Routledge
Taylor & Francis Group

Law and Financial Markets Review

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rlfm20

DLT-based enhancement of cross-border payment efficiency – a legal and regulatory perspective

Dirk A. Zetzsche, Linn Anker-Sørensen, Maria Lucia Passador & Andreas Wehrli

To cite this article: Dirk A. Zetzsche, Linn Anker-Sørensen, Maria Lucia Passador & Andreas Wehrli (2021) DLT-based enhancement of cross-border payment efficiency – a legal and regulatory perspective, Law and Financial Markets Review, 15:1-2, 70-115, DOI: 10.1080/17521440.2022.2065809

To link to this article: https://doi.org/10.1080/17521440.2022.2065809

Published online: 15 Jun 2022.

LAW AND FINANCIAL MARKETS REVIEW
2021, VOL. 15, NOS. 1–2, 70–115
https://doi.org/10.1080/17521440.2022.2065809

Routledge
Taylor & Francis Group

DLT-based enhancement of cross-border payment efficiency – a legal and regulatory perspective*

Dirk A. Zetzsche [a], Linn Anker-Sørensen [b], Maria Lucia Passador [a] and Andreas Wehrli[c]

[a]Faculty of Law, Economics and Finance, University of Luxembourg, Luxembourg; [b]Ernst & Young Tax and Law, University of Oslo, Oslo, Norway; [c]Swiss National Bank. Formerly Bank for International Settlements, Bern, Switzerland

ABSTRACT

Financial law and regulation have, to date, assumed that regulated activities and functions are concentrated in a single legal entity responsible and accountable for operations and compliance. Even with regard to financial market infrastructure where the regulatory perspective acknowledges the need for interoperability of many entities as a system, each entity is subject to its own rules and regulations, and can thus meet its own compliance requirements independent of other system participants. The entity-focused regulatory paradigm is under pressure in the world of DLT-based payment arrangements where *some* ledgers, and thus the performance of the services as such, are distributed. DLT arrangements could provide an alternative to the traditional reliance on a mutually trusted central entity to transfer funds and enable the creation of new foundational infrastructures by distributing technical functions or linking existing systems. As such, we identify and outline concepts for use cases where DLT is potentially improving the efficiency of cross-border payments, namely a Best Execution DLT, a DLT application for a Network of Central Banks, a DLT as an AML/KYC utility, as well as DLT arrangements for an Identity Platform, a Small Payments Platform and, finally, an Interoperability Platform connecting multiple closed-loop and proprietary banking systems. Despite the wide-ranging interest in DLT-based payment systems, research so far has focused on technical concepts and lacked legal details. This article seeks to fill this gap by providing an initial analysis of the legal challenges related to DLT-based payment systems. From a legal perspective, the distribution of functions in DLTs comes with new risks created from the *joint* performance of services and functions as main characteristic of a distributed ledger, and the need for additional agreements, ongoing coordination across, and governance arrangements among the nodes. Further, in a cross-border context, multiple regulators and courts of

CONTACT Dirk A. Zetzsche dirk.zetzsche@uni.lu

*This article benefitted from comments by Douglas Arner, Ross Buckley, Jon Frost, Thomas Lammer, Nadia Manzari, Tara Rice, Takeshi Shirakami, Jannik Woxholth, and participants at the Bank for International Settlements / Committee on Payments and Market Infrastructures (CPMI) conference on 'Enhancing cross-border Payments', 18 March 2021.

