is a network where management responsibilities and risk bearing remain proportional to risk created. A shared network that provides all necessary functions of existing FMI would be indispensable in order for a systemically stable market to operate. These functions include risk and margin calculations, settlement via delivery and payment.[6]

A fundamental requirement is the existence of widely accessible, credible, regulatory compliant and stable digital currencies, issued by central banks or by or regulated private sector institutions, to be used on this shared network. One problem with currently discussed central bank digital currency (CBDC) models[7] is that access to

---

[4] While we recognise that it would be remiss to analyse FMI in isolation, in the interest of brevity, we focus on CCPs in this paper, making reference to other FMI types as and when necessary. We will, however, change focus in future papers to other FMIs.

[5] Prior to the 1970s, certain financial infrastructures were more localized, opaque, peer to peer, and institutional. Beginning in the 1970s, architecture brought automation, equally broader distribution mechanisms, new products but also intermediation and tiers which were not quite possible in the prior generation. However this new architecture was also limiting. The latest generation of financial services and infrastructure aims to provide more products to more people in a more sustainable manner. This could result in a less intermediated and more peer to peer infrastructure.

[6] An independent central bank is arguably still best to create a unit-of-account and store-of-value. When talking about clearing and settlement, shared ledgers (e.g., a blockchain) can provide a secure medium-of-exchange that is linked to the central bank currency or a stablecoin, fully backed in a credible way.

[7] Central bank digital currencies from CPMI (2018)

reserve accounts - and the liquidity support that central banks provide to holders of these accounts as a public good - will be the same as today (e.g., limited to domestic commercial banks and some FMIs).[8] As a result, CBDCs envisioned as such will not inherently, directly solve many of the problems with CCPs and collateral swaps because the foreign financial institutions and non-bank institutions involved may still be unable to hold a settlement asset like a CBDC. Expanding the role of central banking activities into new spheres of digital finance, while is outside the scope of this paper, could be a key development.

This paper explores the past, present and future of FMIs as a pathway toward dFMIs. This will shape how marketplace participants, regulators and their stakeholders could benefit from the adoption of technology that enables safer, incentive-aligned marketplaces with less concentrated risk structures. This is achieved by focusing on post-trade processes in the trade life-cycle within FMI, covering C&S, and specifically discussing CCPs both under the lens of today's capabilities and decentralised technology capabilities. It concludes with a call to action for industry participants to evaluate and explore the potential benefits and challenges of this new paradigm.

B. FMIs Today

Introduction

As per the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI), a Financial Market Infrastructure (FMI) is critical to fostering stability in financial markets and the broader economy. These systems facilitate the clearing, settlement, and recording of monetary and other financial mechanisms. In this section, we analyse the functions of a Central Counterparty (CCP) as they have evolved over time. We connect the risk generated in financial trading with the technology that serves to transfer that risk across counterparties, and ultimately, dissipate it upon fulfilment of obligations. According to the PFMI, the three main infrastructures for this reallocation of risk are:

1. Central Counterparties (CCP), which perform netting and facilitate value, collateralization pooling, mutualisation of risk, provide anonymity and ensure that delivery-versus-payment (DvP) takes place as promised. While CCPs have experienced historical defaults leading to loss of participants due to collateral shortages, over time they have become larger, more organized and thus more important to the financial system.
2. Central Securities Depositories (CSD), which hold securities to facilitate ownership transfers via book entries rather than physical transfers. They were first set up in the early 1970s, during the transition from paper to electronic

[8] See the "money flower" diagram on page 5 in Central bank digital currencies from CPMI (2018). Worth pointing out that many securities settlement infrastructure already settle in central bank reserves (e.g., CLS, Crest, T2S, ASX, Takasbank). See also Wholesale Digital Tokens from CPMI (2019)

trading with the use of mainframes, followed by client/server architecture and now trending towards a more peer-to-peer system.[9]

3. Payment Systems, which perform settlement services for financial transactions where ownership of an asset is transferred against exchange of monetary value.

The current FMIs operate largely under a system envisioned during and for the industrial revolution, with an initial purpose of facilitating global trade of physical assets. Early peer-to-peer settlement systems have moved into intermediated settlement systems, where centralised parties were established to formalise transfers of ownership and of funds. These intermediary institutions are designed to reduce risk by providing the credibility necessary for both buyers and sellers to engage in transactions at a large scale, across borders. With the development of capital markets, this system came to manage trades of increasingly complex financial assets. Mutualisation, along with joint ownership and pooling of funds, facilitates matching buyers and sellers, as well as borrowers and lenders. This saves time, lowers transaction costs and brings economies of scale.

Moreover, centralisation facilitates immobilisation to safeguard ownership certificates and streamline book entry records. This intermediary-based structure also enabled dematerialisation and the substitution of paper-based securities to book entry records. With the introduction of technology through entities such as the Depository Trust Company (DTC), fully electronic bookkeeping further increased the efficiency of trade records.

Yet the very nature of intermediated FMI, which relies largely on mechanisms of pooled funds, also shapes the risk landscape of the global financial market, where losses from defaults can be spread across large groups. When centralised entities function at a scale such that their operations can affect, directly or indirectly, all entities in a system, their idiosyncratic vulnerabilities can produce transmit contagion and pose systemic risk. With C&S processes at the core of interrelated trade relationships transmitting risk in FMI, entities like CCPs are an integral component behind the incentive structures and underlying business models that uphold the current system. Existing C&S mechanisms, particularly the risk structures arising from the use of CCPs, set the context for a dFMI proposal to mitigate risks and improve efficiency, in ways that can bring financial services and their governance structures up to speed with the latest advances in computation and technology.[10]

---

[9] CSDs are an example of an intermediary that was totally driven by client server technology of the day. See also: Couriers Without Luggage: Negotiable Instruments and Digital Signatures by Jane Winn

[10] For the purposes of this paper we are describing the role of CCPs in derivatives markets, where the CCP carries significant long term risk. Whereas CCPs in securities settlement where the novation to the CCP is a relatively short term process that facilitates DVP settlement. Note: in the FX market, CLS performs a similar function for PVP but carries no risk in the event of one party failing.

Brief History of Clearing and Settlement

CCPs existed but were structured differently throughout the 19th century in comparison to today[11]; for instance, paper-based instruments were a P2P form of C&S.[12] Over a century of common law preceded the immobilisation and dematerialisation of financial assets in the 1970s, which brought about functional changes to C&S.

Clearing Houses (CH) were set up to reduce the cost to transact commodities and derivatives for their members. By providing shared services, such as margin calculation, netting, and monitoring solvency of its members, a CH provided these members - and its associated exchange(s) - with protection from the administrative burden of fulfilling their obligations, along with a substantial surety that their counterparties would be solvent.

The evolution toward dematerialisation took several decades, with the following distinct stages:

1. Paper based securities, which were more analogous to peer-to-peer trading but still needed a CCP to ensure Delivery vs Payment (DvP) settlement.
2. CCPs, which were undoubtedly more efficient for paper-based settlement, in which all participants would meet in a single location at a specific time rather than arranging bilateral times. The shift from CHs to CCPs began when CCPs became a counterparty to each transaction on the exchange.
3. Immobilisation, a period in which a new kind of entity was created, a CSD, to hold all the “certificates” of ownership. CSDs became, of course, systemically important to the smooth functioning of the financial ecosystem.
4. Dematerialisation, which occurred when these certificates were transferred to electronic form, where CSDs (or Trade Repositories) were the entities responsible for record keeping of ownership of securities.

The Parallel History of Clearing and Settlement Technology

The pace of change has accelerated with the advent of computers in the form of client-server architecture.[13] This has created an ecosystem of data transfer in which not only are data storage and collection centralised, but also large parts of global computing power are aggregated.

Usage of computers to support the processing of data evolved continuously to support changing business mores. Single-user mainframes and time-shared systems were capable only of supporting batch processing at distinct times of the day and hence

[11] Central Counterparty Clearing: History, Innovation, and Regulation by Randall Kroszner

[12] Arguably, Digicash wasn't trying to create algorithmic central bank or digital gold, it was more conservative with cash settlement on P2P (that preserves something that is very valuable)

[13] Evolving IT Architectures: From Mainframes to Client-Server to Network Computing by S. Madnick

forced CCPs to impose margins adequate to cover the risks of a full day. Modern systems based on the client-server paradigm run various parts of bigger programs in a distributed manner across multiple “servers”, with a speed improvement that has facilitated the spread of lower intraday CCP margin requirements, releasing collateral for other transactions.

With the maturation of the client-server topology, data was collected and commoditised by several large platform players. With the advent of cloud computing, scale economies have driven a centralisation of market-share, where only a handful of players are now responsible for providing critical parts of the internet infrastructure.[14] Without this, the modern internet as we know it would be unavailable. The aforementioned handful of players factored resilience into their systems to satisfy the ‘always-on’ server side of the client-server architecture.

Maintaining the facade of an ‘always-on’ server is a design goal of distributed systems to meet business continuity requirements and strict availability standards such as 99.99% up-time. While peer-to-peer architecture has always existed as a paradigm parallel to client-server architecture, as computing power in individual machines improved, so has the number of peer-to-peer application domains, such as internet telephony and file sharing.[15] Peer-to-peer architectures are decentralized in addition to being distributed, unlike centralised but distributed client-server applications.[16]

Due to the various settlement risks inherent in today’s FMI, including concentration risk, international regulatory bodies such as CPMI and IOSCO have set recommendations and principles to establish resilience based on the existing technology. Similarly, open market access is an important element of MiFID2. Yet the financial services topology and governance structures overall have not kept pace with the evolution of computing, and thus fail to capitalize on important risk reducing opportunities in the globally connected financial ecosystem where we operate today. We believe that part of the standard setting and regulation should evolve to match the distributed topology of the Internet today, and that governance and risk can be decentralised to reset the incentive structures that exist in current financial markets.

In order to assess the potential benefits of dFMI, it is essential to understand the post-trade risks that exist today, as discussed in the next section.

Post-Trade Clearing and Settlement Risks

An important category of risks in the financial system comprises post-trade risks. The post-trade period spans the time from “trading” – when participants agree on the terms

[14] A New Source of Systemic Risk: Cloud Service Providers by David Fratto and Lee Reiners
[15] Technically speaking, P2P networks exist as overlay networks on TCP/IP. Peer to Peer Overlay Networks: Structure, Routing and Maintenance by Wojciech Galuba and Sarunas Girdzijauskas
[16] Tangentially there has been an emergence of computation on a local machine, such as secure enclaves in CPUs and on-device machine learning.

of a transaction – to "settlement" – when the obligations related to the transaction are discharged through the exchange of assets and/or monies (settlement) (CPSS 2010).[17]

The length of the post-trade period (see Figure 1) varies among financial instruments. Today's convention for settling FX and securities transactions is T+2, meaning that transactions are settled two business days after trading. Derivatives are typically longer-dated contracts. Many derivatives contracts settle months or even years after trading. For credit derivatives, for instance, settlement may be triggered by a default event and not by the end of the contract.

One important post-trade risk is replacement cost risk. This is the risk of loss of unrealized gains on unsettled transactions with a counterparty. The resulting exposure is the cost of replacing the original transaction at current market prices, due to the default of the counterparty between the time of the trade and the later settlement.[18] Replacement cost risks increase with market volatility and length of the post-trade period.

