University of Edinburgh
School of Law

Research Paper Series

No 2020/16

# The Architecture of Decentralised Finance Platforms: A New Open Finance Paradigm

**Emilios Avgouleas**
Chair of International Banking Law and Finance
University of Edinburgh – School of Law
Emilios.Avgouleas@ed.ac.uk

**Aggelos Kiayias**
Chair in Cyber Security and Privacy
University of Edinburgh – School of Informatics
Aggelos.Kiayias@ed.ac.uk




Edinburgh School of Law Research Paper Series
University of Edinburgh

## Abstract

The evolving merger of payments technology with technology underpinning investment markets' infrastructure can have a great impact on the mode of supply of financial services, notwithstanding technical, legal and regulatory restrictions. One-stop-shop multi-purpose and multi-asset platforms will be a key characteristic of post-COVID-19 finance bringing a radical transformation of the marketplace. Anticipated benefits range from a drastic reduction of intermediary rents and transaction costs to repatriation of investor control and alteration of today's narrow asset allocation strategies. To facilitate this transformation, we offer a model of decentralised finance that goes far beyond so-called "autonomous" finance. As the technical and regulatory challenges of increasing automation and integration in the supply of investment services will be considerable, a proactive approach is required to resolve these problems. Integrated decentralised platforms are the most promising route to: (a) counter the competitive threat of BigTech, (b) reform investment industry's narrow asset allocation practices whose fragility has been badly exposed by the pandemic, and, (c) spread equally the dividend of financial development.

## Keywords

Open Finance, Decentralised Finance, Investment Democratisation, Cryptographic Integration, Inclusive Finance, Financial Systems, SMEs, Access to Finance, Tokenisation, DLT-Blockchain, Financial Services, FinTech, RegTech, Sustainable Finance, Social Market Economy, Parametrisation, Financial Regulation, Investor Protection

# The Architecture of Decentralised Finance Platforms: A New Open Finance Paradigm

**Emilios Avgouleas*** **Aggelos Kiayias****

## Executive Summary

The evolving merger of payments technology with technology underpinning investment markets' infrastructure will have a great impact on the mode of supply of financial services, notwithstanding technical, legal and regulatory restrictions. One-stop-shop multi-purpose and multi-asset platforms based on Distributed Ledger Technology (DLT) are bound to become a key characteristic of post-COVID-19 finance bringing a radical transformation of the marketplace in three respects:

(a) markets will become less centralised,

(b) investment will be democratised since broader access and reduction of agency costs will bring a greater re-alignment between investors medium and long-term horizons with prevailing asset allocation strategies and the composition of their investment portfolios,

(c) finance will serve better socio-economic goals allowing the emergence of tradeable social market products. To facilitate this transformation in this paper we offer a model of decentralised finance that goes far beyond so-called "autonomous" finance.

Decentralised finance platforms can allow most business to business (B2B) and business to customers (B2C) fintech firms with the necessary regulatory licenses and credit and investment markets to flourish through the platform's market fora and distribution channels while sharing operating costs. The central idea is that smaller fintech firms would have a reliable framework to compete for business and cooperate in terms of platform governance and regulation. Network externalities might attract to the platform larger financial services providers but still these will supply their services on the basis of the same compete and co-operate model.

* Chair in International Banking Law and Finance, University of Edinburgh; Member Securities and Markets Committee, European Securities and Markets Authority (ESMA).

**Chair in Cyber Security and Privacy, University of Edinburgh; Director of the Blockchain Technology Laboratory. Chief Scientist at Input Output Global.

Decentralised finance can allow new types of asset markets, such as markets for social housing and other forms of social market investment to emerge and thrive. Characteristically our consumer credit use case shows how platform-based technology can both introduce competition in the market for low grade consumer creditors while maintaining their privacy. Thus, it can offer a compelling solution to a burning social problem --- that of over-indebtedness of low-income consumers and households. In addition, multi-asset platforms could boost liquidity in previously illiquid assets facilitating long-term/committed investment at the expense of today's investment short-termism. At the same time, smaller issuers will benefit from the platform's lower admission fees and advantageous disclosure regimes for SMEs facilitating small issuers' access to equity capital.

Yet the challenges brought about by increasing automation and integration in the supply of investment services are considerable, both at the regulatory and the technical level. A proactive approach is required to resolve the technical and regulatory tensions. Nonetheless, subject to some simplification certain parts of regulatory rulebooks can be coded automating compliance. We explain how platforms can automate compliance with such rules as counterparty position limits and order and price limits for short-sellers and prohibitions of front-running. Implementation of such automated controls would diminish the cost of regulatory monitoring and augment ex ante compliance. AI technology and supervised and unsupervised Machine learning, combined with cryptographic technology can make ex post compliance audits virtually infallible heightening deterrence.

We identify three fundamental properties that will define decentralised finance systems. First, we utilise *cryptographic integration* as the foundation for the supervening applications that will create a more open and competitive financial system. Secondly, we suggest that decentralised applications will give rise to *positive network externalities* removing the need for investment intermediation by big institutions, even at the investment origination level. Broadening access will lead to more pluralistic investment choices. In this context, we offer use case examples which underscore the potential of multi-purpose and multi-asset platforms to further socio-economic goals. Third, we use *parametrisation* to account for the pluralism of investor preferences that may go beyond risk and return to encompass social and ethical preferences.

The integration of infrastructure and client interface into an accessible single multi-asset platform is not just the realm of financial and information technology. It will also require advancements in regulatory technology as well as the adaptation of private law, especially

property law and the willingness of different jurisdictions to mutually recognise and grandfather these platforms. Standardisation of consumer contracts will be another prerequisite to enable these platforms to operate on a cross-border or even global basis.

Automation of regulatory compliance and detection of wrong-doing on multi-purpose and cross-asset platforms based on effective ex ante operating algorithms and thorough post audit systems would be essential in order to stem fraud, front-running and other forms of abusive and illegal conduct. Thus, research should not just be directed into building up the next generation of blockchain algorithms, but also of multi-sensor systems that go beyond current artificial intelligence (AI) and machine learning methods and allow for real-time compliance as well as smart detection of compliance breaches.

The model of decentralised finance platforms we propose takes the concept of open banking a decisive step forward to achieve the above objectives. We suggest that policy-makers' support for integrated decentralised platforms is the only realistic alternative to the present domination of the fintech space by gigantic financial institutions and the widely expected entry of BigTech which might choke competition. Similarly, we argue that integrated decentralised platforms are the most promising route to alter investment industry's narrow asset allocation practices whose fragility has been badly exposed by the COVID-19 pandemic.

# The Architecture of Decentralised Finance Platforms: A New Open Finance Paradigm

## I. INTRODUCTION

The immediate motivation for this paper comes from the realisation that the economic downfall associated with the COVID-19 pandemic is not just the result of the extensive lockdowns but also of the fact that global finance in the years after the 2008 Global Financial Crisis (GFC) retained most of the weaknesses of the earlier era in spite of widespread regulatory reform. In fact, the glut of liquidity created by quantitative easing (QE) programmes and negative rates, which were necessary at the early stages of the GFC, exaggerated such weaknesses and boosted the four most important ills of contemporary finance: excessive leverage and asset bubbles, monoculture investments, dominant (rent-seeking) market intermediaries and short-termism.[2] A number of respected global fora have dedicated time and energy to the discussion of how the global economy can be rest and re-oriented.[3] Yet so far none of these valuable initiatives try to tackle the serious underlying weaknesses of global finance.

The challenge is enormous. In its present state, global finance is broken and unable to be rebuilt by using the same tools that were used in post-2008 era in genuine good faith. In addition, it hardly contributes to the funding of the real economy especially when it comes to long-term infrastructure, socially responsible investing, the social market economy, e.g., consumer credit, social housing, or the acceleration of divestment from fossil fuels to green energy. Therefore, the issues the COVID-19 crisis raises are truly existential and not just related to the script of financial sector greed, the remedies should be structural, systemic and far flung.

In the post-COVID-19 period both developed and developing countries will have to build inclusive economies while broadening the digital skills set of consumers and digital inclusion.

[2] As all this activity took place against a background of disappearing disposable incomes it is not surprising that it also boosted inequality, especially between the asset rich and the asset light who have to borrow ever higher amounts of money to acquire those assets.

[3] E.g., OECD, "Beyond Growth: Towards A New Economic Approach", Report of the Secretary General's Advisory Group on a New Growth Narrative, 12 September 2019, https://www.oecd.org/naec/averting-systemic-collapse/SG-NAEC(2019)3_Beyond%20Growth.pdf World Economic Forum "The Great Reset" reformulating a new set of principles for inclusive and fair economic development https://www.weforum.org/great-reset/about

For financial markets we take this challenge to mean incorporation of ethical, long-term, and sustainable finance goals into mainstream finance processes as well as the decentralisation/democratisation of these processes. But agency costs are at the heart of the investment chain today and thus stand as a formidable obstacle to such transformation. Namely, while investors' investment horizon is normally medium to long-term, intermediaries have a very strong preference and preponderance to take a short-term view in order to both maximise commission income and boost short-term performance against their peers which is the prevailing performance and compensation benchmark in the investment industry.

Accordingly, we see repatriation of investor control and market democratisation as way to alleviate the disparity of interests between investors and intermediaries. At the same time, decentralisation is the only way to avoid the total domination of financial technology by today's very large financial institutions that offer cutting edge infrastructure and the pending entry of gigantic technology firms (BigTech) into the space.

For investments other than cryptocurrencies and infrastructure other than decentralised payment systems, decentralised finance has been a black-box so far notwithstanding a wealth of good intentions and quasi-scientific statements. More specifically there has been a marked dearth of technological, investment, and regulatory models that could underpin a shift to decentralised finance. Therefore, this paper attempts to supply a holistic model of decentralised finance on which integrated financial platforms based on the cooperate and compete model can be built and operate.

Arguably, given the rapid entry of large financial institutions and BigTech into the space,[4] most of today's financial technology firms (FinTechs) may only survive the fee reductions and the huge size of distribution networks their bigger rivals bring with them only through co-existence on decentralised platforms utilising the cooperate and compete models. The platforms would offer them the distribution networks, liquidity, and drive to innovate that will be necessary for them to stay in the market. As such we see decentralised platforms as capable to deliver three far flung structural changes: democratisation, broadening of the tradeable assets' base, and diversification of investment.

The first structural change is democratisation of investment. This doesn't just mean democratisation of market access, so-called democratisation of finance, but also repatriation of

[4] An instructive recent example is the HSBC-IBM partnership to create a proprietary AI-built set of equity indices. See "HSBC launches AI-powered equity index family", 1 June 2020, https://www.finextra.com/newsarticle/35921/hsbc-launches-ai-powered-equity-index-family

control and decision-making ameliorating some of today's agency problems. Financial market democratisation, which is also the essence of decentralisation, will allow repositioning some financial investment to social market activities according to the wishes and time-horizons of end-investors. Namely, in certain areas, decentralised platforms can change the rules of the game as regards investment strategies focusing on long-term returns, e.g., portfolio diversification, rather than short-term objectives that are often premised on rapid trading and high leverage. A reduction in the level of short-term transacting would also mean an erosion of intermediary rents. Without intermediary preferences dominating investor choices the primary market landscape may also altered bringing a second structural change: enhancement of the number and type of commonly tradeable assets including social market instruments.