various countries (asking for compliance with their own set of rules and regular reporting) will be involved. All of these must decide whether for compliance with any *single* rule they look at the DLT as a whole (herein called 'the ledger perspective') or each individual node (that is each institution participating in the DLT, herein called 'the node perspective'). Moreover, financial and private law must provide for risk allocation, liability, responsibility and accountability for all legal obligations related to each function and activity. This article examines the extent to which the ledger perspective or the node perspective should prevail against the backdrop of a range of DLT use cases, resulting in policy recommendations for regulators. In this article, we propose the adoption of what we call an enabling approach for payment systems: ledger operators must specify in a Plan of Operations subject to regulatory approval to which rights and obligations the ledger perspective applies; in the absence of such a stipulation, rules apply based on the node perspective. However, for systemic risk controls, AML/CFT, data protection and governance, as well as DLT governance, we propose a reversed default rule in which the ledger perspective prevails in the absence of rules stipulating that the node perspective applies. Finally, in private law matters, we propose protecting consumers and SME clients through a standardised payment services contract structure, without mandating details.

ARTICLE HISTORY Received 9 February 2022; Accepted 7 March 2022

KEYWORDS DLT: distributed ledger technologies; risk control; governance; data protection; payment services

A. Introduction

Cross-border payments suffer from high costs, low speed, limited access, and insufficient transparency,[1] and enhanced cross-border payment services would provide widespread benefits for citizens and economies worldwide, supporting economic growth, international trade, global development and financial inclusion.[2]

Distributed Ledger Technologies (DLT) have been proposed,[3] critically discussed[4] and even tested by some central banks[5] and private

[1]cf Financial Stability Board, 'Enhancing Cross-Border Payments. Stage 1 Report to the G20: Technical Background Report' (9 April 9 2020) 2–4 <https://www.fsb.org/wp-content/uploads/P090420-1.pdf>, at 2–4; McKinsey & Company, 'The 2020 McKinsey Global Payments Report' (2020) <https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/accelerating%20winds%20of%20change%20in%20global%20payments/2020-mckinsey-global-payments-report-vf.pdf>.

[2]See Committee on Payments and Market Infrastructures, 'Enhancing Cross-Border Payments: Building Blocks of a Global Roadmap. Stage 2 Report to the G20' (July 2020).

[3]See David Mills and others, 'Distributed Ledger Technology in Payments, Clearing, and Settlement' (2016) Bd of Governors of the Fed Reserve Sys, Finance and Economics Discussion Series 2016-095 at 10–11.

[4]See Ellen Naudts and others, 'DLT for (Cross-Border) Payment Systems: Governance and Oversight – An Abstract (20 January 2021)' 1.

[5]See IMF and others, 'Distributed Ledger Technology Experiments in Payments and Settlements. Note/20/01' at 4; World Economic Forum, 'Central Banks and Distributed Ledger Technology: How are Central Banks Exploring Blockchain Today?' (March 2019) <http://www3.weforum.org/docs/WEF_

entities[6] as technologies that could increase cross-border payments efficiency and financial inclusion.[7] DLT's conceptual proposition of a distributed and synchronised ledger, shared by various entities, is particularly suited to the creation of a multilateral arrangement for public and private Payment System Providers (PSPs), subject to a set of business and operational rules and agreed technical standards.[8] DLT enables a new distributed *infrastructure* for payments, where participating PSPs, the institutional and technical design, and the distinct rulebook for the network represent its *architecture*.

DLTs have inspired great expectations, indeed. Some argue that DLT could result in faster (almost real-time) processing, easier reconciliation and greater transparency on fees, while foregoing, for instance, the risk associated with intermediaries in the payment chain.[9] DLT could also result in an auditable source of information in terms of digital identity, shared and verified across a network of organisations aiming at KYC compliance, given that DLTs allow for certification of the payors' and payees' provenance (due to the immutability of data recorded in the ledger) as well as multi-party aggregation.[10] Further, a DLT-reduction of payment costs could enhance financial inclusion and address the issue of pricy remittance transfers.[11]

Despite the wide-ranging interest in DLT-based payments, the long anticipated DLT-based payment services revolution has not occurred. We show in this article that one of the reasons for the underperformance of DLT payment systems are unsolved legal challenges relating to DLT. The analysis to date

Central_Bank_Activity_in_Blockchain_DLT.pdf>; César A Del Río, 'Use of Distributed Ledger Technology by Central Banks: A Review' (2017) 8 Enfoque UTE 1 <https://www.redalyc.org/jatsRepo/5722/572261717001/html/index.html>; Fred Huibers, 'Distributed Ledger Technology and the Future of Money and Banking' [2021] Acct Econ L (assuming that DLT-based competition and diversity could increase stability and efficiency of the financial system).