Another relevant post-trade risk is principal or credit risk. This is the risk that a counterparty will lose the full value of assets involved in a transaction - for example, the risk that a seller of a financial asset will irrevocably deliver it but not receive payment. Principal risk may exist in FX, equity and bond transactions. Current FMIs eliminate principal risk by guaranteeing simultaneous settlement of both legs of a transaction. This is called Payment vs Payment (PvP) for FX and Delivery vs Payment (DvP) for equities and bonds.

Since post-trade risks are largest for complex derivatives, financial market participants and relevant authorities (i.e. the Committee for Payment and Market Infrastructure (CPMI), the International Organization of Securities Commissions (IOSCO) and the Basel Committee on Banking Supervision (BCBS) have put a great deal of effort on the reduction of post-trade risks throughout the past decade. In response to the Global Financial Crisis (GFC), these regulators, as well as the G20 leaders, have demanded an increased use of Central Counterparties (CCPs). In 2009, the G20 leaders requested that "All standardized OTC derivative contracts should be traded on exchanges or electronic trading platforms, where appropriate, and cleared through central counterparties" (G20 2009).[19]

Figure 2 illustrates credit exposures among 3 market participants as they would arise in the derivatives market. Participant 1 owes 40 to Participant 2 and 50 to Participant 3 (net liability of 90). Participant 3 owes 60 to participant 2 and is owed 50 by Participant 1 (net liability of 10). Participant 2 is owed 40 by Participant 1 and 60 by Participant 3 (net asset of 100). In this example, Participant 2 is exposed to the default of both other

[17] Market structure developments in the clearing industry: implications for financial stability from CPSS on November 2010
[18] CPMI Glossary 2016
[19] G20 Leaders Statement: The Pittsburgh Summit

participants. The default of Participant 1 could be contagious, jeopardizing the financial health of the other participants ("systemic risk").

A CCP is intended to mitigate such systemic risk. It interposes itself between the counterparties to the contracts traded in financial markets, becoming the buyer to every seller and the seller to every buyer, thereby ensuring the performance of open contracts.

As shown in Figure 3, the CCP intermediates previously bilateral contracts. The CCP becomes the counterparty to Participant 1 holding a claim of 40 and owing 40 to Participant 2. Because of CCP intermediation, a default of Participant 1 or 3 will no longer directly affect Participant 2. Since the CCP is the counterparty to all transactions, it can net all obligations (shown by the green arrows). Multilateral netting reduces the obligation of Participant 3 from 60 to 10.

Yet a CCP is not immune to risk. A CCP faces two types of credit risk, current exposure and potential future exposure (CPMI-IOSCO 3.4.14-19, 2012).[20] Current exposure (CE) arises from fluctuations in the market value of open positions between the CCP and its participants. In order to mitigate risks from fluctuations in the market value of open positions, a CCP pays and collects Variation Margin (VM) from its clearing members. The CE is the difference between the current (i.e. at the moment) value of open positions and the value of positions when the CCP last marked them to market for the purpose of collecting variation margin.

Potential future exposure (PFE) arises from potential fluctuations in the market value of a defaulting clearing member's open positions until its positions are closed out, fully hedged or transferred by a CCP following a default. For example, during the period in which a CCP closes out a position following the default of a clearing member, the market value of the position or asset being cleared may change. This could increase the CCP's credit exposure, potentially significantly. Initial margins (paid by both counterparties when the contract is made) are calculated to protect the CCP against PFE, with a high probability.

In order to increase resilience against losses from defaulting clearing members, the CCP relies on pre-funded financial resources, which are largely provided by clearing members. These financial resources are expected to cover the default of the clearing member representing the largest aggregate credit exposure for the CCP in case of extreme, but plausible market conditions.[21]

---

[20] Principles for financial market infrastructures from CPMI-IOSCO

[21] CCP that are involved in activities with a more-complex risk profile or that are systemically important in multiple jurisdictions need to be able to withstand the default of the two largest clearing members (CPMI-IOSCO, PFMI Number 4: Credit risk).

The lines of defense of a CCP are often referred to as “default waterfall.” The sequence in the waterfall typically is:

1. the Initial Margins of the defaulting clearing member,
2. the default fund contribution of the defaulting clearing member,
3. a tranche of the CCP’s capital and
4. the contribution to the default fund from non-defaulting (i.e. surviving) clearing members.

CCPs in general are expected to have enough resources to survive the default of a single clearing member, whereas a special sub-class of CCPs, which are designated by regulators as “systemically important,” must demonstrate the ability to survive a simultaneous default of two clearing members.[22]

While the resilience of CCPs has increased in recent years (for instance, through more conservative stress scenarios, or measures in the area of recovery and resolution), it is undeniable that, inherent in the way that they concentrate risk into single pools, CCPs can still potentially jeopardize the stability of the entire financial system. Several plausible scenarios could give way for such systemic risk to materialize. Actual market dislocations may be larger than anticipated, more than the largest two clearing members may default or the collateral and (initial margins or default fund) may not be liquid and robust enough. Moreover, links among CCPs may give rise to unprecedented contagion transmitted by the balance sheets of common members across different CCPs.

In addition, most of the funds collected by a CCP from its clearing members are held by the members themselves, who provide banking services to the CCP. This wrong way risk, where counterparty exposure is correlated to the credit quality of that same party, is often not considered when CCPs are stress-tested.[23]

As will be discussed further in this paper, well designed distributed mechanisms for CCPs have the potential to reduce post-trade risks in the derivatives markets and central clearing in several areas.[24] For instance,

- Current Exposure of CCPs can be reduced by more frequent calculation and faster exchange of variation margins. The former can be achieved by systems that can provide real-time aggregated positions, with enough computational

[22] Systemic Risks in Central Counterparty Clearing House Networks by Alexander Lipton

[23] Wrong way risk is defined by ISDA as the exposure to a counterparty being correlated to the credit quality of the party. In this case, the CCP’s exposure to the clearing member who also provides it with banking services are correlated. If the bank defaults on the CCP, it is likely to also be unable to pay back the deposits. See: How cash is held by clearing houses from Clarus and Links to EACH Member CCPs statistics in line with the CPMI-IOSCO PQD from EACH

[24] CCPs could also leverage distributed systems to reduce risk.

resources to complete more repeated CE calculations. The latter can be achieved by high quality tokensed collateral, such as a “stablecoin,”[25] usable on modern high-speed payment networks. With tokenised collateral, the time gap between the calculation of the variation margin and its settlement would shrink considerably (if not disappear).

- Distributed CCP infrastructures can also calculate multilateral net positions.[26] Just like conventional CCPs, they can calculate multilateral net positions without resorting to a single computational or clearing agent. Variation margins would be exchanged directly between the participants based on the netted positions, eliminating the risk of having a CCP that may be too big to fail. This would greatly reduce risk for the survivors in the case of certain participants defaulting.

In the next section we study post-trade processing by focusing on CCPs in detail, showing how dFMI could potentially address major risks in the existing market infrastructure.

Central Counterparties

Functional Decomposition of CCPs

The Principles for Financial Market Infrastructures (PFMI) define what a CCP is:

> “A central counterparty interposes itself between counterparties to contracts traded in one or more financial markets, becoming the buyer to every seller and the seller to every buyer and thereby ensuring the performance of open contracts… CCPs have the potential to reduce significantly risks to participants through the multilateral netting of trades and by imposing more-effective risk controls on all participants. For example, CCPs typically require participants to provide collateral (in the form of initial margin and other financial resources) to cover current and potential future exposures. CCPs may also mutualize certain risks through devices such as default funds” (CPMI & IOSCO, 2012, paragraph 1.13).

This way, CCPs may facilitate liquidity in markets, as their business model operates on timely payments and conversions between cleared assets and non-cash collateral into cash. This mechanism is contingent upon rapid and efficient trades, as well as adequate management of margin requirements. Contracts cleared by a CCP can vary in length, from as short as one day (such as in some securities markets), to upwards of several decades (such as in the credit-default swap market). In cases of liquidity constraints, additional margin requirements may put pressure on clearing members and

[25] For the purposes of this paper, a “stablecoin” is defined as a digital representation of either reserves held at the central bank or a central bank-issued digital currency. For a brief history, see Toward a Stable Tokenized Medium of Exchange by Alexander Lipton

[26] Would it be a contradiction to add a “d” to CCP, a dCCP?

increase the risk of default, which at a large scale can threaten the financial markets' stability.

Below we consider both cases:

a) **CCPs in securities markets**

Securities bought and sold on regulated markets are often centrally cleared, which can also occur in OTC markets. As mentioned above, in securities markets, settlement is usually at T+2 (*there are exceptions*), and counterparty risk regards the risk of default over the trade-to-settlement delay. In the case of central clearing, after an agreement between the counterparties, a deal is usually novated into two deals, one between buyer and CCP, and another between CCP and seller.[27] Settlement happens at T+2, for a net amount between each counterparty and the CCP. Interposing CCPs aims at reducing risk by netting, and hopefully by leveraging the better credit quality of the CCP. CCPs manage margins and keep default funds in custody.

In this business model characterized by end-of-day settlement, which is days apart from trading time, notionals are accumulated along the trade-to-settlement delay. Liquidity implications are different in gross versus net settlement arrangements, but in both cases counterparty risk exposures grow over the trade-to-settlement delay, due to both accumulation and adverse market movements. In this setting, multilateral netting of short and long positions across as many positions as possible, as obtained via central clearing, is a very important form of risk reduction. Would this be equally relevant if settlement was delivery-vs-payment with a trade-to-settlement delay much shorter than it is today?

The question itself is mostly relevant to instruments which naturally terminate when a transaction is settled - for instance, shares sold for cash or short dated instruments. For more complicated instruments, such as swaps, which have multiple cash flows, further work is needed. This can be performed more easily if replacement risk is disregarded.

b) **CCPs in derivatives markets**

Central clearing has become mandatory for a large number of OTC derivatives.[28] After agreement among counterparties, a deal is novated into two opposite deals between the counterparties and the CCP. In the same process, the deal is

---

[27] The legal mechanism for the CCP to become the counterparty to its participants' trades can formally vary (effect on risk and liquidity is similar, effect on capital may vary): "In most cases, this is either novation or open offer. In novation, the original contract between the buyer and seller is discharged and two new contracts are born… In an open-offer system, a CCP extends an open offer to act as a counterparty to its participants and is automatically and immediately interposed in a transaction at the moment the buyer and seller agree on the terms" (CPMI & IOSCO, 2012).

[28] According to a relevant report: between 2012 and 2016 the percent of cleared OTC IR derivatives went from 40% to 60%. See p. 9 in Evaluation of the Bank of England's approach to financial market infrastructure supervision from the Bank of England

reported to trade repositories. Counterparty risk in the derivatives market lasts, in principle, until the maturity of the deal, often several years later, and however counterparty risk is closed at the moment the counterparty provides sufficient Variation Margin to cover the exposure.

Unfortunately, Variation Margin never corresponds to exposure since it is settled with a T+2 delay (with exceptions),[29] and moreover it corresponds to the minimum between margin call and the counterparty's valuation (undisputed amount). This creates a gap risk which is mitigated by the Initial Margin and default fund. Interposing CCPs aims at reducing such risk by netting, and hopefully by leveraging the better credit quality of the CCP. CCPs manage margins and keep default funds in custody. The fact that these funds are often (but not always) kept with the clearing members themselves is a very important but subtle source of additional risk.

The global financial crisis has left its impact on the financial ecosystem as a watershed, by irreversibly changing its *modus operandi*. In particular, both the range of products and the number of trades cleared by CCPs increased enormously, largely due to pressure by the G20 and its regulators. Given the fact that trade execution, clearing and settlement, constitute the all-important triad for capital market functioning, this increase in range and volume of trades has profound implications. In addition to stocks, many other products, such as equity derivatives, interest rate swaps, commodities and others, which used to trade over-the-counter (OTC), have now been moved to exchanges. As a result, *nolens volens*, all large banks are engaged in trading on CCPs.