Investment diversification can also bring about the third structural change: enhanced competition. Decentralised multi-functional and multi-asset platforms of the type discussed in this paper enhance competition by first allowing small fintech to offer their - often boutique - products and services to a much wider pool of investors. This space is today entirely dominated by gigantic intermediaries such as Blackrock for global wholesale markets (asset managers, private equity firms, venture capital etc.) or , for example, Ant Financial for the enormous Chinese retail markets.[5] Moreover, the widely anticipated entry of BigTech in the financial space, especially in retail markets, where firms like Facebook have distinct advantages of access to user data, would further supress competition, driving several of today's rising fintech firms out of business or to very low margin activities. Therefore, the emergence of decentralised multifunctional platforms on which today's smaller fintech firms can cooperate and compete may be the only way for them to both loosen the stranglehold of today's financial behemoths and withstand the expected onslaught of BigTech's entry into financial services.

The evolution of market infrastructure towards a structural model of *open finance* that can handle cross-asset markets and portfolios can be a true game-changer both in terms of revamped asset allocation, increasing the "stickiness" of investment and its social utility, and in terms of (retail) investor participation. Investment diversification can build economic and

[5] Xavier Vives, Digital Disruption in Banking and its Impact on Competition (OECD (2020), 14 (Box 3), http://www.oecd.org/daf/competition/digital-disruption-in-financial-markets.htm

Nancy Qu, "Vanguard and Ant Financial to launch advisory service", 27 March 2020, https://fundselectorasia.com/vanguard-and-ant-financial-to-launch-advisory-service/

financial system resilience[6]. An example is construction of tradeable market portfolios that contain stakes in uncorrelated investments, such as, for example green energy bonds or bonds in securitised green loan portfolios, stocks in electric car manufacturers, social housing debt, and other forms of financing of long-term projects. By virtue of tokenisation, these assets could become tradeable on multi-party decentralised platforms operating on the basis of distributed ledger technology (DLT), which can offer transparent pricing and enough liquidity due to positive network externalities to, for example, revolutionize infrastructure finance. On the other hand, liquid secondary markets alleviate the costs of exit making investment in such projects as social housing and project bonds more palatable.

As already said, democratisation of access and repatriation of investor control through migration of trading over DLT platforms will tilt the balance in favour of investors longer-term horizons. This is predicted to have a transformative impact on the allocation of financial resources. In addition, democratisation of access and direct investor control could allow altruistic forces and psychological biases favouring fairness, as discussed by leading game theorist Matthew Rabin and others,[7] to take hold. The combined impact of longer investment horizons and the expression investor preferences that go beyond risk and return could lead to the creation of liquid markets for such social investments as, for instance, social housing bonds. Since altruistic games are mostly motivated by self- and other-regarding preferences,[8] the post-Covid19 period will be in socio-ideological terms the perfect time for the introduction of such social market products into mainstream markets.[9] Increased investment pluralism can also curb today's monoculture approaches and rein in market homogenisation and tightly bound together risk and return correlations.

---

[6] Luiz Awazu Pereira da Silva - Deputy General Manager of the Bank for International Settlements – has recently stated that this crisis requires us "to rethink the trade-offs between the efficiency and resilience of our socio-economic systems". See Pereira da Silva, "Green Swan 2 - Climate change and Covid-19: reflections on efficiency versus resilience", Speech OECD Chief Economist Talk Series, Paris, 23 April 2020 and a Research Webinar at the BIS, 13 May 2020.

[7] See Matthew Rabin, Incorporating Fairness into Game Theory and Economics (1993) 83/5 American Economic Review pp. 1281-1302; Ernst Fehr, Klaus M. Schmid, "Theories of Fairness and Reciprocity - Evidence and Economic Applications;

[8] Moritz Hetzer, Didier Sornette, "An Evolutionary Model of Cooperation, Fairness and Altruistic Punishment in Public Good Games" PLoS ONE 8(11): e77041, https://doi.org/10.1371/journal.pone.0077041

[9] Some of these ideas are further discussed in Emilios Avgouleas, *Financial Markets, Technology, and the New Liberal Contract* (forthcoming)

Given the speed with which markets operate today the only way to allow *open finance* to thrive on decentralised platforms is quasi-automated, systems that provide real-time control and scrutiny and operate as customer-centric mechanisms. But to avoid an increase in costs which may impede or delay the decentralised platform revolution, policy-makers need to accept that integration of functionalities within single platforms e.g., advice, decision-making, execution, conciliation and settlement are inevitable.[10]

The integration of infrastructure and client interface into an accessible single multi-asset platform is not just the realm of financial technology and information technology (IT). It will also require advancements in regulatory technology as well as the adaptation of private law, especially property law and the willingness of different jurisdictions to mutually recognise and grandfather these platforms. Standardisation of consumer contracts will be another prerequisite to enable these platforms to operate on a cross-border basis.

Automation of regulatory compliance and detection of wrong-doing and on multi-purpose and cross-asset platforms based on effective ex ante operating algorithms and thorough post audit systems would be essential in order to stem fraud, front-running and other forms of abusive and illegal conduct. Thus, research should not just be directed into building up the next generation of blockchain algorithms, but also of multi-sensor systems that go beyond current artificial intelligence (AI) and machine learning methods and allow for real-time compliance as well as smart detection of compliance breaches.

Furthermore, following today's revolution in mobile payments, decentralised multifunction/multi-asset platforms can bring a revolution in lending and investment markets in emerging economies. This can be achieved through the elimination of frictions in transferring collateral and investments and drastic reduction of information asymmetries especially once combined with an integrated and effective regulatory system operated via automated platform restrictions and reporting (section IV), where, perhaps, today there is none. We provide in section II a few examples of use cases that can play a pivotal role in bringing about these transformative changes.

A fintech blogger has accurately noted that the ongoing wholesale transformation of finance[11] involves financial transactions moving away from legacy infrastructure "to innovative buy-

[10] E.g. a 2019 OECD paper has noted: "The industry will see a radical transformation and restructuring and will move towards a customer-centric platform-based model." See, "Digital disruption in financial markets – Note by Professor Xavier Vives", 7 June 2019, available at https://one.oecd.org/document/DAF/COMP(2019)1/en/pdf

[11] Gaurav Sharma, "Autonomous-Finance" offers a Re-Imagined Idea of Banking" 3 Nov. 2019, available at https://medium.com

and-build models" where supply chain financing happens through blockchain. Already mortgage onboarding happens through AI, and the risk analysis of portfolios and asset reallocations take place in milliseconds and through Robo-advisors. In his view this makes it possible to "**reimagine product, service and consumer experience stack** in a 360-degree fashion to ensure that money works for people autonomously in a **'self-drive' mode".**[12]

Still the new paradigm we suggest here is a type of decentralised finance and not simply an upgrade of so-called "autonomous" finance. We identify three fundamental properties which will define decentralised finance systems from their innermost layer and the system's foundation to the outmost one which is user-facing.

At the innermost layer, we demonstrate how we can create an open and competitive financial system through utilisation of cryptographic integration. In particular, we outline the design of a platform exhibiting financial integration that takes the concept of *open finance* a decisive step forward.[13] At present, open banking is understood as opening up banking functionalities to third party applications. Application programming interface (API) integration enables the development of applications that offer functionalities across different organisations as long as they individually expose their APIs to third party systems. We introduce a novel concept of cryptographically integrated APIs; such systems offer functions that are cross-organisation by design and are mediated by a distributed ledger which assists as an auditing tool of such operations for compliance. The execution of these functions results in invocation of cryptographic protocols that process data between multiple organisations while ensuring results integrity and data confidentiality.

In the middle layer, customer-driven decentralised applications will not be just a great breakthrough when it comes to operating efficiencies and lending costs but also in resolving important social problems. Properly designed decentralised applications can provide important breakthroughs to a number of socioeconomic problems that have seemed intractable for so long ranging from exclusion to social justice and gender equality. E.g., transferable records of property registers enshrined and stored in blockchain systems could become tradeable on

---

[12] Ibid.

[13] Here we also note the use of a similar term by a High-Level taskforce for the revival of the EU Capital Markets Union project, who see *open finance* as a critical step in building a retail investment market in Europe. See "A New Vision for Europe's Capital Markets", Final Report of the High-Level Forum on the Capital Markets Union", 10 June 2020 https://ec.europa.eu/info/sites/info/files/business_economy_euro/growth_and_investment/documents/200610-cmu-high-level-forum-final-report_en.pdf

relevant multi-asset platforms in a way that can revolutionise the management of households' and SME's collateral giving them access to competitively priced markets. In this paper we offer a number of examples of the socio-economic benefits of integrated platforms including the ways that by means of simple and accessible cryptographic technology women's access to the management of joint property assets can be ring-fenced. Even more critically we offer a consumer credit use case to accentuate the potential of multi-purpose and multi-asset platforms operating on the basis of cryptographic integration to further socio-economic purposes.

Third, at the outermost layer, decentralised finance will radically change the way it interacts with its human operators. While technology that would allow algorithms to recognise in real time the hierarchy of purposes (risk/return maximisation, ethical and social objectives) and continuously align it with the true intentions of human participants seems out of reach (and it might take decades for neuroscience and algorithmic technology to reach that stage), we explain in Section II how that can be approximately achieved through parametrisation. In our model, the interaction between human and the system will take place ex ante rather than real-time through parametrisation of risk-return, ethical, and social preferences of the investor, offering a diversification reflecting the will of the systems' participants, while continuous adjustment of the relevant parameters would enable the system to keep evolving and converging to the operators' predilections. Parametricism is widely used in architecture to design non-linear (pronounced in their asymmetry and unevenness) buildings and surfaces and more or less replaces homogenization (serial repetition) and pure difference (agglomeration of unrelated elements) in favor of differentiation and correlation as key compositional values.

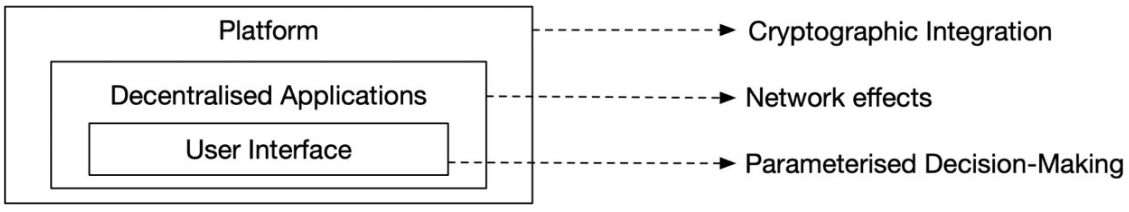


**Figure 1. The three properties of Decentralised Finance Platforms**

One of the key purposes of this paper is to underscore how related are all the required economic policy, technological, and regulatory actions and how interdependent when it comes to achieving the aforementioned objectives, Namely, a holistic approach is required that would replace the current piecemeal approach. It follows that several parts of finance and of its

regulation will have to be reimagined and re-drawn as a result in some cases breaking down or abandoning existing boundaries and classification.