[6]See, for instance, David Floyd, 'Overstock's t0: Reconciling Fiat Currency and the Bitcoin Blockchain' (*NASDAQ*, 16 December 2015) <https://www.nasdaq.com/articles/overstocks-t0-reconciling-fiat-currency-and-bitcoin-blockchain-2015-12-16>.

[7]Projects in this sense are described in Robert M Townsend, *Distributed Ledgers. Design and Regulation of Financial Infrastructure and Payment Systems* (MIT Press 2020), chapter 8, 115–16.

[8]*Financial Stability Board* (n 1) at 12.

[9]Deloitte-MAS, 'Understanding the Regulatory Requirements of the MAS Payment Services Act (2019) at 10 <https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/financial-services/sg-fsi-payment-services-act-2019-wns.pdf>.

[10]ibid at 12; CIPHERTRACE, 'Cryptocurrency Crime and Anti-Money Laundering Report' (February 2021) <https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report>.

[11]See Naudts and others (n 4) 4: Jesse Leigh Maniff and W Blake Marsh, 'Banking on Distributed Ledger Technology: Can It Help Banks Address Financial Inclusion?' [2017] Fed Reserve Bank of Kansas City Econ Rev 53, 59–69 <https://www.kansascityfed.org/research/economic-review/3q17-maniffmarsh-banking-distributed-ledger-technology>; International Telecommunication Union, 'Distributed Ledger Technologies and Financial Inclusion' (2017) <https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Report-on-DLT-and-Financial-Inclusion.pdf>; World Bank, 'Blockchain & Distributed Ledger Technology (DLT)' (*Worldbank*, 12 April 2018) <https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt>; Deloitte, 'The Changing Paradigm of Distributed Ledger Technologies' (2020) at 2 <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology/2020-gbcs-ip-bcm.pdf>.

has dealt with technical concepts and lacked legal detail.[12] This article aims to fill this gap by offering an analysis of the legal challenges regarding the DLT-based payment systems, revealing a conceptual challenge to integrate DLT and its inherent distribution of functions into the existing legal and regulatory environment, and proposing a solution to deal with the challenges identified. To this end, we understand legal challenges as all issues related to law and regulation, including private and public law, financial supervision as well as the system's setup, data privacy and data protection.

In fact, to enhance the efficiency of cross-border payments, it is essential to take a look at law and regulation, for at least four reasons. *First*, law and regulation are part of risk management. Any regulatory approach needs to consider the risks (such as the Herstatt risk[13]) for both payment institutions and end-users. This is true regardless of whether cross-border payments rest on correspondent banks, a closed-loop payment system, a multilateral platform (such as Target2) or a peer-to-peer payment system.[14] *Second*, law and regulation – in association with the work of standard-setting bodies – drive the standardisation of terminology, interfaces and parties' obligations. *Third*, law and regulation are often a precondition and enabler for cross-border cooperation of regulators.

Fourth, the regulation of payment systems is often part of a broader policy agenda. For instance, the immense political investment in a harmonised framework for intra-EU/EEA domestic payments[15] is best explained by the goal of supporting the EU's economic and monetary union. Often, the regional integration agenda conflicts with (1) the global setup and activities of large financial institutions that function as major correspondent banks or as building blocks of interregional multilateral systems, and/or (2) the approach of