Benefits of CCPs and Implications

The practice of central clearing in the years after the crisis (Figure 4), particularly in the derivatives market, has revealed that there are several functions that CCPs perform, consistently with CPMI- IOSCO (2012, paragraph 1.13) and beyond:

1. CCPs "become the focal point for transactions thus increasing market transparency" (European Commission, EMIR). Cleared transactions can be surveilled by regulators by monitoring just one entity.
2. CCPs help "reducing complexity and improving transparency and standardisation in the OTC derivatives markets" (FSB, BIS and IOSCO, 2018). CCPs set standard collateral rules, leading to standardisation of market practices and streamlined processes.

[29] New practices such as settle-to-market - where banks, instead of posting collateral against the change in market value (i.e. variation margin), make outright payments to restore the market value to zero - have additionally contributed to the observed decline in their market values. For example, settled-to-market (STM) models introduced in 2017 are gaining popularity. The CFTC in Letter No 17-51 Oct 12 2017 has requested that all CCPs in the US treat Variation Margin as STM. As described by Eurex Clearing circular 120/17, STM transactions are structured such that all outstanding exposure is fully and finally settled daily. This was originally an option only for Clearing Members on OTC interest rate derivatives but was extended to client-related transactions as well on 2nd May 2019 in circular 037/19.

3. CCPs compress exposures by collapsing netting sets for all counterparties into a single CCP netting set, with a sub-additive effect on counterparty exposure.
4. CCPs collect from member banks and keep in custody the default fund, which is a mutual fund that the CCP can use at the end of the default waterfall. This would leave the market unaffected in case of a default by a CCP member.
5. CCPs improve price discovery since, due to 3 and 4, CCPs are often treated as risk-free, so that CCP prices are affected by no adjustment related to the counterparty's credit risk (or by a small, homogenous one).
6. CCPs allow business continuity since, when the default waterfall covers the default of one counterparty, and the CCP consequently does not default, the deal with the CCP also survives.
7. CCPs guarantee anonymity of transactions and provide the desirable level of opaqueness in the market.

These functions essentially apply, with different technicalities and different materiality, to both cash and derivatives CCPs.

The first three functions have been tested in the last several years and are not the subject of debate. They represent the advantages of using CCPs, which regulators often acknowledge. The latter four functions rely on the assumption that a CCP can manage severe default events and survive with no bail-in. No counterfactual events where CCPs have failed have yet occurred - a record that no regulator wants to be the first to break by taking their eyes off the viability of CCPs under their charge.

With legacy technology available, the pursuit of goals such as transparency, standardisation, exposure reduction and fund mutualisation required a very invasive approach. This entailed novating all deals to replace the original counterparty with a single, large institution to manage a "mainframe" trading book, and simultaneously turn into a single point of failure for both operational and financial risk.[30] We believe that current technology allows us to consider decentralised alternatives to achieve the same regulatory pursuits for the benefits of CCPs with less concentration of risk.

With the increased range and volume of trades that occurred following the GFC, there is a clear need for banks to assess potential losses due to defaults of GCMs (general clearing members) of a given CCP, as well as defaults of CCPs themselves through the network banks participate in. The interconnectedness of the CCPs, which is due to the linkages through common GCMs (general clearing members), highlights the importance of modelling the network itself for potential vulnerabilities in the risk context of today.

---

[30] The genesis of distributed Financial Market Infrastructure (dFMI) arose from multiple articles by Sara Feenan, Rhom Ram, and Robert Sams including distributed Financial Market Infrastructure (dFMI) and the Disintermediation of Digital Assets.

One of the most intriguing open questions is what will happen to London-based clearing houses after Brexit, which could potentially change the network's entire topology.[31]

Another special case of risk insurgence comes from cash flow payments. The cash flow payer's exposure jumps when the cash flow is paid. Collateral should have a simultaneous jump by an equal and opposite amount to avoid risk jumping instead. Yet long collateral time-to-settlement makes this impossible.

Ultimately, the CCP business model provides transparency, standardisation and the perception of reduced risk thanks to netting. In a context characterized by long times for collateral settlement, and frequent misalignments between margin call and collateral received, netting between as many short and long positions as possible becomes a crucial form of risk reduction. Yet if collateral settlement times were short and misalignments unlikely, including mechanisms to make cash flow and collateral payments atomic, the need for netting, and thus the CCP business model, may be less relevant.

Challenges: The CCP Paradox

The reason for mandatory clearing after the GFC was to reduce the likelihood of systemic defaults.[32] In order to perform this role using legacy centralised technology, a CCP had to become the counterpart to all trades beginning on day 0. Several years later, the CCP business model has been well tested for this day-to-day, operationally intensive activity of being a counterpart to all trades. Despite the transparency, standardisation and perception of reduced risk from netting, if we consider the purpose for which CCPs were created – reducing the likelihood and severity of systemic defaults – their business model is untested, and there remain key open questions about it.

Alignment of interests is a crucial issue at hand: if CCPs' incentives are not aligned appropriately with those of market participants, they may in fact become conduits to magnify the very risks they were designed to minimize. If a large default were to occur, would a CCP be effective in managing it? In (Bignon and Vuillemey 2016), the 1974 story of the default of a CCP member is described from a regulator's point of view, which signals that in the default event, the CCP's interests were aligned to those of the defaulting party and not to those of the CCP members. This led to a moral hazard and eventually the default of the CCP itself.[33] The author suggests leaving less discretion in the hands of a central intermediary in order to avoid such distortions in future default events.

---

[31] The impact of this political event has been analyzed by several organizations including: The Impact of a No-Deal Brexit on the Cleared Derivatives Industry from FIA and Cliff Edge Effects under EU Law in a No Deal Brexit Scenario from ISDA

[32] Defaults are not merely an academic exercise. ISDA recently published "CCP Best Practices" which looked at two specific clearing members that have defaulted in the past five years.

[33] The Failure of a Clearinghouse: Empirical Evidence by Vincent Bignon and Guillaume Vuillemey

Given that CCP performance in a default event is not bulletproof, did we really reduce systemic risk by creating a few even larger points of concentrated risk? In fact, we know this not to be the case: the default of a CCP would be a more systemic threat than any credit event regarding an individual player, since a larger number of counterparties would be affected, each on a larger portfolio.

Concentrating all collateral in a CCP transforms risk mutualisation into a threshold risk, whereby once the IM, DF, and CCP's capital is exhausted, the entire market suffers a credit event, not just the counterparts who dealt with the defaulting party. Such a large systemic event involving a CCP could only be brought to an end via bail-out with taxpayer money; otherwise there is no price formation, or market itself.[34]

Recently, regulators have taken measures against this risk, for example (CPMI and IOSCO 2012) (CPMI 2016):[35]

(1) “The arrangements adopted by a CCP should be transparent to its participants and regulators” and
(2) “CCPs should also have rules specifying clearly how defaults will be handled”

Due to additional observations on avoiding indetermination in CCPs’ default management plans, in (ISDA 2017), “ISDA urges regulators and policy-makers to continue working together to finalize unambiguous and predictable CCP recovery and resolution strategies”.[36]

C. Decentralized Financial Market Infrastructures (dFMI)

dFMI Introduction: Straw Man Proposal

dFMIs are consortium entities whose members are comprised of the main participants in a market, organized in a peer-to-peer model, which is governed by dFMI participants themselves rather than a central intermediary. Governance reflects members’ interest in a smooth functioning market, minimizing the occurrence of credit risk and dealing swiftly with risk insurgence.

The Bank of England recognises this governance structure and issues recommendations on ‘governance and assurance’ stating the following:

> “In light of our evaluation criteria and assessment, we believe that now would be an opportune time to review governance and assurance, building on the

[34] A CCP is a CCP is a CCP by Robert T. Cox and Robert S. Steigerwald
[35] Resilience and recovery of central counterparties (CCPs): Further guidance on the PFMI - consultative report from CPMI (2016)
[36] Safeguarding Clearing: The Need for a Comprehensive CCP Recovery and Resolution Framework from ISDA

> achievements described above, and looking at the challenges ahead. This includes the role of the FMI supervisory committees, how best to harness individual members' contributions, and the role of third-party challenge. We also recommend that Court considers augmenting its annual discussion of FMI supervision." (p. 41)

dFMI proposes a decentralised network of connected nodes representing market participants and collectively responsible for oversight. The issue of possible misalignment of interests between a central intermediary and members can be managed and mitigated by design. By design there is no central intermediary separate from the larger network of nodes representing the interests of the market participants themselves. Market participants interact directly with each other, such that the risk of a transaction is contained within those parties involved in it. In addition, the default risk of the central intermediary, and with it the systemic risk it has historically represented, is purposely eliminated.

dFMIs are based on the principle of mutualisation: market participants pool their resources in order to deal with the failure of some members. Because none of the market participants have a central role, they cannot be too-big-to-fail. Consequently dFMIs are about risk mutualisation (among members) without risk socialisation (among taxpayers).

Compared to infrastructures of central clearing through central intermediaries, this decentralised business model reduces risk through several aspects:

1. Economic: the misalignment of interests discussed in the above CCP default example is replaced by member incentives, which are aligned with their business role.
2. Financial: operational and credit risk are no longer concentrated in a single central entity, but can be more diversified across the members.[37]
3. Technological: the single-point-of-failure of the "mainframe" central counterparty is replaced by a distributed network. Resilience comes from redundancy of data and processes across the members.

The advantages of dFMI processes over FMI processes such as CCPs are a direct consequence of the change from a centralised to a decentralised business model. Prior to the crisis, while the structure of financial markets was nominally decentralised, the functions of intermediaries were centralised. The consequence of intermediary default due to collateral shortages represented a loss for all participants, likely a chain of ensuing defaults and most importantly systemic risk. dFMIs propose a change to the fundamental architecture of today's financial system, around a rearrangement of the structures behind systemic loss and trust.

[37] The Qualifying liquid resources (QLR) of the CCPs under EMIR regulations have to cover the default of any two clearing members, a level that is approximated by the two largest members contributing initial margin defaulting. In a dFMI, parties choosing not to deal with the largest members would not be exposed to their risk.

dFMIs can fuse together the advantages of a decentralised market structure with the functions of CCPs, such that the public confidence in CCP capabilities can be met with the right alignment of interests. Investors dependent on the proper discharge of CCP functions would ultimately assume a level of risk that more accurately accords to their level of risk aversion.

While much of the financial system still runs on legacy systems, a dFMI would be built around modern technological advances that facilitate, streamline and increase the security of operations. Following the mainframe and minicomputer eras - between the 1950's and 1970's - there have been continued advances in technology including involving cryptography, distributed ledgers and additional automation. Together these support a much needed change in market structure and business model through dFMI.

Clearing and Settlement for dFMI

The evolution of client-server technical architectures to peer-to-peer technologies through blockchain technology allows for direct and real-time C&S. There is no need for a centralised counterparty to manage and provide credibility during a delayed C&S process of T+2 or longer times, or the legal and governance implications during the days it takes to transfer ownership of assets, where ownership titles can be unclear. With direct and shorter settlement times, dFMI (Figure 5) allow greater transparency and efficiency.