The proper function of decentralised platforms requires stream-lining of rulebooks and cutting down of regulatory complexity, which automated monitoring/auditing and safeguarding systems may not be able to handle. Regulation will also influence decisively to what extent large incumbent players and BigTech will dominate the new type of multi-functional/multi-asset consumer-centric platforms.[14] Big players like BlackRock in wholesale markets and Ant Financial Services (a subsidiary of AliBaba) in retail have already created significant strangleholds that stifle competition.

The type of multi-party financial platforms envisaged here can redress these market failures reintroducing competition in the market. The challenge for regulators is to keep a level playing field striking the right balance between fostering innovation and protecting consumers and financial stability on the one hand and permitting multiparty integrated platforms to operate and experiment within and outside the sandbox. Even before the increased digitalisation of social and economic activity due to COVID-19 financial regulators stood at cross-roads since the emergence of investment platforms was already challenging previous regulatory models of institutional and/or functional regulation.

Post-COVID-19 regulators are required to make a quantum leap forward switching pre-existing frameworks retooling themselves with state-of-the-art technology and gearing rulebooks towards platform and service rather than individual institutional compliance. While this model could herald for many the "uberisation" of finance, nevertheless it has distinct advantages including in augmenting competition, investment pluralism, and resilience in the financial sector as well as protecting consumers by means of a number of ex ante switches and ex post audits. Future regulatory regimes will police platforms and platform functions and services against streamlined (and simplified) rulebooks and calibrate regulatory and legal remedies accordingly resolving also the problem of who is to be held accountable if the algorithm goes rogue one day augmenting multiparty checks and balances throughout the investment chain.

For automated collective compliance to be achieved, platform organisation and revenue distribution will have to operate a platform insurance fund. Under such organisation decentralised co-operative platform operators would not be to the size of their share in the fund

[14] This observation reflects, in part, Stigler's approach to regulation as something that is mainly demanded from policymakers by industry to safeguard their interests and protect their rents. See George Stigler, "The Theory of Economic Regulation"2(10 *The Bell Journal of Economics and Management Science*, (Spring, 1971), pp. 3-21.

jointly and severally liable for platform dysfunctions. At the same time, any compliance breaches would impact symmetrically on the platform insurance fund's premia heightening collective compliance incentives and minimizing the risk of defection or free riding by the members of the cooperative platform.

The remainder of the paper is in four sections. The second section gives examples of socially beneficial innovations that could be promoted through technology in the form of multi-function/multi-asset financial services platforms accessible to both retail and wholesale investors. It also discusses the benefits and risks of such innovations. The third section offers examples of technical solutions to the operational changes presented by such platforms. The fourth section focuses on legal and regulatory challenges and offers ideas about how these could be resolved. The fifth section concludes.

## II. FINANCIAL PLATFORM INTEGRATION: BENEFITS AND USE CASES

### 1. Overview

The first step to very cost-effective (including a reduction of rents) and user accessible supply of financial services is the creation of complete virtual value chains via decentralised DLT platforms. These will cover most forms of investment services from investment advice and asset management to trading and clearing of various assets including securities and derivatives whether on-exchange or OTC. Fintech efficiency benefits are well known and, as enumerated in an OECD note, include[15]:

(a) more effective screening of candidate borrowers via statistical models based on big data to overcome information asymmetries

(b) targeted pricing through the use of wider datasets and interest rate-setting models.

To these the authors of this paper add: operating efficiencies in the form of cost reductions as DLT systems can eliminate the need for use of a multiplication of communication, trading and conciliation systems driving down transaction costs.

Arguably, the biggest socio-economic benefits can only be delivered through a radical transformation of market structure and a shift to customer-driven multi-asset platforms which would combine full connectivity between asset markets with easy access. A good early example of the changes that DLT can bring to the financial market structure is the cradle to grave system that the Israeli securities regulator is attempting to build with the help of the

[15] Digital Disruption in Banking and its Impact on Competition (OECD (2020) (note 4), 12-13, http://www.oecd.org/daf/competition/digital-disruption-in-financial-markets.htm

industry. What is very important in this context is the fact that the regulator has signalled to the industry that it is ready to change its rulebooks to accommodate innovation and asked the industry to bring a credible proof of concept on which it would base the new operating and regulatory framework. In particular the Israeli regulator has highlighted the following benefits[16]:

(a) democratisation of access: low-cost DLT-based platform have the potential of opening up extra financial opportunities for new entrants in the market

(b) faster trade settlements and streamlined clearance.

(c) lower transaction costs across the market value chain and especially with respect to the generally expensive IPOs.

In addition, multifunctional investment platforms can prove instrumental in achieving the "holy grail" of securities markets: collectivisation of primary markets and of investment origination. While, as said in section IV, the fundamental premises of securities laws such as issuer due diligence and disclosure will have to be fully respected, burdening issuers, investment originators in general, and their professional advisors with the relevant costs, expensive intermediary-based information verification processes could be revolutionised. The same applies to solicitation and syndication of investors' interest in IPOs and other investment origination activity. Platforms can allow for these processes to be performed in transparent and collective way that drastically reduces the rents of the investment intermediaries that dominate the IPO markets today. Namely, investment banking functions such as information verification, marketing of new issues, and solicitation and intermediation of investors' interest could take place on and through the platforms using cryptographic protocols that would secure the privacy of the issuers and the integrity of the information.

But to achieve this objective multi-party platforms will have to integrate today's disparate functionalities at the origination and distribution levels. These will include, first, information processing to secure the integrity of the information disclosed by the issuer or originator. Secondly, once this process is performed, information would have to be disseminated to interested parties via the platform in a way that keeps its confidential nature and complies, for

[16] Danny Nelson, "Israel's Securities Regulator Asks Private Sector for DLT Proof-of-Concepts", Coin Desk, 27 January 2020, https://www.coindesk.com/israels-securities-regulator-asks-private-sector-for-dlt-proof-of-concepts

instance, with the EU Market Abuse regime on soundings,[17] to attract investor interest and boost the liquidity of the primary market and thus the success of the new issue. Therefore, integrated platforms will have to utilise an *open finance* model based on cryptographic integration. We outline how this model will function in the next section.

More open markets operating by means of integrated multi-asset platforms will also lead to provision of better tailored products and services with enhanced accessibility. Especially multi-party platforms operating successful governance frameworks can thrive on the collaborate and innovate model supplanting today's proprietary model which has created over-dependence on dominant intermediaries, which, however, offer essential liquidity through intermediation. It is assumed that well-functioning decentralised platforms will be able to replace such liquidity by sourcing it either via small fintech firms or directly from users due to enhanced transparency and wider availability of pricing tools. Arguably, any such reduction in the domination of the investment chain by big financial intermediaries would open up the markets to more pluralistic investment attitudes and policies.

## 2. Platform Architecture

Unlike several cryptocurrency DLT systems, the model of decentralised platforms we propose requires that these operate on the basis of access approval once a customer's identity and origin of funds have been established under Know Your Customer controls (KYC). The key difference to classic KYC, is that member firms would distribute costs and expedite customer permissioned access (also known as on-boarding) by sharing on the platform customer KYC details, while preserving customer privacy through cryptographic techniques and zero knowledge proofs.

The best way to understand the level of integration we set out to achieve in this work is to juxtapose it with the type of integration currently achieved via initiatives such as open banking via the EU Payment Systems Directive II (PSD2) and other similar initiatives outside the EU. In this setting, financial organisations open up their application programming interfaces

[17] Art. 11, Market Abuse Regulation (*Regulation EU 596/2014*) (MAR). Art. 11(1) describes: a "market sounding" as "a communication of information, prior to the announcement of a transaction, in order to gauge the interest of potential investors in a possible transaction and the conditions relating to it such as its potential size or pricing, to one or more potential investors". See also ESMA Guidelines on the Market Abuse Regulation - market soundings and delay of disclosure of inside information, 13 July 2019, ESMA/2016/1130

(API's) and facilitate the development of third-party applications that offer functions that can take advantage of multiple API calls to different interfaces. However, the integration is purely "logical", i.e., access control to the API is bound to the terms of each individual organisation. It is not feasible to directly ask organisations to work together or apply operations on data that are not strictly siloed within an organisation and are not public.

In contrast, the platform architecture we suggest enables applications to perform, in addition, operations across organisations. A platform-level API enables us to organise functions to run as cryptographic protocols which are shared by the various organisations that participate in the platform. The platform itself incorporates the functionality of a distributed ledger and a privacy-preserving bulletin board that mediates users, applications, and organisations and facilitates the execution of operations at the platform level. Third party developers can write more versatile code that will ask organisations to execute cryptographic operations on private databases they own individually without exposing confidential data.

The platform and its API functions are organised in a similar manner as a permissioned distributed ledger in the sense that a set of entities provide maintenance and operational support collectively without a single point of failure. Nevertheless, the similarity ends here; the core operations of the platform are not diffused across the set of participants but are cryptographic protocols that are executed "off-chain" between specific subsets of the parties as identified in each platform API call. As we illustrate in the next section, by following the above techniques we can facilitate complex operations such as cross-referencing information between different private databases and creating assets and financial instruments indexed with information that is maintained privately by multiple organisations.

In the case of securities markets, once the bulk of non-High Frequency (HFT) securities trading has moved on to blockchain platforms - due to their inherent operating speed limitations DLT cannot handle HFT - the costs of trade confirmation and transaction conciliation diminish. The same applies in the case of derivatives markets operated on DLT.[18] However, in the case of OTC derivatives markets a system developed by the authors of the present work (D-Chain, White Paper, November 2019) proves that decentralised DLT platforms can also offer a greater number of functionalities, including real-time assessment and regulation of risk and mechanisms to alleviate liquidity shortages.

[18] See E. Avgouleas, A. Kiayias, "The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the 'Holy Grail' of Systemic Risk Containment" (2019) 20 *European Business Organization Law Review* 81–110.

Furthermore, in our model platforms could allow users to opt for investment choices which can reflect ethical or environmental preferences. Technology is today unable to introduce a dynamic hierarchy of priorities based on human actors' ethical and social preferences and their investment objectives which would allow algorithms to pause and redirect investment decisions on the basis of such considerations. But such priorities can be put into parametric models and programmed in advance giving different weights to different preferences even at the expense of risk-return optimisation of distributions.