[12] *IMF and others* (n 5) at 2–8. See also Christoph Aymanns, Mathias Dewatripont and Tarik Roukny, 'Vertically Disintegrated Platforms' (20 December 2019) <https://ssrn.com/abstract=3507355>; Alexander Lipton, 'Blockchains and Distributed Ledgers in Retrospective and Perspective' (2018) 19 J Risk Fin 4, 14–15; Thomas Ankenbrand and others, 'A Structure for Evaluating the Potential of Blockchain Use Cases in France' (2017) 17 Perspectives of Innovations, Economics & Bus 77, 83–85; Deutsche Bundesbank, 'Distributed Ledger Technologies in Payments and Securities Settlement: Potential and Risks. Monthly Report' (September 2017) 35–49; Philip Paech, 'The Governance of Blockchain Financial Networks (2017) 80 Modern L Rev 1073.

[13] Hal S Scott and Anna Gelpern, *International Finance, Transactions, Policy, and Regulation* (23rd edn, Foundation Press 2020) 728–42.

[14] *Financial Stability Board* (n 1) at 8, figure 5. For financial market infrastructures, a framework for addressing inherent risks is set out in Committee on Payment and Market Infrastructures (CPMI) and the International Organization of Securities Commissions' (IOSCO's), 'Principles for Financial Market Infrastructures (PFMI)' (April 2012) <https://www.bis.org/cpmi/publ/d101a.pdf>.

[15] See, in particular, the Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015, on Payment Services in the Internal Market [2015] OJ L337/35 (PSD2) and the EU Digital Finance Strategy (DFS) as the last building block. In particular, PSD2 aims at enhancing competition, reducing fees and improving system resilience in the payments industry by lowering barriers to entry for Fintech and other new participants seeking access to financial data of payment system users. See also Dirk A Zetzsche and others, 'The Evolution and Future of Data-Driven Finance in the EU' (2020) 57 CMLR 331, 347–49 (specifying the underpinning on which PSD2 started to operate and describing the role of PSD2 in 'pushing forward the transition to data-driven finance in Europe's Single Payments Market and potentially more broadly').

globally active closed-loop systems that seek to build a *global* rather than regional payments platform.

In the legal context, the IMF[16] has identified two questions that have yet to be answered: First, to what extent does the use of DLT require new interpretations of existing international standards for payment systems and capital market infrastructure more generally? Second, what are the implications for regulation, supervision, and oversight in a world that is moving toward greater real-time settlement, flatter structures, continuous operations and global reach?

While comprehensive answers are out of reach, we nevertheless provide some early steps to address these questions. Currently, law and regulation of payments are contingent on the assumption that ownership, governance, accountability and responsibility for legal rights and obligations are concentrated in *one* legal entity. In turn – applied to a DLT context – the law so far looks at each node separately, establishing the duties and obligations of that node, and in turn, each node can meet its compliance obligations independently and irrespectively of others. For this viewpoint (referred to as '*the node perspective*'), the perspective of the ledger is derived from the individual rights and obligations of each node and is thus of secondary importance. Adapting existing payment laws to DLTs – which by definition rely on some degree of distribution of functions – will require, for single *each* legal, regulatory and contractual right and obligation, a decision as to whether the technical distribution of functions among the ledgers should be acknowledged by law (i.e. whether the law shall adopt what we call herein '*the ledger perspective*'). In this article, we examine the extent to which the ledger perspective or the node perspective shall prevail against the background of a number of DLT use cases, culminating with policy recommendations for regulators.

The article is structured as follows: Part B summarises the current state of research and regulatory reports on the origin and cost drivers of cross-border payments, as well as the potential of DLT to improve cross-border payments in general; Part C describes specific use cases where DLT is potentially enhancing the efficiency of cross-border payments; Part D deals with the general legal perspective, arguing that the core legal question is whether the ledger or the node perspective prevails; Part E provides policy considerations; and Part F concludes.

B. DLT as a focal point for more efficient cross-border payments

To provide some context on the potential impact of DLT on payments, we first give an overview of the cost drivers, as well as the benefits and risks of DLT-based (cross-border) payments.[17]

[16] *IMF and others* (n 5) 8–9.