Functional Decomposition of dFMI for Central Counterparty Activities

How can dFMIs perform functions similar to CCPs? We start from functions 4-6 described above, from CPMI- IOSCO (2012, paragraph 1.13), which define the role of CCPs in managing default risk.[38]

dFMI mechanisms are designed to ensure that one party's default will only affect its direct counterparties and not the entire market. In the event of a major default, this eliminates the risk that a default fund from member banks, as utilised in the CCP context, may not have enough resources at the end of the default waterfall. The default of one market participant would not affect the market as a whole, regardless of the depth of a default fund's resources. This provides not a partial degree, but essentially a full degree of security against contagion.

As for price discovery, some dFMIs would record offers (bids and asks) as transactions on a blockchain, which are immutable, transparent, real-time, and available to all participants in a network, even if a node may fail. This design pattern would be applicable to both conceptual central order books and request for quotes type markets.

This is contingent upon a properly functioning market infrastructure with no technical or service disruptions. For CCPs, on the other hand, netting sets compress exposures into

---

[38] EBA and ESMA report on the functioning of the regulation (EU) no 575/2013 (CRR) with the related obligations under regulation (EU) no 648/2012 (EMIR) from European Banking Authority

a single netting set, which reduces the risk in addition to the use of a default fund mechanism. The resulting perception of CCPs as being risk-free adds to the overall credibility of CCP prices. These prices are not subject to adjustment for counterparty credit risk, and thus foster transparency and price discovery as long as the CCP is functioning correctly.

Moreover, dFMI ensures business continuity more fully than CCPs. dFMI has resilience built into the core of its design, so there is no need to rely on a separate and limited pool of funds that may not be sufficient enough to cover a certain scale of losses. Risk exposure is inherently contained between two direct counterparties transacting with each other, which bear the risk and also the consequences of potential default. CCPs merely enhance business continuity by relying on the default waterfall to provide resilience to the system in the case of one counterparty's default. If a CCP can survive despite a member's default, so can the deal with the CCP.

Finally, dFMI provides anonymity inherent to the blockchain infrastructure on which it operates, without compromising on transparency or the dynamics of efficient markets. CCPs require a more complex approach to ensure anonymity, with implications on other market dynamics. By acting as a counterpart to every trade, CCPs ensure that trading partners remain anonymous to each other. Clearing members don't need to worry about the creditworthiness of their trading partners and are free to trade with any other CCP members. Yet the downside risk of this system is that if one trading partner faces a liquidity constraint, such as borrowing a large sum of money or making a large investment, the market will not turn against it thanks to the CCP's perceived risk reducing role, maintaining high levels of liquidity.

Potential Benefits of dFMI over CCP Functions

a) Default Fund Mutualisation

As mentioned above, dFMIs are consortia where members also operate the nodes of a distributed network working on a ledger where global state is shared; commonly referred to as a blockchain.[39] On such a blockchain network, digital resources can be mutualised with no need to find a central, third party administrator to take custody of the assets. Assets can be pooled at an account controlled by a *smart contract* that can only be modified via multisignature. This ensures that only a qualified majority of the members has control over the resources. 'Smart contracts' and decentralised applications can be used to create "unambiguous and predictable" rules for the release of funds, including automatic rules that make mutualised funds available in case of

[39] Not all 'blockchains' that are promoted as 'blockchains' are an actual blockchain. Some in fact, are centralized and/or proprietary shared databases. For the purposes of this paper, a blockchain consists of peer-to-peer nodes that validate and manage a global state shared amongst all participants in the form of blocks, or containers filled with transactions; the protocol of which is open-source and not governed by a single company.

credit issues, following a codified waterfall where risk participation is proportional to risk creation.[40]

Such smart contracts can also be used for Initial Margin, which cannot be re-hypothecated and must remain segregated from the control of either party.[41]

In a peer-to-peer business model, an entity that is counterparty to every deal just in order to pool resources and construct a mutual fund is unnecessary. Mutualised, loss-absorbing capital in a purely bilateral model could exist, for instance, in the form of a cash fund to cover potential losses from cybersecurity breaches, theft, execution errors, or counterparty defaults. This would provide investors added comfort regarding business continuation and overall stability of an underlying trading system. Technology today can lower multilateral contracting and monitoring costs dramatically, making this approach much more practical than it once was.

Moreover, mutualisation can be more directly tied to the alignment of incentives among participants in a dFMI context, where the consequences of risk taking are contained among the participants of a transaction. Fee structures can be contingent upon the amount of capital contributions, as directly proportional to risk taken by individual participants. Mutualised capital contributed by investors remains linked to the outcomes of their decisions. This incentivises responsible behavior more directly than in a CCP context, where mutualised capital is deposited with a central party that will spread risk regardless of the individual contributor's risk level.

b) Credit Risk Reduction

dFMIs operate on a settlement platform that uses a digital currency, where settlement takes place at the moment a consensus algorithm is successfully executed.[42] The consensus algorithm proves the (byzantine fault-tolerant) agreement of a qualified majority of validators and runs in real time.[43] This new business model minimises trade-to-settlement time from days to hours, such that counterparty risk exposures do not accumulate but can amount for only a fraction of what they represent in FMI given current settlement delays. Rather than relying on a hopeful assumption that a CCP is risk free, this system reduces credit risk based on an objective, measurable criterion:

---

[40] 'Smart contracts' are best described as 'transactional scripts' or 'persistent scripts.' See Transactional Scripts in Contract Stacks by Shaanan Cohney and David A. Hoffman

[41] What happens if the majority refuse to sign? In one implementation, the only signature is at inception, then the smart contract follows what is written in the code. The parties cannot do anything else because the smart contract controls the Initial Margin. This is in line with regulations requiring Initial Margin to be segregated. In current regulations, the Initial Margin is not really under your control, unlike Variation Margin. This can be done with smart contracts rather than only custodians, lawyers and liquidators. A qualified majority always needs to have the possibility to change the smart contract, for errors or changes in the rules, that's what multisig is for. But the party whose initial margin has to be used can't withdraw it.

[42] Based on recommendations from the PFMIs (central bank money) and in this case, a central bank digital currency.

[43] The main benefit and purpose of using a BFT system is to operate under the assumption that a minority may become malicious.

shortening the delay between the opening of a credit exposure and its close, by means of a deal or margin settlement.[44]

Collapsing the trade-to-settlement delay to a very short time can reduce risk dramatically when coupled with delivery-vs-payment arrangements. The latter feature can be obtained without central intermediaries, using instead escrow smart contracts or other cryptographic techniques. The networks ensure that payments are triggered only if the securities are actually transferred, and vice versa. On-chain digital currencies can also be used to reduce operational risks and improve intra-day liquidity.[45]

Moreover, price discovery also improves when counterparty risk is negligible for all parties over a very short settlement delay. This phenomenon currently occurs in the overnight market, where banks can lend money to each other at a standard market rate, since a short lending maturity (less than 24 hours) makes their credit risk homogeneous and very low.[46]

In the case of derivatives, risk is reduced by shortening the interval between measurement of exposure and settlement of the corresponding collateral update, as well as by making collateral updates much more frequently than in FMI. Collateral rules can be codified through precise software implementation, reducing the scope of misalignments, automating cash flows and corresponding collateral updates and providing for automatic covenants in case of non-performance. The tools to achieve this reside in the concept of 'smart contracts,' either at layer one (all the business logic is on the blockchain) or at layer two (the blockchain works more as a settlement platform and a guarantee of correct execution).[47]

In this new business model, risk of default may be sufficiently reduced so as to make netting of a large number of long and short positions less crucial. This could surely become a replacement of today's system of counterparties, operating with a centralized third-party collector of systemic risk.

c) Business Continuation Guarantee

When a counterparty defaults in a dFMI, there is no central counterparty in between to spread the losses across the entire system in the event of insufficient recovery resources. Therefore, dFMI aims to function within a business model where default can occur among

[44] The confidence of a bail-out as a back-stop has been used to justify this.

[45] Would this require excessive collateralization? With much shorter settlement cycles, collateral required is less *not* more. However, this is a model which requires more pre-funding. See also Smart Margin Calls from Synechron.

[46] This was discussed in a related topic around a hypothetical 'narrow bank': The Fed Versus the Narrow Bank by Matt Levine and Narrow banks and fiat-backed digital coins by Alexander Lipton, Alex P. Pentland, and Thomas Hardjono.

[47] It bears mentioning that definitionaly there is a difference with how advocates of anarchic blockchains (such as Bitcoin) market "Layer 1" as a "settlement layer." Proof-of-work-based cryptocurrencies - by design - lack the necessary functions to provide definitive legal settlement finality. See Layer 2 and settlement and Settlement Risks Involving Public Blockchains both by Tim Swanson.

individual entities, with minimum or even no losses for the other counterparties. This is made possible by the short settlement delay, and the ability to automate covenants when one party does not perform.

dFMI provides no business continuation guarantee as in FMI. Deals are terminated (in case of derivatives) or cancelled (in case of securities) with little or no credit risk, and there is no replacement deal. Margin can cover replacement risk, which refers to the risk of denying the non-defaulting counterparty the gain from the canceled transaction. Yet a certain degree of liquidity risk may remain, since the derivative or the security removed could have been instrumental to other deals. A typical covenant in the case of non-performance requires deal termination and the application of initial margin, from the counterparty and network default fund, to cover the (already much reduced) loss arising from market movements.

This business continuation concept for dFMI opens yet another possibility: the concept of systemic default as alien to dFMI, so that dFMI members have no legal recourse on the assets of a non-performing party beyond the resources provided by the counterparty or pooled by the dFMI itself. This would make dFMI a market system unable to generate or spread systemic risk, opening a totally new era for financial markets.

Yet does a lack of systemic loss, necessarily result in systemic stability? In a liquid market, there is no systemic concern, since replacing a counterparty is not difficult. A parallel scenario for FMI refers to the imbalance that a CCP would suffer when a counterparty defaults, which gets diversified away across different counterparties with no systemic concern. In practice, this imbalance could be even smaller for securities, since it is not spread across a long leg between trade and settlement (Devriese 2005).[48]

This underlying liquidity requirement could be enhanced by additional measures to further ensure systemic stability. Guarantors specified by members can replace them in case they drop out of a deal. For derivatives, the imbalance could even be covered by the dFMI members themselves, through novation of defaulted portfolios.[49] As (CPMI & IOSCO, 2012) states: “in markets where a CCP does not exist, a guarantee arrangement may provide market participants with some degree of protection against losses from counterparty defaults”.

In case of dFMIs, the guarantee would apply mainly to liquidity risk, since the above arrangements cover principal and replacement losses. Referring again to (CPMI & IOSCO, 2012), “replacement-cost risk is the risk… the cost of replacing the original transaction at current market prices. Principal risk is the risk that a counterparty will lose

[48] “If technology could allow for realtime settlement, for example, participants would not need to form expectations about their cash and security holdings. Although settlement failures in response to a major disruption would still occur, multiday contagion effects would no longer arise.” Liquidity Risk in Securities Settlement by Johan Devriese and Janet Mitchell.

[49] The primary point of decentralisation is contractual: your counterpart is still your trading counterpart, not novation over to CCP. In dFMI this remains bilateral rather than trilateral. Having a single counterpart face everyone in the market means that failure of that counterpart can cause a financial crisis.

the full value involved in a transaction, for example, the risk that a seller of a financial asset will irrevocably deliver the asset but not receive payment".