Parametricism is widely used in architecture to design non-linear (pronounced in their asymmetry and unevenness) buildings and surfaces. The aim is to build up more spatial complexity while maintaining legibility, i.e. to intensify relations between spaces (or elements of a composition) and to adapt to contexts. It mostly replaces homogenization (serial repetition) and pure difference (agglomeration of unrelated elements) in favor of differentiation and correlation as key compositional values and often at the expense of efficient exploitation of available space. It is, thus, the most apt parallelism for a new algorithmic formula that would incorporate beyond investment objectives and risk preferences in CAPM type of linearity, investors' social and ethical preferences. The process would be subject to ex post audits with incremental corrections until the desirable balance in the composition of investment portfolios is achieved.[19]

[19] For the first full analysis of how the concept parametricism could be incorporated in the investment management chain and a first illustration of the possible applications of the principle and climate change finance see Emilios Avgouleas, "Sustainable Finance and Spatial Modelling – The Challenge of Parametricism for Climate Finance Regulation" *Law and Contemporary Problems* special issue Climate finance 2020/21.

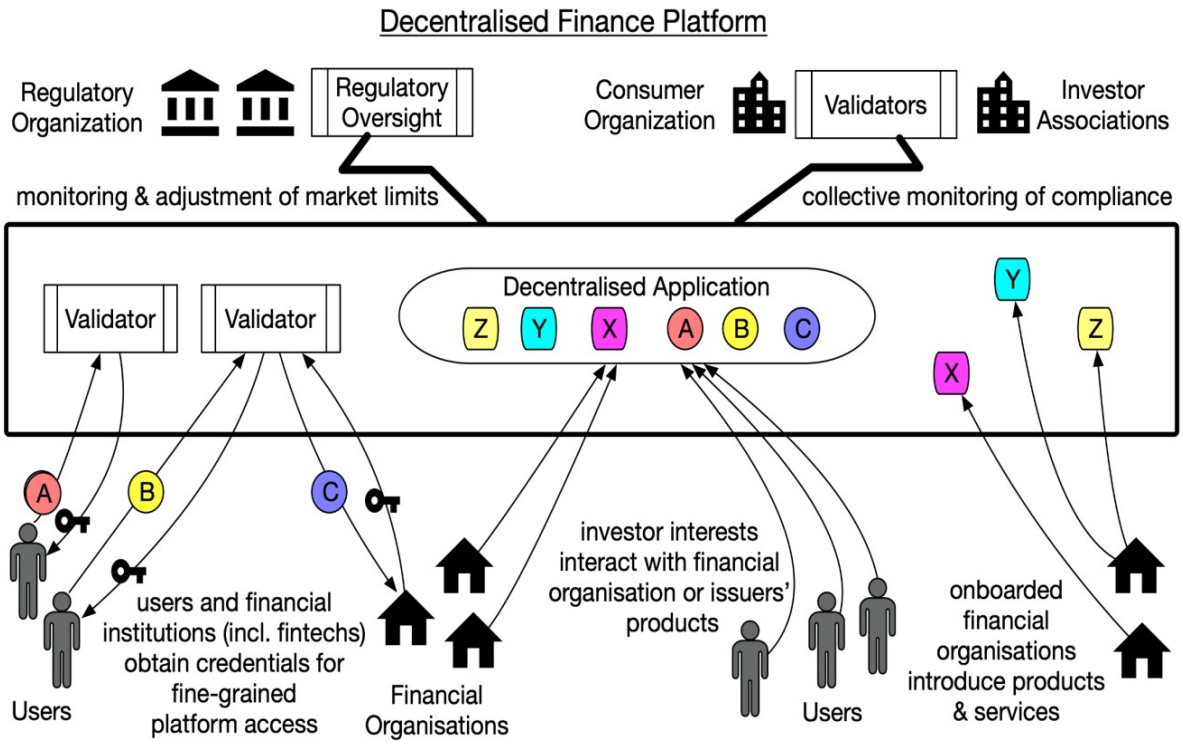


**Figure 2. Overview of Decentralised platforms architecture**

## 3. Platform Governance

Platform governance will have to rely on three pillars: *regulation*, *self-regulation and peer monitoring*, and *partnership organisation* vis-a-vis decision-making. This trinity of preconditions is indispensable otherwise decentralised platforms could become associated with fraud, client abuse, and sharp practice, which would stigmatise them and drive them out of business.

As regards the first pillar: *regulation*, this would be augmented, where possible, via automation of compliance (see Section IV). Naturally, regulation attached to platforms and not merely institutions and individuals, who will of course still remain subject to the traditional regulatory requirements, will raise serious challenges for regulators. How these will be addressed will be crucial both for the success of decentralised platforms and for their ability to bring about anticipated benefits. The ability of financial regulators to monitor financial activity on the platform as close to real-time as possible and their ability to alter restrictions, e.g., position limits, price limits, composition of margins etc. can augment rather than undermine the quality and effectiveness of regulation in spite of the decentralised nature of the platform.

The second pillar is self-regulation, namely internal platform governance and peer monitoring. The roles of nodes here will be critical as will be the transparency of operations on the platform and free flows of information. Governance will not be merely confined to transaction validation by nodes. On the contrary the platform will offer the opportunity for ad hoc committees to arise to decide on critical matters (see Section III). Moreover, individual compliance with the regulatory rulebooks and applicable laws would be augmented by collective monitoring. Such collective decision-making may never be successful, however, in the absence of strong incentives. Powerful incentives to comply may only be matched by strong sanctions for defection. These would be automatically provided via the third governance pillar which would be a cooperative type of organisation running the platform.

## 4. Examples of possible use cases

Integrated platforms can indeed provide decentralised access to the financial system in a way that assets, payments in fiat (including Central Bank Digital Currency (CBDC)) or other virtual means of payment including cryptocurrencies, and financial instruments move seamlessly (subject to regulatory and platform permissions) across the platform while preserving privacy by means of cryptographic protections. Thus, integrated platforms have the potential to revolutionise economic functions and the investment landscape in emerging economies. First, they can introduce an integrated and effective regulatory system, through automated restrictions and reporting (see section IV below), augmenting user protection and public interest in the form of enhanced oversight and enforcement. Secondly, they can eliminate frictions in investment and not just payments. We provide below a few such examples of use cases and explain the benefits they can bring.

*(a) Household and SMEs Lending and collateral management*

Tokenisation of a variety of assets and the ability to trade different assets stored in a single digital wallet on the same platform can result in a radical transformation in the way that property rights are traded and collateral is managed both the households and SMEs and not only within developed legal orders but also in those where property rights are less defined.

Thus, assuming formal recognition by national property registers of property rights based on equity, customary law, long-term possession, or even transformation of ubuntu[20] (in parts of

Africa), then such rights and fractional stakes on them could subsequently be tokenised and become tradeable.[21] This breakthrough could revolutionise lending in the developing world and bring a sharp reduction in interest rates. Modern pricing mechanisms for property assets and a relatively liquid market can save developing world households from the menace of loan sharks, establish a transparent market price for property rights in those countries where none existed before and dampen price volatility. For example, even where the informal market or the black-market offer price indications the emergence of efficient lending markets in emerging economies is today hampered by several market failures, such as lack of transparency, occasional lack of liquidity, and lack of legal certainty as regards debt enforcement and liquidation of collateral.

*(b) Emergence of secondary markets*

Based on the same principles underlying blockchain systems SME loans (and attached collateral) could equally be tokenised and be made tradeable/transferable creating a secondary market for, in principle, illiquid bank assets. Trading such assets on DLT platform that also offers full ownership and pricing could create a competitive auction processes in the post-underwriting stage for such credits. As a result of having such a process and existence of tradeable collateral, extortionate mark-ups, usury, extortion, and corruption can all gradually disappear from the market for small household and SME loans.

In the process the International Finance Corporation (IFC) and other public or private sector organisations can provide tradeable guarantees to such a market and also boost green economy projects as they could offer better terms for SME loans for green economy actions - subject to a monitoring framework – leveraging its resources and creating more complete/effective outcomes. The same, of course, applies to donor guarantees.

*(c) Inalienable use of savings*

[20] Nonetheless, post-Apartheid South African courts have used equity/ubuntu as a negative right so far, e.g., the right to desist eviction. See Drucilla Cornell and Muvangua Nyoko (eds), *Ubuntu and the Law: African Ideals and Postapartheid Jurisprudence* (Fordham University Press, 2012), esp. pp. 126-128.

[21] Where the legal possibility exists tokenised securities backed by such real estate rights/assets or fractional stakes in them can become fully negotiable on DLT based securities markets. See Liquefy, Sidley Austin, KPMG, Colliers, "Real EstateTokenization: Hong Kong Singapore", 1April 2020, https://mainpage.liquefy.com/storage/app/media/Real%20Estate%20Tokenization_V005.1.pdf

Using technology to enable speedy transfer of remittances at nearly zero costs (including as a major innovation dynamic FX conversion) in an environment that is safe from external threats can have an appreciable impact on financial inclusion, especially where remittances are an important part of a family's annual income. Through the use of digital identity, it can secure access to the unbanked,[22] giving them the opportunity to keep the bulk of the remittances in safe storage.

Safe storage of savings in fiat (if they are not in the form of CBDC) or even in other forms of payment emanating from the remittances, once a part of them has gone into consumption, is very important. It gives poor households and the previously unbanked the possibility to receive stable/predictable returns on savings, which would allow for better planning of the households' consumption and investment needs. Then, the transfer of some of the balances into a savings account would allow the very poor and the unbanked to use some of the funds to buy insurance to cover the impact on earnings of health and other contingencies (e.g., a bad harvest).[23]

Carefully preserved savings balances may eventually be used for the purpose of human capital development including private investment on education to augment education vouchers from aid organisations and public literacy programmes. Given that women are often the victims of reduced education opportunities the surplus of carefully managed remittance savings can even redress the gender gap in education.

Equally, integrated platforms can help these low-income savers to safely use cash balances as collateral to acquire on credit capital assets such as machinery which will boost the productivity and income of a small business or of a farm. Even more importantly integrated platforms can use fail-proof stable-coins to tokenise government tax credits or donor aid subject to government or donor agreement. This would make state credits or donor aid liquid and capable to be used as collateral for a loan, expanding the use of such state or donor assistance in credit and commerce maximising their economic and social impact.

(d) *Innovative asset backed and other retail instruments*

[22] This is one of the main requirements of financial system access. See D. Arner, R. Buckley, D. Zetzsche, R. Veidt, "Sustainability, FinTech and Financial Inclusion" (2020) 21 *European Business and Organization Law Review* 7-35.

[23] Moreover, turning part of the remittances into savings in a seamless process constrains consumption for instant gratification and can boost the long-term investment plans of low- income households. See Emilios Avgouleas, "International financial regulation, access to finance, systemic stability, and development", Brooks World Poverty Institute WP 49, June 2008.
http://hummedia.manchester.ac.uk/institutes/gdi/publications/workingpapers/bwpi/bwpi-wp-4908.pdf

An integrated platform for the transfer of property stakes and lending can also allow a market for property futures of the type of Case-Shiller contracts[24] to emerge, creating truly liquid markets for the hedging the risk of households' most precious asset: their house. Moreover, specially designed DLT platforms can allow mini-CDS to be traded allowing for instant hedging of credit risk especially where the platform offers P2P (B2B) lending.