[17] Mahdi Zamani and others, 'Cross-Border Payments for Central Bank Digital Currencies via Universal Payment Channels' at paragraph 2.3 <https://www.bis.org/events/cpmi_ptfop/proceedings/paper14.pdf>.

I. Introducing DLT as an infrastructure

A distributed ledger is 'a database that is consensually shared and synchronised across networks, spread across multiple sites, institutions or geographies, allowing transactions to have [multiple private or] public "witnesses"'.[18] Data sharing results in a sequential database distributed over a network of servers that all work together as a ledger.[19] Distributed ledgers are characterised by no (or minimal) central administration and no centralised data storage. They are, therefore, 'distributed' in the sense that permission to record a given piece of information stems from the software-driven interaction of multiple participants. Coupled with cryptographic solutions, these features (decentralisation and distribution across a computer network) reduce the risk of data manipulation, thus solving the problem of trusting third parties, and specifically data storage service providers.[20]

The modus operandi of distributed ledgers is best understood by contrasting them with a traditional electronic concentrated ledger administered by a single entity. The latter entails a number of risks. First, if the hardware where the register is 'located' is destroyed, the information contents and the authority to ascertain that they are correct are lost.[21] Second, an unfaithful administrator (or disloyal employees, as the case may be) can manipulate the information stored in the register. Third, a cyber-attack may result in manipulations and data losses.[22] Distributed ledgers address these problems by raising the barrier for manipulation. The underlying technology requires the consensus of many data storage points ('nodes'). If there are *n* nodes (instead of one concentrated ledger) and *e* describes the effort necessary to break into any single server, all other conditions being equal (safety per server etc.), the effort necessary to manipulate all the linked servers will be *n* x *e* rather than 1 x *e*.

[18]World Economic Forum, 'Innovation-Driven Cyber-Risk to Customer Data in Financial Services – White Paper 6' (2017) <https://www.weforum.org/whitepapers/innovation-driven-cyber-risk-to-customer-data-in-financial-services>.

[19]See *Mills and others* (n 3).

[20]See Michèle Fink, *Blockchain Regulation and Governance in Europe* (CUP 2019) 12–14. See also Sinclair Davidson, Primavera De Filippi and Jason Potts, 'Blockchains and the Economic Institutions of Capitalism' (2018) 14 J Inst Econ 639 (arguing that blockchain technology is a new governance institution that competes with the other economic institutions of capitalism, i.e. businesses, markets, networks, and even governments); Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Harvard UP 2018) at 55, 136–40 (arguing that the spread of blockchain will lead to technology-based business practices that could induce a loss of importance of centralised authorities, such as government, and urging a more proactive regulatory approach).

[21]In practice, payment system resiliency and contingency plans usually limit this risk with hot copies of the ledger at a secondary site of operations.

[22]Any server *can* be manipulated with sufficient computing power and time (even if no other weakness in an encryption system is known to the attackers). See, generally, Jean-Philippe Aumasson, *Serious Cryptography: A Practical Introduction to Modern Encryption* (No Starch Press 2017) 10–18, 40–48.

The distributed ledgers of today are usually paired with a blockchain protocol.[23] Blockchain refers to the storage of all data parts as data bundles (the 'blocks') in a strict time-related series which links each block, through a time stamp, to the previous and subsequent blocks. The blockchain renders data corruption even harder, because a successful cyber-attack would require simultaneously corrupting not just one set of data, but multiple data sets (i.e. the whole blockchain) as well as the time stamps. Distributed ledgers have provided fertile ground for the application of another innovation that may solve the problem of trust in human interactions: smart contracts. While neither smart, nor contracts, they are in fact self-executing software protocols that reflect the terms of an agreement between two parties.[24] The conditions of the agreement are directly written into lines of code. Smart contracts permit the execution of transactions between disparate, anonymous parties without the need for an external enforcement mechanism (such as a court, an arbitrator, or a central clearing facility). They render transactions traceable, transparent, and irreversible. Since processes driven by smart contracts are often saved on distributed ledgers, we refer to these three technologies collectively as 'distributed ledger technologies' ('DLTs').