As mentioned above, automated covenants can be set up to ensure market functions in the case of a non performing party. The strawman model (Figure 6) shows how a collateralized derivative can be implemented as a smart contract. The smart contract is authorized to transfer Variation Margin from the wallet of one party to that of the counterparty. Meanwhile,the Initial Margin remains under direct custody of the smart contract, in line with regulations requiring it to be segregated from the parties. The smart contract has a 2-of-2 multisignature architecture, so that it can be modified upon agreement from the parties, and not by a single party. This is an example of how multisignature can implement joint custody of an asset, in this case the Initial Margin.

d) Market Transparency

A dFMI is built upon a real-time shared ledger, and can apply cryptography in order to modulate the visibility of its contents to the public and to relevant authorities. A global settlement ledger where changes to the state of all accounts are reported at a level of detail which is sufficient to recreate the underlying transactions provides transparency, promoting market integrity and facilitating surveillance. It can significantly reduce the burden of FMIs to provide data via a plethora of reports that have shown to be inefficient, corruptible and difficult to reconcile.[50]

As described earlier, this record is shared by consortium members, each of which confirms the validity of each subsequent mutation to a ledger's state. The ledger does not violate privacy laws, since both counterparties and value exchanged are shielded by proven cryptographic techniques, which allow encrypted data to be verified without the need to see it in the clear.[51]

Transparency toward the public can exert a normalizing influence on fees and charges - and improve efficiency due to the threat of competition. For example, a dFMI can enforce norms such as a consistent approach to disclosing trading fees, providing certainty regarding the cost of trading. Without a dFMI consortium, entities such as

---

[50] "Around 85 data fields are to be reported for each transaction...Such a wide-scaled and detailed reporting implies huge data volumes. Over the first year of reporting, almost 10 billion of records were received and processed by the six TRs in Europe...the heterogeneous landscape in TR data provision and non-standardised data collection pose significant challenges for regulators accessing and analysing the data...any meaningful data aggregation requires the reconciliation of the information between the duplicated trades... the other data fields submitted by the two counterparties very often do not match, which raises the question which of the two to keep in the final database with de-duplicated trades. Even for trades reported to the same TR, there can be significant discrepancies for variables such as execution timestamp, price per contract or notional value." From Reporting of derivatives transactions in Europe – Exploring the potential of EMIR micro data against the challenges of aggregation across six trade repositories by Malgorzata Osiewicz, Linda Fache-Rousova and Kirsi-Maria Kulmala

[51] These techniques include, but are not limited to, obfuscation techniques, zero-knowledge proofs (including bulletproofs), mimblewimble, and homomorphic encryption. Certain hardware-based solutions, like SGX, are not considered fully reliable at this time due to continual exploits and compromises.

trading platforms in the retail market for digital assets may choose not to disclose their fees or to hide them within the margins charged for digital assets themselves.

The provision of high quality, timely and granular information about transactions to the authorities facilitates ease of compliance to modern mandates for reporting such as those imposed on cleared OTC derivatives. For the Regulators, if such information is taken directly from a common source system of record instead of being obtained at lower frequency through indirect systems, surveillance can be conducted in a more direct manner.

The new operating model for a dFMI based on the use of a shared ledger provides for tailored levels of access - instead of requiring third parties to slice and dice aggregated datasets into specific segments for reporting to different regulators based on their various geographical or industry mandates, it is possible to selectively mask portions of the ledger directly from certain parties based on cryptographic keys. This capability reduces the scope for mistakes being made by third parties in the pre-processing of data for presentation to the regulators, and allows for errors found to be corrected back at the source - which benefits all other users of the same data source.

e) Standardisation

The standardisation brought by central counterparties is largely derived by the mutualisation of a collective process led by market members. According to (CPMI & IOSCO 2012), "in certain OTC derivatives markets, industry standards and market protocols have been developed to increase certainty, transparency and stability in the market. If a CCP in such markets were to diverge from these practices, it could, in some cases, undermine the market's efforts to develop common processes to help reduce uncertainty."

The main effect of CCPs has been to codify a set of standards into a single rule that applies to both parties in a transaction. With a centralised solution, standardisation was ensured to be immediate across all participants. dFMIs are conducive to the same form of standardisation, since all players participate in the same network and agree on the smart contracts that regulate their business. Standardisation, in this case, builds upon a network of bilateral agreements, leading to a domino effect toward global standardisation, where potential diversification of approaches can make markets more resilient. Different players are incentivised to interact and interoperate, and thus need consistency in their interactions with a dFMI platform, which will favor a single standard of operations.

Price discovery is a key aspect that dFMI favors by promoting reliable operations and services that ensure functionality, transparency, and if needed, cash reserves for purposes akin to regulated FMI marketplaces. Otherwise, arbitrage as seen across certain digital asset exchanges can arise due to operational inefficiencies such as temporary service outages and restrictions on access to trade, withdraw or deposit funds. Outside of a dFMI consortium, trading operators trading on their own behalf within their own platforms may provide liquidity at the expense of conflicts of interest that could hinder the integrity of markets. Front-running customer order flows, price manipulation, inflating and deflating prices are practices that would undermine price discovery, which dFMI standardisation measures would mitigate.

f) Multilateral Netting

We have seen above that a dFMI reduces credit risk by shortening settlement delays, enforcing atomic swaps, reducing misalignments and pooling resources. While payment or exposure netting with a single counterparty can also be customary for dFMIs, multilateral netting is not part of the native features of dFMIs because trading remains bilateral. With a central counterparty, multilateral netting and compression are by-products. Two opposite positions with two counterparties B and C cancel out when B and C are collapsed into a single party. Netting and compression are also achievable in a system without a central counterparty. dFMIs can facilitate this process by performing computations collectively and bringing to consensus the correct result.[52] In a dFMI, all deals take place through the ledger, and netting rounds can be computed by members through multilateral offsetting of gross obligations. This provides compression ratios of multilateral netting but a much lower amplifier in the case of default: only the counterparts to the defaulting party suffer a credit event, whereas everyone else in the offsetting cycle only suffers a liquidity event.

Moreover, netting in a dFMI context could solve potential conflicts of interest that exist in CCPs. Computations require knowledge of the global state of contracts, which is usually private information of the parties.[53] Today, netting is allowed only for members trading directly with the CCP, so the CCP not only knows of all the deals, but is also a party to all the deals. As an alternative, related technology for sharing data for computation without revealing private information consists in using trusted execution environments, where computations are performed in private enclaves.[54] In principle, regulated entities, such as Trade Repositories, already have access to the global state of contracts required for multilateral netting. This technological layer allows multilateral netting without the risks intrinsic to having single third party entities responsible for data privacy and security, while simultaneously guaranteeing correct netting computations. In a dFMI, on the other hand, a trusted third party may perform the computations required

[52] There are several ways to get the computations done without a central counterparty. One can use verifiable computations and trusted execution environments. In this case one or several machines only execute the pre-agreed code and everyone can verify it via proofs "similar" to digital signatures. There is still some "trust" in the technology, but not the reliance on a central entity fully responsible for computations.

[53] It bears mentioning that several platforms that market themselves as “blockchains” but are unable to share state amongst all participants should not be classified as an actual blockchain. See also: The Path of the Blockchain Lexicon (and the Law) by Angela Walch

[54] "A Trusted Execution Environment (TEE) is a hardware based technology that executes only validated tasks, produces attested results, provides protection from malicious host software, and enforces confidentiality of shared encrypted data," Enterprise Ethereum Alliance Off-Chain Trusted Compute Specification V1.1

for multilateral offsetting, without becoming a party to all deals. This is already possible with the current framework[55]. Furthermore, today's financial cryptography offers methods to perform encrypted computations on data that remains private even when shared. Cryptography solutions include obfuscation, zero-knowledge proofs and/or multiparty computations.

For most derivatives, computations involved in netting are very complex, and thus not applicable for immediate standardisation. The above dFMI solutions are likely to reach scale for securities trading sooner than for derivatives trading.

g) Cross-Margining Agreements

dFMI are much better suited than a CCPs to pool capital across entities to prevent losses, as defined by cross-margining agreements. According to (CPMI & IOSCO, 2012), a cross-margining agreement is an "agreement among CCPs to consider positions and supporting collateral at their respective organisations as a common portfolio for participants that are members of two or more of the organisations".

Maintaining enough collateral to absorb risk is key for the survival of CCPs. Yet there have been incidents where insufficient collateral caused default losses to spread. An important historical example of this is in energy clearing, where the default of one participant resulted in an unsuccessful auction: a turn of events that was altogether unanticipated. For a Norwegian power trader, the costs to replenish the default fund were staggering, at over $100 million euros.[56] Scenarios like this bring to question the role of the CCP. In theory, one potential strategy for CCPs could be to pool resources together with cross-margining agreements. Such agreements are strongly favoured by regulators, and yet they are not frequent among CCPs (likely due to their resistance to interoperability, as discussed in the dFMI challenges below). This is unfortunate since cross-margining agreements are of crucial importance for reducing systemic risk.

Moreover, exposure compression within separate markets may not reduce global exposure if deals are allocated across markets without coordination.

In a dFMI model, exposure compression scales to a global level more easily than in a central clearing model. Different dFMIs can interoperate and merge without changing their governance model, unlike CCPs. As a result, this can open new scenarios for managing and preventing systemic risk.[57]

---

[55] MiFIR Recital 8: "Portfolio compression may be provided by a range of firms which are not regulated as such by this Regulation or by Directive 2014/65/EU, such as central counterparties (CCPs), trade repositories as well as by investment firms or market operators."(emphasis added)
ESMA /2014/1569, p. 441: "Multilateral compression is usually a service provided by a third party service provider within a legal and contractual framework that applies to all participants in the compression"

[56] How a Lone Norwegian Trader Shook the World's Financial System from The New York Times (2019)

[57] A strawman DCN could start with the creation of a DCN via a single private key that manages the contract. This could be seen as the operating company and can reference legacy infrastructure (such as

Potential Challenges

a) Regulatory Oversight

Arguably the main challenge to implementing dFMI at scale is the level of regulatory complexity we currently face, both within and across different jurisdictions globally. Several blockchain trading platforms have either chosen not to comply or remain unprepared to comply with US securities laws at a state and federal level. These platforms often take less responsibilities for consumer protection in comparison to regulated mainstream exchanges. With regard to the risk of money laundering and illicit activity, they may not be equipped to verify the origin of funds, so as to confirm trades are "clean". Nor do they provide trading protections common in FMI contexts, such as liquidity reserves.

Consumers and public entities may not be able or willing to conduct trades in the absence of pre-established protections such as liquidity reserves, which in turn could affect low levels of confidence and adoption of dFMI. They may demand a level of regulatory safeguards for trading on dFMI systems that is parallel to the safeguards in FMI fiat and securities markets. To meet customer expectations, dFMI must tackle this issue if it aims to achieve scale in the financial system.

Moreover, managing and regulating a consortium of players presents additional complexities over regulating a single intermediary entity. On a network level, dFMI would have to comply with regulations in multiple jurisdictions, which may present certain contradictions in their requirements. Yet dFMI can cooperate with authorities by leveraging transparency with regulators, which, as stated before, can be observer nodes in the network. It can also be helpful to keep a white list of AML/KYC checks off-chain.

b) Standardisation

dFMI can incentivise widespread standardisation due to the connectivity and interoperability they support across market participants. Yet this presents challenges in implementing consistent norms on a global, cross-jurisdictional level, especially when local standards and regulations may contradict each other. Standardisation for dFMI thus becomes less drastic than for FMI, such that different approaches to operations may coexist within a broader network. These differences need to be accounted for in ways that will not hinder the consistency of processes, especially for cases of disputes.