Using same principles as mini forwards or futures contracts, farmers and their advisors can tokenise their animal stock or anticipated harvest and sell the coins that allow for both physical delivery (e.g. grain) and cash settlement in exchange of tokenised fiat, CBDC, or other means of payment.[25] Once tokenised, all these instruments can be made tradeable and transferable on DLT platforms allowing households to buy fertiliser or seeds for the harvest or animal stock without risking their home or having to borrow at punitive rates. E.g., some of these tokens could be bought by the government or donor organisations (acting essentially as a no interest loan in the form of pre-payment) and can either be redeemed later at commercial value, or ask for physical delivery if there is a supply shortage, or be rolled over to another year if there is a bad harvest, or even be forgiven.[26]

*(e) Other Advantages*

The examples of possible use cases offered above also present a number of other important advantages. In summary they can allow for:

i. the widespread indexing and comparability of property prices and prices of proprietary rights across entire regions diminishing exploitation of especially poor households and of women;

ii. the eventual development of mini-property derivatives for hedging could bring in more sophisticated players who wish to diversify their asset portfolio (as Africa presents lots of uncorrelated risks compared to developed world assets) without having any exposure in the cash/spot markets;

---

[24] According to Chicago Mercantile Exchange (CME) "S&P/Case-Shiller Home Price (CSI) Indices futures and options are the first comprehensive financial tools that make it possible to manage U.S. housing risk". See CME Group, "Alternative investments S&P/Case-Shiller Home Price indices Futures and Options https://www.cmegroup.com/trading/real-estate/files/housing-fact-card.pdf

[25] A lot of private operators already look at this and a good example is Beefchain a food provenance and safety firms that has partnered with Wyoming cattle ranches to augment safety and quality in the supply of beef and the reward of ranchers that use grass-fed techniques to produce to raise cattle. See https://beefchain.com/about/

[26] See for complete analysis Emilios Avgouleas, *Financial Markets, Technology, and the New Liberal Contract* (forthcoming)
Of course, such schemes will have to be tightly supervised and regulated offline so that no farmer overextends and also no family goes hungry.

iii. the safeguarding women's access and management of their own property stakes and other family assets and joint control through own cryptographic key without having to possess more than a smartphone and an electronic wallet;
iv. a system of credit scoring can be operated extracting information from the platforms (based on individual full authorisation) in the mode described in paragraph II.5 below facilitating access and lowering the cost of credit. SMEs may even be paid for the right of credit scoring agencies to use their data and meta-data;
v. the secure comparability of lending rates for borrowers with similar credit profile and quality of collateral thus helping to root out in the process racial, religious, or gender discrimination. Using explainability techniques it will be easy to identify if banks or other loan providers discriminate in favour of one group or another on the basis of pre-programmed exclusion criteria or directed learning paths for the algorithm.

## 5. Consumer Credit Platforms – A Compelling Use Case

A very good example of the use of integrated platform technology to help alleviate nearly intractable social and economic problems constitutes the suggested here development of specialised consumer credit platforms.[27] The design and implementation of such consumer credit platforms are analytically discussed in depth in section III.4 below where aspects of the scheme are laid out in some detail, thus, we provide below a brief summary.
In our scheme pay-day borrowers allow their spending, savings, consumption data to be collected and taxonomised by debt charities. Trusted debt charities keep the data safe and taxonomise each borrower on the basis of pre-set criteria that grade borrower creditworthiness against income, savings, education level, state of health and spending and other behavioural habits. These are mapped against a properly adapted matrix of default probabilities starting from 100% and ending with zero. Then each interested borrower is assigned a different colour on the basis of this grading and are furnished tokens with a corresponding colour which can be auctioned on an anonymised basis to interested lenders. Credit providers then may compete on a reverse auction platform operated by a consortium of charities vis-à-vis offer interest rates for pay-day loans in different lots depending on the size of the loan. While the matching is done on the platform on an anonymised basis where zero knowledge proofs are used until the signing of the contract and only after the interest rate for the loan and required sum have been

[27] For a full description of the conception of this scheme see Emilios Avgouleas, *Financial Markets, Technology, and the New Liberal Contract* (forthcoming).

agreed. Still the charities operating the DLT lending platform can act as nodes validating the transaction (contract) between the interested borrower and interested creditor, once their identities have been automatically revealed, to add an extra layer of confidence/security in the system.

Naturally a consumer credit system operating on the above basis will send interest rates crashing down, given the existence of a reliable grading system, ameliorating the cost of borrowing for this vulnerable part of the population. But the biggest advantage of this system is anonymity until the contract is signed, avoiding penalties due to personalised credit searches. It will also bring competition and liquidity to this type of lending making sure that, on the one hand, lending costs do not reflect unnecessary margins due to information asymmetries and on the other that such vulnerable borrowers do not borrow more than they can afford, plunging them into a lifetime of debt.[28]

The same principles of course apply to credit card lending for the less well-off parts of society as well as to those in the developing world with no prior access to the financial system. Therefore, if the experiment works it can also be used for all forms of consumer finance from credit cards to insurance and microfinance. Borrowers and lenders pay a small fee to the platform allowing charities to recoup their costs. And such use of technology can revolutionise not just the cost of borrowing for these social groups but also the cost of funding as credits can become more credibly rateable and repackageable in securitisation schemes.

## III. TECHNOLOGICAL INFRASTRUCTURE AND API INTEGRATION

### 1. Basic Platform Architecture and Properties

At a high level, an integrated platform consists of two components: the front-end, which handles all the participants' interactions with the platform's environment and the back-end which communicates, maintains and advances the system's state.

The back-end of the platform can be thought of as a state machine.[29] At a high level, a state machine is defined by a set of states Q, a set of transactions T, a set of outputs O and a transition function δ that maps the product set QxT to the product set QxO, i.e., shows how the state machine at state q, given transaction tx, updates its internal state as well as produces the

[28] For analytical discussion of the economic and social consequences of this conception see also Emilios Avgouleas, *Financial Markets, Technology, and the New Liberal Contract*

[29] A state machine is a simple way to abstract computation. We refer the interested reader to John E. Savage, *Models of Computation: Exploring the Power of Computing* (1998). Addison-Wesley, for a broad overview of methods and models that abstract computation.

corresponding output. Not all transactions are admissible for a given state of the state machine. In particular, when a transaction tx is inadmissible with respect to the state q, the transition function assigns as the output the special "empty" symbol ε and leaves the internal state q unchanged.

In the context of state machines, a regulatory rule R is characterised by a subset of the product set QxT, i.e., it is a set containing state-transaction pairs that are "legal" or admissible with respect to R. Set R then determines whether a transaction is admissible or not. However, to enforce that within a state machine we need to determine how regulation can be encoded within the state of the machine. Let E be any relation over states and regulations. We say that a state machine has *regulatory expressibility* according to E, provided that the following holds: If (q,R) belongs to E, then for any (tx,q) that is not in R, it holds that $\delta(tx,q) = \varepsilon$, i.e., transaction tx is inadmissible at state q. In other words, regulatory expressibility suggests that the state machine is capable of encoding all rules R for which there is a state q such that (q,R) is in E; importantly, when the state machine is at state q, all transactions that would breach/contravene R, will be inadmissible.

To add clarity on how a legal and/or regulatory rule (both as regards prescription of permitted and prohibited behaviour) can be expressed in a mathematical way as the set of state transaction pairs that are admissible let us use as an example position limits to contain counterparty riskiness or price and order limits if there is an uptick rule for short selling or a circuit breaker. In specific, where position limits are set at X for a certain party who has exposure Y in terms of open position, then at any state q of the ledger that party will only be allowed to transact subject to limit X. All transactions that exceed the limit would be automatically rejected in the same way that a car with automatic speed controls cannot run beyond the permitted speed limit. The same applies to orders to trade that do not move to a higher tick or would push the price below the daily limit of the circuit breaker.

We note that regulatory expressibility is a minimal requirement for a state machine to be useful in our context, as it does not necessarily prescribe how the state machine can reach a state where a certain regulation is encoded, i.e., what is the exact sequence of transactions that inscribes the regulation into the state, and whether such encoding is "robust", i.e., it does not get inadvertently destroyed when the state is updated. However, it is sufficient for the current level of exposition to underscore the ability of our state machines to encode regulation and enforce it. Sound platform governance and formal verification can facilitate the encoding of regulation and its robustness.

Implementing a state machine for an integrated platform is centred around four major pillars: *decentralisation*, *integrity, confidentiality* and *integration*. Decentralisation describes the operating environment and fault resiliency of the implementation; it highlights the aspects such as the responsiveness of the system and its ability to operate even when participants diverge in their incentives or fail to act as required due to hardware faults. Integrity captures the assurance the participants should have that the state of the machine cannot be tampered with. This property is paramount since among others, it ensures that the integrity of regulations encoded in the state cannot be tampered with. Confidentiality suggests that the state of the machine is not public knowledge and different participants have different and well-defined views of the state of play. Finally, integration points to the fact that it is possible to develop applications that operate on top of the platform integrating the functionalities of all the participants into one unified system. We expand on these aspects below.

The first pillar is decentralisation. The key concept behind a decentralised system is the distribution of the system's functionality across a number of distinct participants so that no entity individually becomes a single point of failure. At the onset, the integrated service is supposed to be bootstrapped by an initial set of participants which they have authenticated each other out of band, and subsequently the set of participants evolves over time as new participants are onboarded following a system-specified identification and validation process. To fully appreciate the concept, it is worth comparing the benefits of a decentralised approach vs. a centralised one. While in principle centralised approaches can provide a higher level of responsiveness, they leave as open question the incentive structure of system custody and maintenance. Moreover, they are inherently asymmetric as participants with closer ties to the entity running the service can potentially exploit such proximity to gain an advantage with respect to the other participants. Instead, a decentralised organisation removes such asymmetries creating a neutral foundation over which participants can engage in a symmetric fashion. Moreover, decentralised platforms can also facilitate some centralisation at a higher protocol layer so that the highest possible responsiveness can still be attained if necessary.

The second pillar is integrity as a property of the underlying system. System integrity refers to the system's ability **to provide at all times a consistent view of the state to all participants**. Thus, two geographically distant participants accessing the system at the same time should have the same understanding about the current state of the system. This also implies that the system will be expected to operate in the same way in the view of these participants and react to their input according to their level of access. Moreover, consistency should also extend in

the time domain, and when a participant observes the system evolution over time the system's state should transition to new states in a plausible manner, i.e., there will always exist a plausible sequence of events that justify the current state of the system based on one previously observed in the past.