II. DLT as a means to enhance payments efficiency

The Financial Stability Board (FSB) and the Committee on Capital Market Infrastructures (CPMI) identify four impediments to efficient cross-border payments: costs, lack of speed, limited access, and lack of transparency.[25]

Costs comprise transaction fees, account fees, compliance, FX and liquidity costs and fees along the payment chain, with charges for cross-border payments amounting 'up to 20 times those for domestic transactions'.[26] Some of these costs are related to legal matters: on the *front-end*, the know-your-customer and client onboarding rules, and ongoing diligence processes to update clients' status later add to the costs. Meanwhile, *back-end* costs

[23] See, e.g. *De Filippi and Wright* (n 20) 33–58; Dirk A Zetzsche, Ross P Buckley and Douglas W Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' [2018] U Ill L Rev 1361, 1372.

[24] See, e.g. Anthony J Casey and Anthony Niblett, 'Self-Driving Contracts' (2017) 43 J Corp L 1, 5; Joshua Fairfield, 'Smart Contracts, Bitcoin Bots, and Consumer Protection' (2014) 71 Wash & Lee L Rev. Online 35, 36; Karen EC Levy, 'Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and The Social Workings of Law' (2017) 3 Engaging Sci Tech & Soc'y 1; Kevin Werbach and Nicolas Cornell, 'Contracts ex Machina' (2017) 67 Duke LJ 313.

[25] *Financial Stability Board* (n 1) at 13–14; Committee on Payments and Market Infrastructures, 'Cross-Border Retail Payments' (February 2018) <https://www.bis.org/cpmi/publ/d173.htm>. This time-related issue is perhaps even worse given that 'the lack of common communication or messaging standards across systems often hinders seamless interoperability' (European Central Bank – Bank of Japan, 'Synchronised cross-border payments' (June 2018) at 1 <https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical190604.en.pdf>). For a general overview, see Jon Cunliffe, 'Cross-Border Payment Systems Have Been Neglected for Too Long' *Financial Times* (London, 13 July 2020) <https://www.ft.com/content/a241d7e0-e1de-4812-b214-b350cbb7d046>.

[26] *Scott and Gelpern* (n 13) at 744.

include costs for compliance, AML and regulatory reporting, as well as negotiation and management of interbank service agreements (including charges).[27] Issues increase with countries less often involved in cross-border transactions[28] (i.e. where fewer correspondent banks (if any) are active and legal matters non-standard and/or unknown).

As for lack of speed,[29] the main drivers include a lack of technical integration, manual processes, and the need to review diverging legal requirements. Meanwhile, limited access impacts SMEs and individuals who might lack access to services to make cross-border payments. Moreover, PSPs may face limitations when it comes to accessing local or foreign payment systems, due to high barriers of a technical, financial or regulatory nature. In addition to Herstatt risk mitigation, ongoing legal due diligence requirements add to the costs of maintaining a cross-border network. Finally, transparency is limited since cross-border payment data (with volumes and fees) are rarely published with names of parties and payment institutions involved.[30] Central banks, applying the 2020 IMF Transparency Code,[31] increasingly abandon aggregated data collection in favour of more granular reporting. However, additional efficiency gains could stem from integrating correspondent banks and closed-loop systems into one transparent payment *architecture and infrastructure* run and managed in the public interest.[32]

Enhancing cross-border payments is a multifaceted problem requiring a comprehensive approach, and DLT could be one way of addressing these inefficiencies. Employing distributed networks for that purpose is not new per se. Relevant approaches include, for instance, the *Hawala* payment system[33] dating back to the 700s that, beyond

[27]The diversification of the front end and the back end levels is described in Financial Stability Board (n 1) at 8.