In FMI standardisation is imposed by each vendor to its clients. Some approaches are more effective, and some less. dFMI cannot follow this model, as there would not be a need to follow a specific vendor and its interests while defining standards. Yet private

---

an RTGS). In terms of governance, more autonomous governance models could be set up, to be owned by the constituent members. These could be similar to decentralized autonomous organizations (DAOs).

entities, such as the myriad of FMI intermediaries, imply regulatory boundaries that limit the scope of market coverage for standardisation: an issue no longer relevant for dFMI because the role of third parties would be replaced by market participants themselves.

Thus standardisation for dFMI adjusts to be both more adaptable to the needs of specific members' activities and more easily adopted by broader networks of connected nodes relative to the current CCP context. dFMI represents a more easily prevalent yet less radical form of standardisation: two parties may want to regulate their netting with a different model than the average norm, approved by other parties sharing the management responsibilities of a particular ledger or network.

Because standardisation is partial and less immediate than in the CCP case, it can lead to uncertainty in the regulatory realm. Therefore, off-chain and legally enforceable contractual agreements would be better suited to establish the rights, benefits and obligations of participants, rather than solely relying on source code, the underlying blockchain or network attributes. The latter technical attributes should be consistent with the contractual agreements, which provide clarity for business operations to ensue. This also allows for flexibility, analysis and discretion where necessary in the application of rules on a case-by-case basis.

c) Joint Computations & Privacy

In the absence of CCPs, there are no other operating frameworks that reliably provide privacy and multilateral netting at the same time. One particular advantage of the CCP structure is that it provides obfuscation services: a member of a CCP will not know other members' positions. Moreover, as CCPs have increased in size and importance over time, along with their underlying systems to provide services, greater risk carried by these third party entities translates into a greater level of commitment that better aligns their interests with those of market players.

It is possible to perform multilateral netting without CCPs, but doing so presents important challenges. dFMI structures can perform the same level of multilateral netting that currently requires a central party. Yet while the technology available today for providing multilateral netting could be made available for dFMIs, they would still have to perform the same replication and flows without CCPs. Implementing this could be a challenge for dFMI, in a way that multilateral netting also implies concentration risk and model risk.

Yet as discussed before, CCPs are also not as bulletproof as they can be assumed to be because FMI structures operate upon placing risk on a third party whose interests at their core are not aligned with those of market players. The design of a CCP-based structure does not fully guarantee incentive alignment with market players. Furthermore, regulators' interests may not perfectly align with those of CCPs, market members or core elements of financial stability. For instance, while members want choice, regulators want transparency and market stability. CCPs, on the other hand, are ultimately for profit entities, often publicly traded companies which derive revenue from the need to provide services like risk modelling and operational efficiencies.

Implementation of dFMI functionalities could help provide the benefits of CCPs in this realm to market participants, in a way that better aligns incentives across stakeholders.

d) Collateral Management

We have seen the advantages of dFMI, specifically Decentralized Clearing Networks (DCN), in operating automatic covenants, holding initial margin segregated from the accounts used for variation margin, moving collateral, standardising computations and ensuring collateral movements on par with derivatives cash flows. Yet implementing such a model for derivatives is complex because the time to maturity of derivatives can be several years or even decades. Moreover, counterparty risk from trade to settlement can be extensive and long, and can also involve changes in regulations, disputes and restructuring. dFMIs need oracles for computing collateral amounts, a digital currency with settlement finality, and appropriate changes to regulations, regarding in particular collateral management at default. dFMIs for cash products share some of the same challenges. As a result, these operations eliminate discrepancies of cash flow payments, as addressed by a number of papers. Overall, DCN utilities can be much more elaborate for long term collateral management, as opposed to short term spot cash products.

e) Mutualisation of Capital

Mutualisation of capital in a dFMI context would imply proper alignment of incentives, which is key in order to ensure the completion of deals and the greater sustainability of dFMI over time. While different mechanics that apply to derivative CCPs can be factored into the functionality of blockchain-based dFMI systems, this is challenging. The FMI business model borrows from a long tradition of centralization of mutualized assets on the books of a third party, while a decentralized model requires an important change in business models and contracts, still to be detailed.

f) Liquidity

Implementing a decentralised business model for dFMI based transaction operations would require a certain degree of scale in order to sustain adequate market dynamics, where buyers find enough sellers and lenders find enough borrowers to transact on a peer-to-peer basis. This is the essence behind network effects. Achieving that degree of scale requires alignment of incentives across parties involved, as well as buy-in from participating entities. This may require high level agreements at an institutional level, as well as technical updates which may take significant time and effort to complete. One example of a challenge toward achieving the right conditions to support liquidity in dFMI could be resistance from existing CCP structures to changes proposed on a regulatory and market infrastructure level. There is also a debate around the utility of *tokenisation* with respect to providing additional liquidity to relatively illiquid assets.[58]

g) Implementing Interoperability

While interoperability is crucial for dFMI to scale, this could resurface a longstanding argument between regulators and clearinghouses, placing dFMI at odds with clearinghouses' advocacy efforts against interoperability. This dispute emerged immediately after the crisis and continues to persist today.

While regulators have favored interoperability, clearinghouses have been incentivised to preserve their business expansion prospects and revenue streams in ways that undermine interoperability. They drafted a number of letters and papers to present to regulators, arguing that differences in risk models (different businesses) across clearinghouses would make interoperability risky. For instance, a very large clearinghouse could net many trades internally and create margin efficiencies for its own clients. Another clearinghouse with less clients and less or financial instruments traded has a different business model. Therefore, trying to connect these two entities with divergent attributes could create more risk.

One component of this argument involves interoperability in equities markets. In the EU there are several cash equities markets: Bob can clear part of his shares in one clearinghouse and the rest in another. He would prefer the two to communicate with each other so that the risk is not segregated which is beneficial to Bob as a client from a margin perspective. While there interoperability exists to some extent in the EU, in the United States there is only one clearinghouse. Therefore some aspects of dFMI could be useful by promoting market competition and implementing an interoperable system. Yet each clearinghouse is incentivised to have all of the business.

The same trend has occurred with derivatives. Just after the crisis, regulators pushed derivatives onto clearinghouses, which readily accommodated. Alice could trade outside of a normal trading venue and agree on a price. The trade was then sent to an exchange, where pre-matched OTC derivatives and later exchanges would send it to a clearing route. Pricing would be agreed upon between Bob and Alice. Many exchanges adopted this route, which would go through the clearinghouse and increase their revenues. It was beneficial for both exchanges and clearinghouses, which had previously operated in vertical silos. Yet while regulators had pushed for improving interoperability for years, clearinghouses argued that this would increase risk rather than decreasing it. IOSCO had tried to promote clearinghouses with derivatives, but clearinghouses replied stating that the risk models and technology used (operational models) between them were too different.

[58] Tokenisation which is a broad, germane topic, may not be a prerequisite for dFMI, and a number of early initiatives are underway to leverage the benefits stated above in ways that support liquidity levels for digital assets, which may include both tokenised and non-tokenised value traded on a blockchain.

Regulators, on the other hand, eventually favored interoperability precisely due to the risk of clearinghouses becoming excessively large. Over time, regulators continued to advocate in favor of interoperability, based on the fact that clearinghouses were not well capitalized. What is the real endpoint, who provides backing if everything fails?

Clearinghouses are connected to central banks, a development that was beneficial for the short term but could present additional risks for the long term. Moreover, entities were more interested in competing with one another to generate additional revenue rather than maintain the quality of their service. This is a challenge for dFMI, but also shows an additional benefit: reducing the incentives against standardisation. Finally, this is yet another example of better interest alignment for dFMI, in this case between dFMI and regulators. Yet given the historical context and potential measures to curb interoperability due to clearinghouse lobbying, dFMI may have to collaborate closely with regulators and ensure the right regulatory landscape to protect interoperability in its decentralised operations.

h) Seamless Execution of Trading-Clearing-Settlement

dFMI consortia need to operate on technology that can support high volumes of traffic and rapid trading activities, as observed in mainstream financial markets. Current distributed ledger-based platforms frequently lack these capabilities, and often experience disruption and significant errors when attempting to process multiple simultaneous trade requests. dFMI should propose a structure to prevent the technical issues of early distributed ledgers that have shown to cause exchange outages for the span of hours, errors in pricing, restrictions to users' ability to access their own funds, and poor overall service. One possibility could be to implement custom-built features to support specific markets and dynamics of supply and demand.

Clients may be turned away by the lack of pre-trade and post-trade services, unless dFMI consortia take initiatives to offer them. These services could include analytical tools for decision making prior to trades, as well as trade confirmations, reports, and pricing details after trades. Clients may demand tools they are familiar with in the FMI context, to monitor and manage blotter, positions, and technical analysis strategies. These added services, while largely off-chain, could enhance transparency and effectiveness while lowering trading risks.

i) Centralised Intermediation and Security

dFMIs bring a form of disintermediation to many of the functionalities currently conducted by the FMIs. This is primarily through a radical change of the existing business model to support financial transactions, but it does not imply the disappearance of the current FMIs as accountable legal entities. Whenever present forms of market infrastructure generate economies of scale that cannot be replaced in a distributed design, such forms of centralisation will remain.

Current regulations define the role of a CSD in maintaining a legally relevant list of who owns each security. Even when these roles become distributed and no longer require a centralised body, additional roles will emerge that still require proper intermediation. Key management and custody are paramount examples. Other tasks may be associated with KYC/AML screening for all account holders, or the possibility for regulators and other authorities to screen the cryptographic obfuscation layer that preserves privacy. From the standpoint of risk reduction related to concerns of illegal activity, dFMI trading platforms can implement features to make the history of trades available for trade participants, and upon request by regulatory agencies for the purpose of transaction monitoring. These measures would require discretion in light of the use of private keys and private data.

Customer protection measures are another area that requires a centralised authority to ensure credibility. An inherently decentralised system for CCP functions essentially collapses the space and time between buyers and sellers. Yet when dealing with money transfers and ownership of assets, custodial and fiduciary responsibilities come into play, as well as governance structures to ensure reliability and credibility of operations. This entails adequate collaboration with regulators to ensure a sense of trust and transparency. It also calls for adequate regulations to standardise consistent best practices, as well as the role of centralised authorities to ensure security and credibility that are key for scale, without interfering with direct, peer-to-peer interactions among market players.

D. Conclusion

The central thesis of this paper is that financial services mechanisms and governance structures have not kept pace with the evolution of computing, and thus fail to capitalize on important risk reducing opportunities in the globally connected financial ecosystem where we operate today.

From trading to clearing and settlement, financial market infrastructures and their participants are central to the operation of our markets. With the introduction of technologies to financial services, the market started operating on relatively siloed market infrastructures, in a world perceived as completely connected from the user's perspective. This became a top concern for regulators and policy makers after the financial crisis of 2008. The call for transparency and better risk management brought the need for connectedness across market structures, both horizontally and vertically across the value chain. The available technology, access and governance paradigms have poised significant challenges and unveiled a range of misaligned incentives resulting from the increased intermediation.

Meanwhile, the demands of end users of our markets started to evolve. New areas of differentiation furthered innovations for financial services, including the distribution of new products, speed, transparency, choice and on-demand capabilities. These digital capabilities emerged as vital to address increasing customer demands. In addition to meeting these requirements, core infrastructure needed to comply with regulatory requirements and standards such as the PFMIs. The dFMI concept is a proposed path to address the challenges of our market structure today, as we build the future of product development and distribution in financial markets.