The third pillar is confidentiality. Each participant has access to the system's state only according to a specified level of access she is entitled to. Moreover, access control is enforced cryptographically, i.e., there is no local component in the domain of a participant that, if circumvented, will enable the participant to elevate her access privilege to the platform. Switching the level of access of a particular part of the system's state can be done by issuing the appropriate cryptographic keys to the intended recipients. Each party can create new platform elements (such as addresses and other relevant metadata) and post them on the ledger subject to the access control mechanism. Only permissioned addresses can receive payments with respect to any asset. The platform identifies, implicitly or explicitly, at any time a Committee that collectively maintains it and updates the access control information as required.

The fourth pillar is integration. The participants in the system are financial organisations (banks, brokers, investment companies) that may serve a number of customers. Onboarding an organization makes available various metadata about the financial. Importantly it includes a reference to the application programming interface (API) that the organization is using as well as the master public-key of the organisation. Integration suggests that it is possible to combine API operations and data processing across all the organisations that participate in a way that respects the first three pillars.

Implementing a globally scalable platform that provides the level of integration we described above may seem an infeasible task. In the remaining of this section, drawing from recent results in modern cryptography and the theory of distributed systems, we will describe how it is possible to tackle the problem. We start with the integration problem in Application Programming Interfaces.

## 2. **Application Programming Interfaces and Logical Integration**

In this section we describe APIs, their relevance to the setting of financial technology as well as the current state of the art in API integration which we describe as logical integration. Subsequently we introduce the novel concept of cryptographic API integration that relies on an integrated platform that engages multiple service providers and organisations.

An application programming interface (API) for a service is a specification of a set of functions and procedures that enable the interaction of the API user with the algorithms and the data that

the service offers. Given an API, it is possible to write executable code that will take advantage of the API and update the state of the service. In the banking setting, an API may enable a user to perform various operations such as open an account, transfer funds between accounts, place buy and sell orders, create new financial instruments and so on.

Given an API, it is possible to develop a front-end application that enables a user to engage with a service. Such front-end applications can operate within a web-browser or in stand-alone smart phone applications. Access to the API, or to certain functions of the API, especially in the banking setting, is subject to access control. This means that executable code that takes advantage of the API should authenticate itself to the service.

A simple example of typical functions offered by a banking API are as follows. The function below creates a counterparty for a given account. It will require the caller to have the ability to introduce new counterparties for the given account and it will also require the routing information (e.g. in the SEPA setting it would be the IBAN of the counterparty account). The function returns an identifier for the counterparty.

Create Counterparty(Account A, Routing Information R) => Counterparty Identity CID

The above can be followed by another API function which requests a transfer of value B to be made to a certain counterparty from the given account and returns success or failure, depending on whether the account has sufficient funds for the transfer.

Transfer Request(Account A, Counterparty Identity CID, Value B) => Success / Failure

A single front-end application may have access to multiple different service APIs at once provided suitable authentication is performed. In the banking setting, this enables a first level of integration which enables users to execute code that is "cross API."

We refer to the ability to use multiple APIs and write combined executable code that is cross API as *logical* integration. This type of integration is promoted by initiatives such as the PSD2 and the standardisation of banking APIs.

## 3. **Cryptographic Integration of APIs**

We introduce next the novel concept of cryptographic integration for APIs. In order to understand the distinction between logical integration and cryptographic integration, it is instructive to consider how access control affects API access. In particular any API call is labelled by the attributes that characterise the access capability of the caller. Thus, the caller should be authenticated and then ensured that it is authorised to have access to the specific function of the API. Subsequently the API function will be executed or report failure due to lack of proper authorisation. The front-end interface will be responsible for informing the user

of such events and ask authentication and authorisation depending on the specific functions to be used for a certain operation.

This logical separation can be quite limiting. Consider for instance an API that offers access to a customer database via a SELECT function that can match users based on various attributes, e.g., name, address etc. Suppose now there is an application that integrates two APIs and attempts to produce the set of customers that the two organisations share in a certain city. Such operation can be prohibitive via standard logical access control: the reason is that the application user may not have full SELECT privileges in both interfaces. Thus, it is not possible to write code that performs the two successive SELECT operations and subsequently calculate the intersection between the two lists. For these more complex operations, cryptographic API integration that we introduce next, is the suitable method.

Operating with APIs using cryptographic integration operates in two stages. In the first stage executable code interacts with an API at a certain level of authentication that normally her requests would have been denied. Contrary to regular requests, the outcome of such API processing would not affect the internal state of the service immediately; instead any resulting sequence of actions and state updates that stem from the API call would be cached and assigned a unique "input identifier" which would be returned to the caller function. At this moment, the API call completes and control is returned to the user.

The second stage of integration requires the utilisation of the "platform API." This API is designed with the aim of running operations across institutions. It operates on private inputs that have been previously constructed in the first stage and referred to by the input identifiers. Platform API operations are not executed directly by any individual organisation. Instead they are recorded to the platform's state machine and acted upon by the organisations via executing a corresponding cryptographic protocol that matches the platform API function. For instance, in the above example the application can run the SELECT operations to generate the two client lists in the respective organisations, receive the input identifiers and then request the execution of the intersection operation that will be performed by running a private set intersection (PSI)[30] cryptographic protocol between the organisations. Requests for running the operation will be subject to policy which will be automatically enforced by the platform. Moreover, the platform

[30] Examples of a such protocol are offered in M. J. Freedman, K. Nissim, and B. Pinkas. Efficient private matching and set intersection. In Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings. Lecture Notes in Computer Science 3027, pages 1–19.

will maintain an audit trail for all cross-API requests and will enable select participants to inspect it.

An overview of a cryptographic API integration is presented in Figure 3 below.

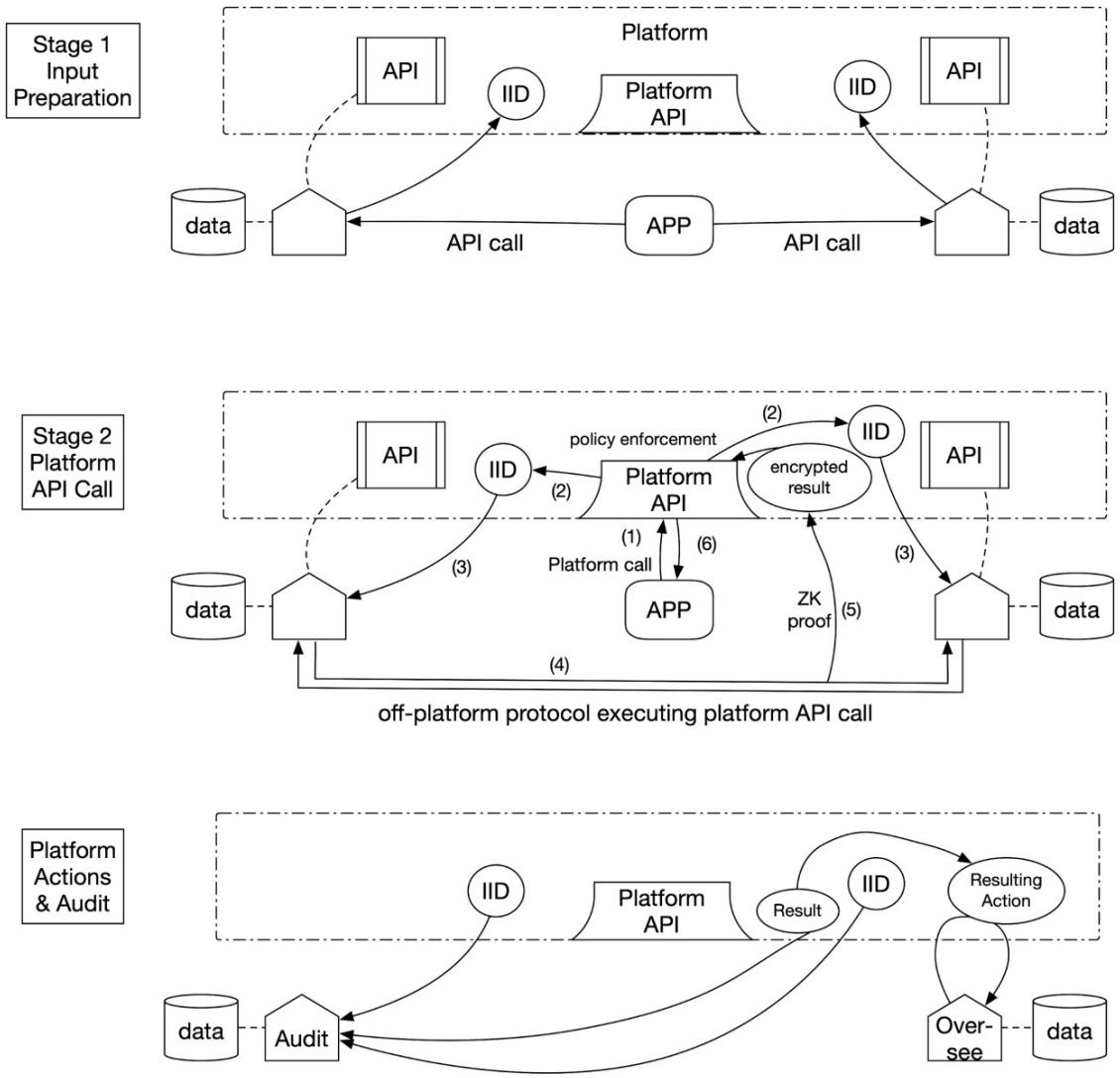


**Figure 3. System overview illustrating the two stages of a platform API call by an application that interacts with the system**

In stage 1, inputs and corresponding identifiers (IIDs) are prepared by interacting with the APIs of individual organisations. In stage 2, the platform API call is initiated; assuming it is policy compliant which is automatically enforced by the platform, it results in an off-platform protocol that executes the platform call. The platform call result is recorded on the platform and guaranteed for correctness without compromising privacy via zero-knowledge proofs. Finally,

resulting actions can take place which would be recorded and processed by an overseeing entity and an auditor capable of parsing the input identifiers with their metadata as well as the result calculated and recorded in the platform.

## 4. **Platform Use-Case: Consumer Credit Module**

In this section we show how the generic platform of the previous section can accommodate a consumer credit module (CCM). The CCM recognises three types of distinct roles: (i) credit providers (which will be banks, specialised high-risk credit companies and other similar institutions), interested borrowers, data processors and guardians (which will be debt charities and consumer organisations) and validators (which are consumer organisations).

As with all platform modules, joining the CCM as an interested borrower requires completing the platform's specific KYC process. Similarly, all the other entities fulfilling the roles described above are thoroughly vetted prior to be onboarded to the platform. Subsequently, the interested borrower empowers a data processor of her choice to collect information and perform data analytics on her platform history. This action cryptographically delegates the ability to the data processor to use suitable API calls, as well platform API calls, and collect the necessary data for producing a specific credit worthiness designation of the interested borrower. The data collector will contact all the various organisations and service providers that the interested borrowers has engaged with. Subsequently, unsupervised machine learning is used to identify with enhanced certainty the spending and saving patterns of the consumers concerned. Then through supervised machine learning the algorithms will fit identified patterns into credit scoring matrixes assigning a colour for each creditworthiness grade within the pre-agreed with lenders matrix (scoring system). Without loss of generality we assume that credit worthiness is designed by a number of different classes that are described collectively by the set C.