[28]Whereas mainstream countries are 'moving towards one common global standard for financial messaging, called ISO 20022. Global adoption of this standard is accelerating with a number of high-value payment market infrastructures already live and more planned to go live by 2023.' (KPMG, 'A New Standard for Payments' (2020) <https://home.kpmg/xx/en/home/insights/2020/02/payments-standard.html>).

[29]The need to accelerate the pace of cross-border payment systems is not, however, a last-minute requirement, as the following contributions testify: Morten Linnemann Bech, Yuuki Shimizu and Paul Wong, 'The Quest for Speed in Payments' (March 2017) at 57 et seq. <http://www.bis.org/publ/qtrpdf/r_qt1703g.htm>; 'IBM Launches Blockchain Banking Network To Speed Cross-border Payments' (*ICT Monitor Worldwide*, 17 October 2017).

[30]On the general lack of transparency issue, see KMPG, 'Cross-Border Interbank Payments and Settlements. Emerging Opportunities for Digital Transformation' (November 2018) at 13–14 <https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Cross-Border-Interbank-Payments-and-Settlements.pdf>.

[31]International Monetary Fund, 'The Central Bank Transparency Code' (30 July 2020) <https://www.imf.org/en/Publications/Policy-Papers/Issues/2020/07/29/The-Central-Bank-Transparency-Code-49619>.

[32]Casper L van Ginneken, 'Settlement of Cross-Border Transactions Through Central Bank Digital Currency (CBDC): Analysis from a Risk Management Perspective' (M.Sc. thesis, University of Twente 2019) 73 <https://essay.utwente.nl/78027/1/Ginneken_MA_BMS.pdf>.

[33]*Hawala* is an informal value transfer system (without money movement) based on the transfer of debt between a network of money brokers (the *hawaladars*) operating outside of, or parallel to, traditional

raising criticism due to its intransparency,[34] is said to have inspired the Ripple DLT.[35]

In fact, a closer look reveals that DLT comes with features that potentially assist in removing or lowering the four barriers just mentioned.

First, through DLT any data stored on the ledger become very hard to delete (immutability).

Second, DLT relies on the same software code stored and run on multiple ledgers simultaneously, ensuring technical synchronisation of all servers participating in the ledger. Once the code has been designed, programmed, and implemented, full technical integration, including a built-in settlement mechanism, increases the speed of technical processing (if the code is well programmed and a sound governance mechanism ensures that code updates are properly managed).

Third, as a multilateral system, a DLT-based system is in principle accessible by many parties at roughly the same time. A DLT creates a network by connecting all nodes by means of a code; each node is connected to every other node, avoiding a single point of failure. In terms of payment systems, connections represent embedded links across the nodes which could be used for many purposes (information distribution, account relationships, etc.).

Finally, DLT improves transparency as it shares information with all nodes storing the same data almost in real time,[36]and could therefore improve the efficiency and quality of supervision, even levelling the playing field among small and large firms.[37] At the same time, advanced data partitioning concepts, with only a portion of the data accessible to all nodes, potentially reduces data protection and privacy concerns (Figure 1).[38]

The enhanced transparency, access and speed can be used to create and activate competition as well as for regulatory or supervisory purposes. For

banking, financial channels, and remittance systems. *Hawala* is distinguished from other remittance systems by the reliance on trust amidst the brokers that form the *Hawala* network, rendering it operable even in the absence of legal enforcement. See Gamal Moursi Badr, 'Islamic Law: Its Relation to Other Legal Systems' (1978) 26 Am J Comp L 187.

[34]NS Jamwal, 'Hawala – The Invisible Financing System of Terrorism' (2008) 26 Strategic Analysis 181; Rachana Pathak, 'The Obstacles to Regulating the Hawala: A Cultural Norm or a Terrorist Hotbed?' (2003) 27 Fordham Int'l LJ 2015; Financial Action Task Force, 'The Role of Hawala and Other Similar Service Providers in Money Laundering and Terrorist Financing' (2013); Patrick M Jost and Harjit Singh Sandhu, 'The Hawala Alternative Remittance System and Its Role in Money Laundering' (2000) at 5.