Significant amount of work is still required in order to begin implementing dFMIs. This can imply the transformation of existing infrastructures, as well as the emergence of new ones. As building blocks of this paradigm, the recent and most well known initiative includes the Utility Settlement Coin initiative, which is now being developed by a consortium backed entity. The list of additional proposed initiatives is long and involves changes in business models, such as supporting trading of listed and over-the-counter instruments from a single inventory.

Moreover, broader trends such as tokenisation should be considered as an opportunity to build the next generation of dFMIs.[59] Practical examples of this construct take the form of digital assets, including tokenised securities and cash.[60] As our markets move from dematerialised to digital assets, the markets supporting these instruments started getting organised with decentralised attributes. The upstream product and operational efficiency of tokenised cash or peer-to-peer cash initiatives will facilitate a range of decentralised functionality.[61] Yet challenges remain in tying a new and more resilient infrastructure with business models that do not reintroduce intermediation through single-points-of-trust.

---

[59] In the realm of asset tokenisation, liquidity constraints are an important consideration. Initially, tokenised assets may not be traded as expected or as required in order to maintain adequate volumes to sustain market efficiency and price discovery. This could pose significant implications on trade execution, where low and fragmented levels of demand may hinder proper C&S functions. A proper legal and regulatory framework to support should incentivise adoption and liquidity, so as to promote the development of tokenised assets to run on dFMI platforms. With tokens becoming adequate legal representatives of their underlying assets and value, this could present a sensible legal proposition to support a decentralised infrastructure. This should provide the ability to move in and out of contracts legally and efficiently. In the absence of intermediary fees, trades in tokenised assets can be more cost effective than in FMI structures, which would further support liquidity levels once the right network effects are achieved. In addition to cost savings, the higher transparency, efficiency of trades, anonymity and security are all attributes of a dFMI that would eventually support liquidity levels.

[60] On an economic level, markets should initially tokenise assets where the benefits above present a clear advantage for trading financial instruments in existence today. These should also be financial instruments for which there is a strong demand. On a technical level, it is important to determine the right blockchain structure, with the right economic incentives in place, to sustain an adequate market dynamic for a tokenised asset. These factors could ultimately determine the use cases for which tokenised assets acquire adoption, the possibility of scaling and ultimately incentivise liquidity overall across dFMI.

[61] We contend that peer-to-peer cash must incorporate global state otherwise the network is bifurcated with single-points-of-trust maintaining control of key infrastructure. This is a systemic risk and should be avoided. Several organizations have attempted to re-intermediate the network through business models involving licenses to these key pieces of infrastructure. This is a step backwards and historically results in vendor lock-in and specifically, the Hold Up Problem. See also Wholesale digital tokens from CPMI (2019).

Concepts outlined in this paper have begun moving from theoretical stages to a practical application.[62] As a whole, market participants have the opportunity to innovate around key function and decentralise some of the functionality as relevant, while addressing some of the challenges of the FMIs outlined in this paper.

Acknowledgements

We would like to thank Pinar Emirdag and Martin Walkerfor their numerous contributions to this paper.

References

1. Carstens, Agustín "The future of money and the payment system: what role for central banks?" speech given on December 5, 2019
2. Monte, Daniel, and Roberto Pinheiro. "Costly Information Intermediation as a Natural Monopoly." *Available at SSRN 3296978* (2018).
3. Löber, Klaus, and Aerdt Houben. "Central bank digital currencies." *report submitted by the Committee on Payments and Market Infrastructures Markets Working Group, Bank for International Settlements, Basel* (2018).
4. Löber, Klaus. "Wholesale Digital Tokens." *report submitted by the Committee on Payments and Market Infrastructures Markets Working Group, Bank for International Settlements, Basel* (2018)
5. Winn, Jane Kaufman. "Couriers without luggage: Negotiable instruments and digital signatures." *SCL Rev.* 49 (1997): 739.
6. Kroszner, Randall. "Central Counterparty Clearing: History, Innovation, and Regulation." *Economic Perspectives* 30, no. 4 (2006).
7. Madnick, S. Evolving IT Architectures: From Mainframes to Client-Server to Network Computing. (1998).
8. Frato, David, and Reiners, Lee. A New Source of Systemic Risk: Cloud Service Providers. (2019).
9. Galuba, Wojciech, and Sarunas Girdzijauskas. "Peer to Peer Overlay Networks: Structure, Routing and Maintenance ." (2009): 2056-2061.
10. Wetherilt, Anne. "Market structure developments in the clearing industry: implications for financial stability." *report submitted by the Committee on Payments and Market Infrastructures Markets Working Group, Bank for International Settlements, Basel* (2010).
11. CPMI Glossary 2016.
12. G20 Leaders Statement: The Pittsburgh Summit. (2009).
13. Bank for International Settlements (BIS)/International Organization of Securities Commissions (IOSCO). "Principles for Financial Market Infrastructures." (2012).
14. Lipton, Alexander. "Toward a Stable Tokenized Medium of Exchange." (2019).
15. CPMI-IOSCO, PFMI Number 4: Credit risk
16. Lipton, Alexander. "Systemic Risks in Central Counterparty Clearing House Networks ." (2018).
17. Khwaja, Amir. "How cash is held by clearing houses." *Clarus* (2016).
18. Links to EACH Member CCPs statistics in line with the CPMI-IOSCO PQD from EACH
19. CPMI & IOSCO, 2012
20. Evaluation of the Bank of England's approach to financial market infrastructure supervision Independent Evaluation Office of the Bank of England. (2017).
21. The Impact of a No-Deal Brexit on the Cleared Derivatives Industry from FIA (2017) and Cliff Edge Effects under EU Law in a No Deal Brexit Scenario from ISDA (2018).

[62] While CCPs might be a better option in some respects, some of their failures can be solved with dFMI capabilities. Advantages of CCPs are greater advantages for dFMI overall.

22. ISDA recently published "CCP Best Practices" (2019) which looked at two specific clearing members that have defaulted in the past five years.
23. Bignon, Vincent, and Guillaume Vuillemey. "The Failure of a Clearinghouse: Empirical Evidence." *Review of Finance* 24, no. 1 (2020): 99-128.
24. Cox, Robert T., and Robert S. Steigerwald. "A CCP is a CCP is a CCP." *Federal Reserve Bank of Chicago, PDP* 1 (2017).
25. Resilience and recovery of central counterparties (CCPs): Further guidance on the PFMI - consultative report. CPMI (2016).
26. Safeguarding Clearing: The Need for a Comprehensive CCP Recovery and Resolution Framework. ISDA. (2017).
27. EBA and ESMA report on the functioning of the regulation (EU) no 575/2013 (CRR) with the related obligations under regulation (EU) no 648/2012 (EMIR) from European Banking Authority (2017)
28. Cohney, Shaanan, and David A. Hoffman. "Transactional Scripts in Contract Stacks." *U of Penn, Inst for Law & Econ Research Paper* 20-08 (2020).
29. Smart Margin Calls from Synechron
30. Morini, Massimo. Smart Contracts for Derivatives and DvP. (2018).
31. Levine, Matt. "The Fed Versus the Narrow Bank." (2019)
32. Lipton, A., A. Pentland, and T. Hardjono. "Narrow banks and fiat-backed digital coins." *Capco Institute Journal of Financial Transformation* 47 (2018): 101-116.
33. Swanson, Tim. Layer 2 and settlement (2017) and Settlement Risks Involving Public Blockchains (2016).
34. Devriese, Johan, and Janet Mitchell. "Liquidity Risk in Securities Settlement." *Journal of Banking & Finance* 30, no. 6 (2006): 1807-1834.
35. Osiewicz, Malgorzata, Linda Fache-Rousova, and Kirsi-Maria Kulmala. "Reporting of derivatives transactions in Europe – Exploring the potential of EMIR micro data against the challenges of aggregation across six trade repositories." *BIS Report* (2015).
36. Walch, Angela. "The Path of the Blockchain Lexicon (and the Law)." *Rev. Banking & Fin. L.* 36 (2016): 713.
37. MiFIR Recital 8
38. ESMA /2014/1569, p. 441: "Multilateral compression is usually a service provided by a third party service provider within a legal and contractual framework that applies to all participants in the compression"
39. Erwing, Jack, and Schreuer, Milan. How a Lone Norwegian Trader Shook the World's Financial System from The New York Times (2019).
40. Walker, Martin. Front-to-Back: Designing and Changing Trade Processing Infrastructure. (2018).

Figures

Fig 1. Post-Trade Risks

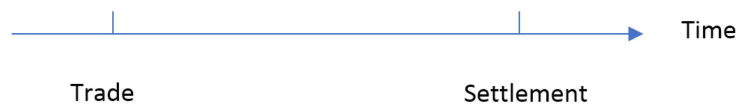


Fig 2. Exposures among 3 participants

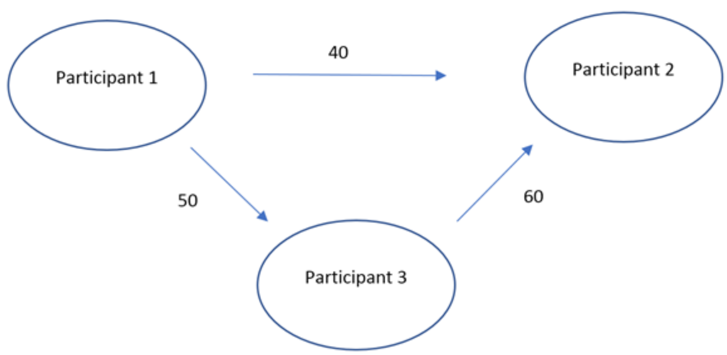


Fig 3. Exposures with a CCP

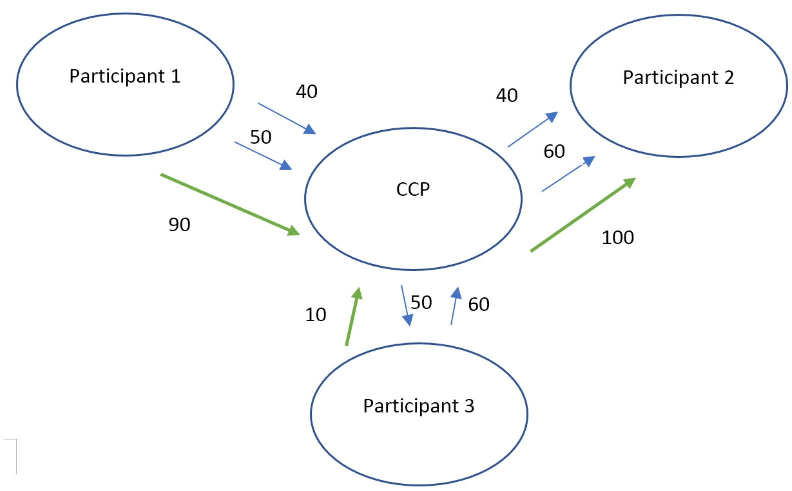
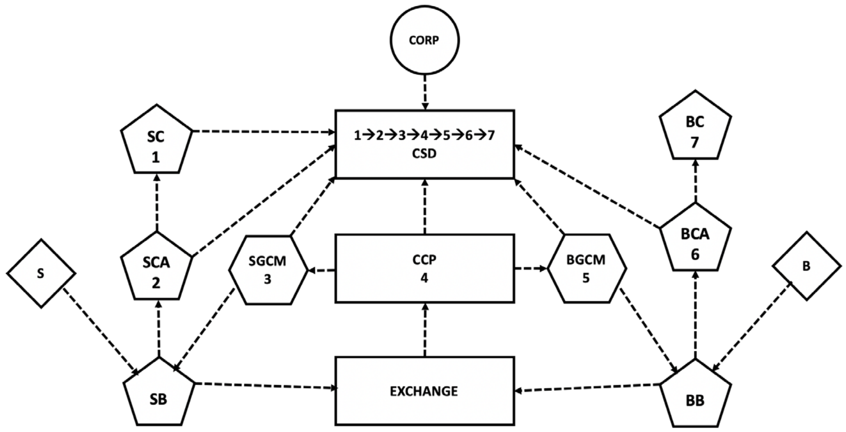