We do not venture here to describe the exact algorithm that is used by the data processor. Standard credit score algorithms incorporate a number of different elements of the subject's record that include payment history and regularity, the current level of debt, the total length of the credit history, as well as they are sensitive to the presence of specific event sets such as opening multiple credit cards or overdraft accounts in a short period of time. Upon completion of the operation, the interested borrower is mapped to a specific class from C. Once the class is determined, it is recorded in the platform and it becomes possible via the platform API for the interested borrower to obtain a token that is representative of her class. We note that the

token itself does not carry any other identifying information beyond the class that is assigned to her. Moreover, the token contains a cryptographic key that allows the borrower to issue digital signatures.

At the same time, the CCM runs continuously reverse auctions in which interested borrowers and credit providers can participate. Interested borrowers register interest in an auction by using their class token to digitally sign the type of contract they wish to enter. In a typical setting, the contract can specify a collateral as well as payment schedules and interest. A range of different contracts can be signed by an interested borrower thus allowing a range of options to given for consideration. Moreover, given that multiple interested borrowers can register interest, a single auction can involve multiple class tokens and ranges of contracts.

Subsequently, the credit providers engage by registering sealed bids to the platform that are accepted up to a specified deadline for each auction. Each bid specifies the type of contract that the bidder is willing to enter with the corresponding interested borrower. Sealed bids are submitted to the platform and are encrypted with the validator's public-key. The validator collects all bids, decrypts them, and calculates a matching between interested borrowers and credit providers following a suitable algorithm for the auction. The matching is binding and is published to the platform.

In order to facilitate the process, it is important that the contract types submitted by the interested borrowers are standardised and can be ordered and compared with each other. For instance, we may impose a total order in the types of contract that are submitted. Consider a range of contracts denoted by R. A total order over R is a relation "<" for which the trichotomy law applies: for any elements a, b in R, it is either the case that a<b, a=b or b<a. As a result, the total order organises the range of contracts in a spectrum of which the one end is the most preferable to the borrower and the other end is the most preferable to the lender.

We do not detail further the specific algorithm and the exact relation R to be used in the auction setting. A number of options exist, and it is expected that the CCM in the platform will support different algorithms. As an example of what may be readily deployed, consider a total order R and a validator applying a reverse Vickrey auction for the single interested borrower that pronounces as the winner the lowest bidding credit provider in terms of the total order R. Following the Vickrey mechanism, the interested borrower and the winning credit provider are bound according to the terms of the contract submitted by the second lowest bidding credit provider. The advantage of such a mechanism is that it has enforces truthfulness on the part of the credit providers as a dominant strategy.

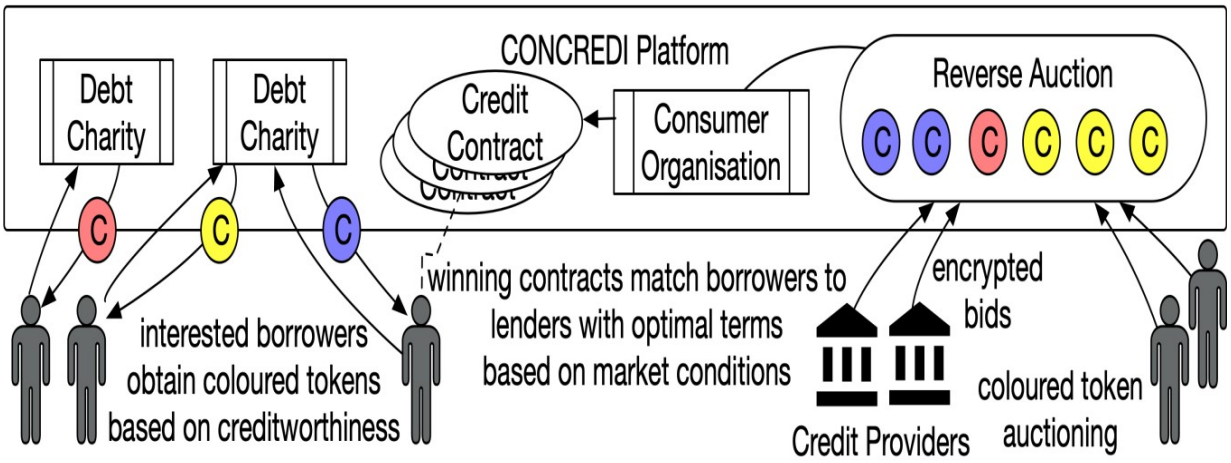


**Figure 4. Overview of the consumer credit platform ("concredi")**

## IV. THE CHALLENGE TO REGULATION

### 1. Overview of Legal and Regulatory Challenges

Decentralised finance platforms will inevitably face several legal/regulatory challenges whose resolution would be key to the success of decentralised finance. The first challenge is the type of regulation the platforms would be subjected to. This is of critical importance to also overcome the second challenge which is the cross-border issue. Today's complex spaghetti of overlapping regulatory regimes and bulky rulebooks are patently unsuitable for platform finance where rulebooks would have, to a certain extent, be coded to automate, again to the extent possible, compliance.

We have already explained in Section III how especially clear prescriptions of permitted behaviour and regulatory prohibitions can be coded and thus automated more or less in the same fashion that speed breaks work in automobiles. In the same section we explained how automated platform controls can work with respect to counterparty position limits in derivatives markets or price/order limits in short sales as regards compliance with uptick rules or circuit breakers. But this is not the only automated compliance function the platform can operate. For example, front-running can be deterred through the employment of suitably fine-grained cryptographic techniques that encrypt transactional information while still allowing the platform logic to process the trade.

This formula heightens deterrence while it minimises the costs of monitoring and any monitoring errors. In addition, the enhanced traceability of DLT systems and the availability of algorithmic techniques to conduct robust ex post audits of the fidelity of system prohibitions

and compliance checks makes ex post enforcement cheap and reliable in the event of a breach that couldn't be deterred/contained by today's regulatory technologies (RegTech). It is, therefore, highly desirable and very much in the interest of platform users, investors, consumers, regulators, and the industry for regulators to perform a large-scale simplification of their rulebooks, since any loss of discretion will be more than compensated through deterrence and enforcement gains.

On the other hand, decentralised platforms would ideally wish to operate cross-border in order to address a wider pool of investors and also to generate economies of scale and scope for the member firms. This doesn't mean, however, that all types of platforms or that all member firms and all types of investment products will have to be offered on a cross-border basis, at least in places other than the EU, which operates a single financial market. The third challenge is, of course, the matter of territoriality, especially of consumer protection laws.

In the ensuing paragraphs we offer some preliminary thoughts on how to deal with all three of them by such legal/regulatory techniques as: contracts terms standardisation, race to the top when it comes to consumer safeguards, and a stable equivalence/mutual recognition regime. Thus, we deal in turn with each of these issues offering preliminary summary proposals that can help with the resolution of some of these challenges to a satisfactory (albeit not absolute) degree of legal and regulatory certainty.

## 2. Platform Lex and Contract Standardisation

The first requirement for the smooth cross-border operation of decentralised platforms is standardisation of contractual terms that will lead to the emergence of a special *lex* attached to the platform to which both member firms and investors will have to adhere. Both fintech business and investors dealing via the platform may have to contract with it in the first place. They will be doing so on the basis of its general terms of business. Product and service contracts may be provided either exclusively by the platform acting as the agent of the supplier or bilaterally with member firms, following peer review by the system nodes and approval. Then the terms of the "smart" service and product contracts concluded on or traded through the platform will provide the law governing the contract and the forum in which any disputes would be adjudicated. The decisions of the relevant courts or tribunals in the chosen jurisdiction will be deemed as final if made in accordance with the laws and judicial norms of that jurisdiction or arbitration forum. This is already standard practice in all kinds of cross-border commercial

transactions concerning businesses and would prevent any problems with foreign judgement recognition.

On the other hand, standardisation of consumer contract terms and recognition of governing law and jurisdiction beyond the platform's general terms and conditions may prove a more challenging task if consumers are required to waive the protections of their country's consumer laws in favour of the law of the contract. Therefore, consumer contract standardisation will have to go for the maximum and not minimum level of consumer protection where the contract is offered/traded on a cross-border basis. This way automated consumer contracts offering standard terms, will compel respect by public authorities regardless of jurisdiction. Namely, cross-border consumer contracts on decentralised platforms would only become the norm if they offer the highest level of protection.

## 3. Platform Regulation and Mutual Recognition

i. *Platform Regulation*

The type of regulation decentralised platforms and financial activity on the platforms would be subjected to is very important both for domestic operations and cross-border activity. The bulk of today's financial regulation is geared towards licensing, regulation and supervision of firms and individuals as well as of investment activities. Functional regulation, whereby the rulebook focuses on the type of investment service offered or investment activity performed by the platform, would suffice to supply effective platform regulation in most cases. Yet, where the platform acts as one-stop shop offering integrated services (e.g., both advice and execution etc.), decentralised financial services platforms could stretch existing regulatory tools and concepts.

Given obvious economies of scale and scope involved in running decentralised platforms that operate as one-stop shop the pressure on regulators will be to rigorously test in sandbox and then allow some further experimental operation of integrated platforms before full licensing. Assuming, however, that the model proves successful, the subsequent form and substance of the regulation of integrated platforms in the Post-COVID-19 era would require regulators to make a quantum leap switching to platform regulation in addition to the inevitable incremental automation of compliance.

Regulation should not prevent decentralised platforms from achieving high volume and cost savings by being used to provide different functionalities, e.g., robo-advice, securities or credit broking, P2P lending, and trading forum. Regulators would still licence the type of financial

services offered via the platform and their providers. But it is also reasonable where the platform acts, as it will often be the case, as a distinct distribution channel and trading forum a further regulatory layer is imposed that deals with the platform itself. This would be in addition to the regulatory frameworks governing financial firms active on the platform and on individuals working with such firms.

Given the decentralised nature of the discussed platforms, institutional and individual compliance obligations of firms active on the platform would be supplemented by collective compliance (peer review of conduct on the platform) if the platform is also acting as a trading forum. Moreover, while the DLT platform itself will not handle HFT, it can be used for other oversight operations for an HFT system, e.g., as a registration platform for HFT algorithms and a foundation where properties of such algorithms are committed and verified.[31]

Still collective compliance at the top of individual institution compliance would necessitate a cooperative (partnership) structure for platform governance, which would augment accountability and re-align incentives, giving regulators enough comfort to allow the platform to operate even where the platform does not fully fit with today's functional and financial intermediary regulation models. Moreover, some form of platform (joint liability) insurance fund would be inevitable to incentivise platform collaborators to engage into collective monitoring of compliance and to minimize the possibility of free-riding or defection.