Figure 4: Current State of Trading, Clearing and Settlement

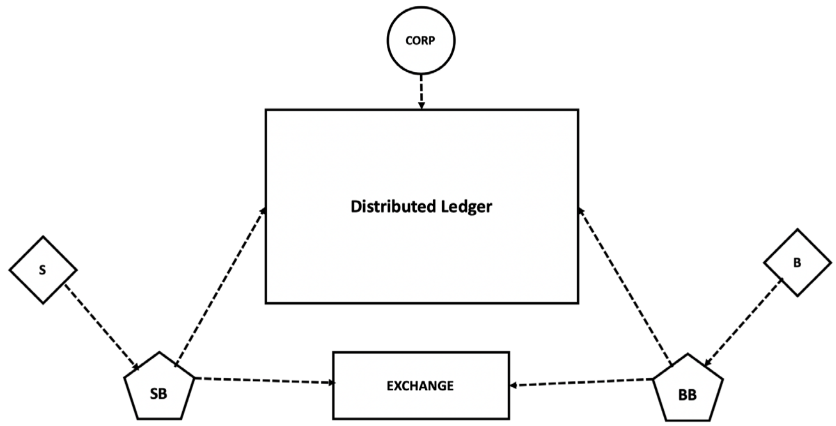


- Seller (S) instructs her Broker (SB) to sell a security. At the same time, Buyer (B) instructs her Broker (BB) to buy this security.
- The exchange matches both brokers, SB and BB. The exchange can be organized in a variety of ways, for instance, as a Limit Order Book (LOB).
- When the orders are matched, the information is sent to Central Counterparty (CCP=4), where the trade is novated. As a result, the trade is transformed into a pair of trades:

    1) a sale of the security by Seller's General Clearing Member (SGCM=3) representing the SB to the CCP

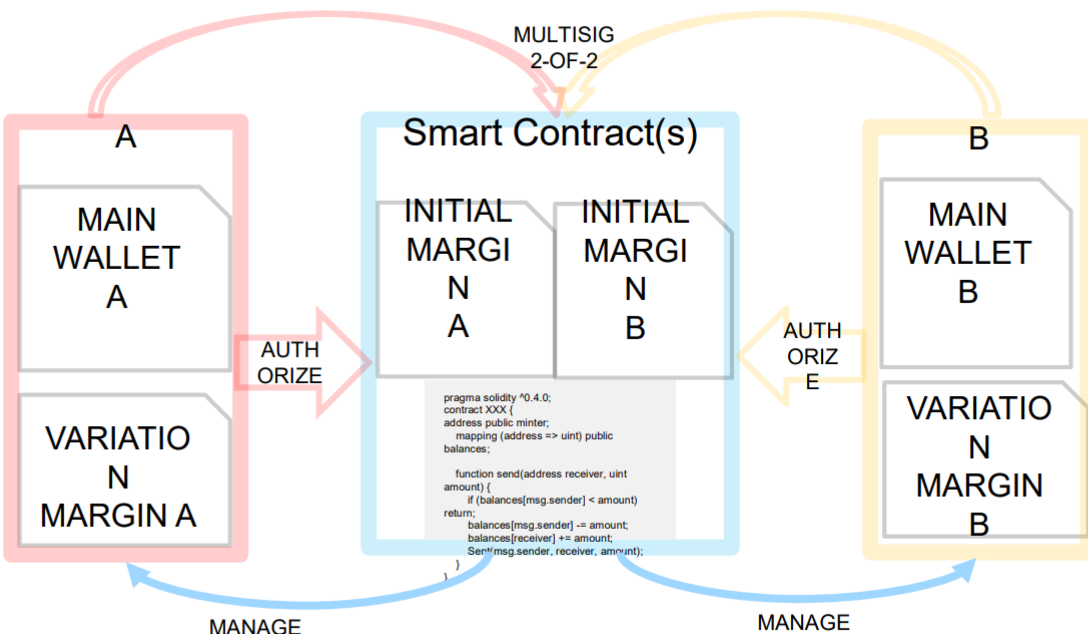
    2) a sale of this security by CCP to Buyer's General Clearing Member (BGCM=5) representing the BB to the CCP
- SGCM asks SB to deliver the corresponding security.
- SB sends this request to Seller's Clearing Agent (SCA=2), who, in turn, forwards it to Seller's Custodian (SC=1).
- A series of transfers of the security ownership take place in Central Securities Depository (CSD):
  (A) from SC to SCA (1→ 2)
  (B) from SCA to SGCM (2→ 3)
  (C) from SGCM to CCP (3→ 4)
  (D) from CCP to BGCM (4→ 5)
  (E) from BGCM to Buyer's Clearing Agent (BCA=6) (5→ 6)
  (F) from BCA to Buyer's Custodial (BC=7) (6→ 7)
  As a result, the security in question originally held by SC is now held by BC. The flow of money, which is not shown in the diagram, occurs in the opposite direction than the flow of the security from seller to buyer as described above.
- It is important to note that brokers are not always members of CCPs, and a seller-buyer trade can connect a seller to a CCP

Figure 5: Future State of Trading, Clearing and Settlement



Functions of most agents are replaced by the power of distributed ledger. Further details can be found in A. Pinna, W. Ruttenberg, (2016) Distributed ledger technologies in securities post-trading. Revolution or evolution? ECB Occasional Paper Series, and A. Lipton, (2018) "Blockchains and distributed ledgers in retrospective and perspective", The Journal of Risk Finance, Vol. 19 Issue: 1, pp.4-25.

Figure 6



(Morini 2018)

Annex

In 2012, the International Organization of Securities Commissions (IOSCO) and the Basel Committee on Payments and Market Infrastructures (CPMI) issued a foundational regulatory document that gives the cardinal rules and standards for Financial Market Infrastructures (FMIs). In their definition, FMIs are *payment systems, central securities depositories, securities settlement systems, central counterparties* and *trade repositories*.

The document is called the Principles for financial market infrastructures (PFMI from now on) and suggests application of similar principles also for infrastructures not formally included such as *trading exchanges, trade execution facilities,* or *multilateral trade-compression systems*.

There are 24 principles divided into nine macro-principles:

1. *Organization* (principles 1-3)
2. *Credit and Liquidity Management* (principles 4-7)
3. *Settlement* (principles 8-10)
4. *Depositories and exchange systems* (principles 11 and 12)
5. *Default Management* (principles 13 and 14)
6. *Business & Operational Risk Management* (principles 15-17)
7. *Access* (principles 18-20)
8. *Efficiency* (principles 21 and 22)
9. *Transparency* (principles 23 and 24)

Some of these macro-principles address general issues. This the case for Organization, Operational Risk, Access, Efficiency, Transparency. The other macro-principles regard more specific financial issues.

The general macro-principles are transformed by the adoption of peer-to-peer, distributed systems based on a shared ledger. Consider for example *Access*. The PFMI requires that "an FMI should have objective, risk-based, and publicly disclosed criteria for participation, which permit *fair and open access"*.[63]

Fair and open access is a native feature in a peer-to-peer system, to an extent that may exceed the expectations of regulators in 2012. When building over peer-to-peer technology, open access is satisfied by construction, so that the institution deploying and regulating a permissioned dFMI will be able to focus on designing risk-based rules for access which can even be codified into the network protocol, achieving objectivity and disclosure well beyond legacy technology. A self-sovereign approach to identity management, based on a chain of market attestations, can be useful in building a risk-based participation criterion.

[63] Open in the distributed systems sense, not specific to cryptocurrencies. For instance, there are incentives for someone to participate and share using BitTorrent.

Another such topic is *Transparency*. For systems that are based on a shared global ledger, transparency, in the sense of full availability of reliable records of all market objects and events, is an existential condition. Principle 24 focuses on Trade Repositories by requiring them to "provide timely and accurate data to relevant authorities and the public in line with their respective needs."

A dFMI is built upon a real-time, accurate shared data ledger, and will be able to use cryptography in order to modulate the visibility of the ledger to the relevant authorities and to the public, removing the need for FMIs to provide data via a plethora of inefficient, corruptible and difficult-to-reconcile reports. Here new roles emerge, such as the capability to process and summarize information from the ledger for regulatory monitoring, and the management of the credentials controlling the cryptographic obfuscation of shared data, also for legal and judiciary requirements.

Principle 24 addresses the transparency requirement on the procedural side: "An FMI should have *clear and comprehensive rules and procedures*", and such rules must be "*publicly disclosed*". The same point is touched upon within the first macro-principle, *Organization*, where in Principle 2 the FMIs are required to "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".

A dFMI is based on a technology stack which has profound influence on governance and operational procedures. A dFMI works by applying the rules of a protocol, and fulfills its role through a consensus algorithm. In stake-based consensus, objective market criteria decide upon the relevance of each player, allowing for the design of forms of governance that supports safety, efficiency, and stability through alignment of economic incentives.

Beyond consensus, most of the dFMI business processes will be codified as some form of *smart contract*. Therefore, rules and procedures in a dFMI are made transparent into code and their clarity is attested by *determinism*: if run by different entities on different systems, they will lead to same state transition and same transformation of inputs into outputs. In today's markets, FMIs have made a large effort to increase the clarity of their rules. Yet, being paper-based and subject to large areas of interpretation, judgement, and variations, massive uncertainty and arbitrariness still exist. A dFMI will be natively based on a set of clear deterministic rules, and decisions requiring judgment will be streamlined and conferred to the relevant stakeholders.

Operational Risk is covered in Principle 17. This principle focuses on *business continuity management* and advices that "systems should be designed to ensure a high degree of security and operational reliability". In Annex F, regulators present the "oversight expectations applicable to critical service providers" and require critical FMIs guarantee "reliability and resilience".

On resilience, again distributed architectures may surpass the expectation of regulators. In the explanatory notes we read that "each site should have robust resilience based on the duplication of software and hardware". In a really distributed system, far more than duplication is implicit in the architecture. All users are network nodes, and in a basic design all of them replicate the entire database, achieving maximum resilience. In a more advanced design, forms of *sharding* can avoid the poorly scalable requirement of full replication in all nodes, while providing at the same time the desired level of redundancy of data across multiple parties, well beyond sheer duplication.

The last general area is Efficiency. In spite of the fact that a distributed system is not, from a performance point of view, more efficient than a decentralized one, dFMIs seem to fulfill this requirement in the PFMI interpretation. Principle 21 says: "An FMI should be efficient and effective in meeting the requirements of its participants and the markets it serves". A peer-to-peer technology is particularly effective in serving its permissioned market participants, since it is not mediated by the approval of layers of centralized intermediaries and can potentially operate 24h with no national or geographical barriers.

The requirements of Principle 22 are more specific: the need for efficient *payments, clearing, settlement* and *recording*. We have already considered recording when we addressed Transparency: detailed, transparent and resilient recording is inherent in a dFMI based on a shared ledger with decentralized consensus. Settlement and clearing are specifically the topic of two other macro-principles that we cover below. On payments, this involves a deeper discussion of cash-on-ledger typically described via CBDC.