DLT platforms have inherent advantages in fostering continuous peer review to prevent platform members from going rogue due to their engendered properties of transparency, record immutability. These properties of DLT systems would mean that decentralised multi-party/multi-asset platforms can heighten the effectiveness of ex post audits using also atypical logic and black-boxing techniques to go through all available information. By nullifying the possibility of non-detection ex post, platform regulation can also heighten ex ante deterrence which in the case of financial crime is more or less a factor between the probability of detection and the size of the sanction. Thus, assuming that the sanction is high enough the greater the possibility of detection the lower the incentive of rational actors to engage in abusive or other criminal behaviour or behaviour that can result in the breach of a regulatory prohibition and attendant sanction.[32]

[31] In a subsequent paper we discuss the challenge for HFT for DLT platforms and the way a DLT platform can handle evidence of certain behaviours from the HFT platform.

[32] On the theory of deterrence for market abuse see Emilios Avgouleas, *Mechanics and Regulation of Market Abuse: A Legal and Economic Analysis* (Oxford University Press, 2005), Ch. 8.

Therefore, we argue that partial automation of compliance and augmentation of collective monitoring incentives can make multi-party cooperative platforms better regulated than the traditional models of financial services delivery in three respects. First, regulators will have real time access to platform operations giving them the capability of readjusting protective rules such as margin requirements, position limits, and even price limits increasing the possibility of timely action to minimise large-scale market shocks. Secondly, the platform could be equipped with a number of switches which would nullify the possibility of certain types of rogue behaviour such as front-running, automating, to some extent, the prevention of market abuse. Another good example in this context is building a smart contract with ex ante permissions which controls the grant and exercise of executive stock options automating compliance. The stock option schedule would be enforced algorithmically based on timing information and/or market conditions, while the smart contract code itself will be updatable only in specific circumstances that are publicly verifiable.

While none of the above would automatically resolve the problem of conflict of interests that may arise due to possible full integration of investment advice via Robo-advisors and trading and execution services, still knowledge of the possibility of rigorous and speedy ex post auditing of suspicious behaviour can bring ex ante compliance to a very high level. Cryptographic techniques can actually play a significant role in improving the ability of ex post audits in the context of Robo-advisor machine learning models as demonstrated recently via the use of hashing to identify specific instances of machine learning models and tying them to the advice they produce.[33] Moreover, certain other safeguards such as best execution can be fully automated resolving a major regulatory headache in this context.

Similarly, as all decentralised platforms shall be permission-based to avoid the problems that have plagued cryptocurrency platforms, there will be a set process for permitting new members on the platform (whether firms or investors), so-called "onboarding". In terms of cost savings, the advantage of integration will come from the ability to share onboarding costs between different organizations. Using a distributed ledger to organize and share information across banks and financial institutions can dramatically slash the costs of onboarding for the system

[33] See Lamprini Georgiou and Aggelos Kiayias, "The right to Robot-Identification: using cryptographic hashes to manage AI black-boxes". Manuscript. (2020). Available from the second author.

as a whole.[34] At present, costs for KYC are substantial (up to $500M per year per bank)[35] while the process itself is cumbersome with low customer satisfaction (a staggering 89% of customers are not satisfied with their KYC experience).[36]

Onboarding will also presuppose compliance with Know Your Customer (KYC). Thus, client classification in accordance with pre-set conduct of business rules could become much faster and also shared via the platform in a privacy preserving way, creating serious cost savings and synergies for platform members.

The benefits of integration for KYC/AML go beyond cost savings though. Detecting money laundering requires collecting and processing information that is drawn from different sources. This is to some degree facilitated by reports such as Suspicious Activity Reports (SARs) required, e.g., in the UK under the POCA[37] 2002 and similar legislation in other countries. Nevertheless, international crime networks have managed to continue operating covertly (as exemplified e.g., by the infamous "Global Laundromat" operation which laundered more than $20B from Russia in the period 2011-2014 with 50% of the funds transferred via the UK).[38] This highlighted that significant improvements in automation and cross organization data processing would be needed to detect money laundering activities. Integration via cryptographic protocols, as we advocate here, have already been identified as the fundamental game-changer in this context.[39]

---

[34] See José Parra Moyano, Omri Ross: KYC Optimization Using Distributed Ledger Technology. Bus. Inf. Syst. Eng. 59(6): 411-423 (2017)

[35] Ibid.

[36] See Thompson Reuters (2016) Know your customer (KYC) independent survey, Available from https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html (last accessed June 5, 2020).

[37] See Part 7, Proceeds of Crime Act 2002, Available from http://www.legislation.gov.uk/ukpga/2002/29/contents (last accessed June 5, 2020).

[38] See Caelainn Barr and Cath Levett, More than half the funds laundered in a major Russian scheme went via the UK, The Guardian, 25 March 2017.

[39] See for instance, the 2019 Global AML and Financial Crime TechSprint, where systems like "Secret Computers" demonstrate how suspicious transaction networks can be identified by cross-correlating in a privacy preserving manner data across different institutions via cryptographic protocols. Available from https://www.fca.org.uk/events/techsprints/2019-global-aml-and-financial-crime-techsprint, (Last Accessed June 4th, 2020).

Nonetheless, other parts of regulatory rulebooks such as compliance with certain Conduct of Business rules, e.g., the requirement to treat customers fairly may be impossible to automate based on today's technology and thus regulators will inevitably have to ban platforms from offering or selling very complex financial products to retail customers. Similarly, at the investment origination level all rules on due diligence and disclosure ought to be observed by issuers to gain access to primary markets and these will also incur the relevant costs. Still platform nodes and users may engage with the scrutiny of disclosures and the fidelity of due diligence documents stored in cryptographic hashes. This form of likely peer review, given also the higher level of transparency that DLT platforms offer, can lead to very effective levels of scrutiny probably higher than that applicable today in primary markets.

The same applies to trading and reporting in secondary markets. In fact, issuer disclosure and regulatory reporting processes are ripe for automation. Similarly, smaller issuers will benefit from the combination of platform's lower admission fees  advantageous regime for SMEs going public like those in the EU Prospectus Regulation.[40] As a result, EU and domestic regimes governing equity crowdfunding and other forms of equity (or shared benefit) finance will have to be streamlined and upgraded to both secure investor protection and facilitate retail investment market integration and the faster/easier access of EU SMEs to equity capital.

*(ii) The Cross-border Dimension*

It may prove impossible for decentralised platforms to succeed if they face the risk of compliance with multiple legal and regulatory orders when they operate on cross-border basis, at least outside the EU which maintains a single rulebook for its 27 member states. It follows that these platforms would either need to operate locally, which would harm platform efficiencies or become the subject of some serious political and regulatory horse-trading under a mutual recognition or equivalence regime. The preference would of course be for a streamlined and secure processes that would go beyond equivalence reviews.[41] But the path to such streamlined process is today quite unclear and may not be possible in the short-term. It follows that in terms of platform regulation, as with legal contracts offered by the platform,

[40] Regulation (EU) 2017/1129 on the prospectus to be published when securities are offered to the public or admitted to trading on a regulated market, and repealing Directive 2003/71/EC (esp. Art. 15), as amended by Regulation (EU) 2019/2115 as regards the promotion of the use of SME growth markets.

[41] E.g., in the EU "equivalence "reviews and decisions to grant the corresponding status are conducted by the EU Commission a body strictly comprising political appointees who, however, should be working to further Union interest and not the interests of the member state governments which appointed them

only a race to the top would allow decentralised finance platforms to pass equivalence tests conducted by foreign regulators to secure cross-border access.

On the other hand, the importation of the regulatory *lex* may be automated. When, for example, the asset allocation and execution services are delegated in systems' code, the same code could "delegate" (pass on) the rules with which the delegated should comply with - de facto exporting different conduct of business rules. Essentially this process would turn jurisdictions to which the service is outsourced to rule-takers. However, in the event of a complaint, conflict of jurisdictions may still arise depending on where the court will deem the place of characteristic performance, also relating to the place of investor's residence to be.

## V. CONCLUSION

Our aim in drafting this paper was three-fold. First to highlight how the development of decentralised finance outside the cryptocurrency space can augment socio-economic growth and inclusion while serving long-term investment objectives. Secondly to offer a model of decentralised finance architecture ranging from cryptographic integration to platform governance and regulation. Third to explain through use cases how decentralised finance can resolve thorny and complex socio-economic problems including that of consumer and household over-indebtedness and of privacy preserving access to finance.

One of the least discussed and appreciated aspects of moving fundamental market infrastructure to DLT is the recovery of control to ultimate investors. Arguably, the current FMI for both securities and derivatives markets gives rise to a number of social costs. In the case of securities, a chain of custodians holds in a sequence the dematerialised security which investors control only indirectly. But while asset dematerialisation and fungibility have improved system efficiency by increasing liquidity they have also led to loss of investor control in a way that favours intermediaries' short-termist investment strategies which are further augmented via short-selling, leverage, and leveraged repo financing, all lubricated via intermediary control of investors' securities and of the investment chain.

Repatriation of control through migration of trading over DLT platforms may have a transformative impact on the allocation of financial resources. Especially combined with democratization of access, discussed below, can allow altruistic forces and psychological biases favouring fairness to broaden asset allocation choices. This wouldn't just make financial markets more pluralistic placing them at the service of society's pressing needs for

sustainability and social market investment, but it would also augment economic and financial system resilience through diversification.

In the model of *open and decentralised finance* we offer in this paper we identify three fundamental properties. First, we demonstrate how we can create an open and competitive financial system through utilisation of cryptographic integration via API (application programming interface) integration. Thus, we introduce a novel concept of cryptographically integrated APIs to offer functions that are cross-organisation by design and are mediated by a distributed ledger which assists as an auditing tool of such operations for compliance.

In the middle level, customer-driven decentralized applications will facilitate important breakthroughs to a number of socioeconomic problems that have seemed intractable for so long. Even more critically we offer a consumer credit use case to accentuate the potential of multi-purpose and multi-asset platforms operating on the basis of cryptographic integration to further socio-economic purposes.

Third, at the outermost layer of our model of open decentralised finance algorithms will recognise in real time the connection (but not hierarchy) between express investor goals (e.g, risk/return maximisation plus ethical and social objectives plus sustainability) and market conditions, including availability alternative investments. Then it would continuously weigh through parametrisation and align investor portfolios with their express investment preferences, even if such portfolio composition does not maximise risk-return efficiencies. Parametrisation can lead to greater pluralism in resource allocation and investment diversification reflecting the will of the systems' participants, while continuous adjustment of the relevant parameters would enable the system to keep evolving.

Finally, we have highlighted the key directions financial and regulatory technology must take and the approach policy-makers need to adopt to foster open decentralized finance. Moving in that direction at a rapid speed is also necessary in order to avoid the domination of the new infrastructure by big financial institutions and BigTech which will not only choke competition and the pace of future innovation but will also perpetuate today's model of speculative and monocultural finance. This trend towards investment homogenization has not only done a dis-service to humanity in terms of furthering society's needs for socio-economic growth but has also created fragile economic and financial systems.