[35]Due to trust-based account re-balancing similar to modern correspondent banking, *Hawala* functions cross border without actually transferring money, yet rather than using capital-based counterparty risk mitigation Hawala relies on a kind of collective liability of all nodes. We will turn back to this particularity which is at the heart of the legal dimension of DLT, below at D.

[36]Committee on Payments and Market Infrastructures, 'Distributed Ledger Technology in Payment, Clearing and Settlement. An Analytical Framework' (February 2017) 1.

[37]Raphael Auer, 'Embedded Supervision: How to Build Regulation Into Blockchain Finance' (2019) BIS Working Papers No. 811.

[38]See Xiaohui Yang and Wenjie Li, 'A Zero-Knowledge-Proof-Based Digital Identity Management Scheme in Blockchain' (2020) 99 Computers & Security 102050 (arguing that a non-interactive zero-knowledge range proof protocol could erase data protection concerns).

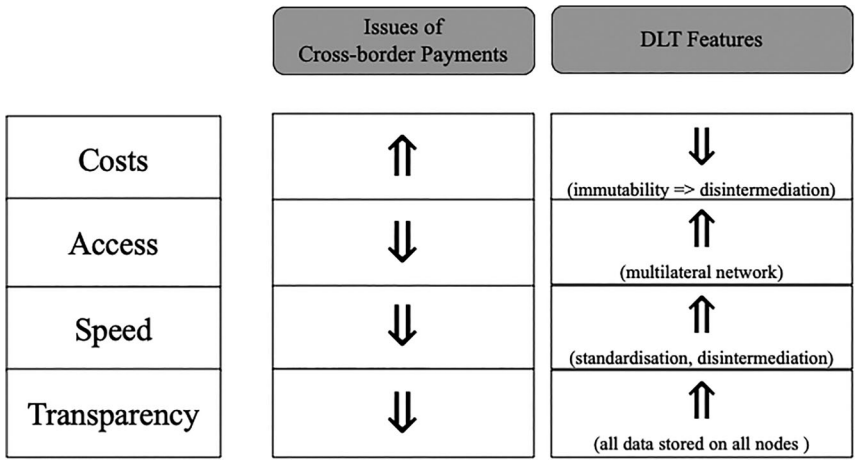

Figure 1. Issues of cross-border payments v DLT.

instance, through DLT, a payer's institution could ask all ledger participants about their terms. The institution offering the best execution as to costs, counterparty risk and settlement time would then be chosen as the counterparty. Or, given that compliance processes with anti-money laundering, counter-terrorist financing, and state sanctions determine how 'real-time' any payment can potentially be,[39] regulators[40] could become a node in the payments DLT, thereby receiving real-time access in lieu of reports, tap into the data stream for regulatory tracking, and – being technically equipped – intervene if suspicious names or transactions appear in the data stream. Of course, such applications would depend on the allocation of responsibilities, among private and public authorities (see for all DLT use cases below, under C.).

III. Challenges and risks

Despite these clear advantages, DLT is not a panacea. The use of DLT is, like any technology, subject to risks and challenges. While this is not the place to discuss the risks and challenges of DLT in general,[41] some

[39]Christophe van Cauwenberghe, 'Blockchain and Payments: Lessons Learned and Future Prospects' (*Societè Generale*) <https://www.securities-services.societegenerale.com/en/insights/expert-views/banking/blockchain-and-payments-lessons-learned-and-future-prospects>.

[40]We understand regulators to include financial services agencies, central banks, authorities in charge of enforcing AML/CTF rules and potentially law enforcement authorities.

[41]See *Zetzsche, Buckley and Arner* (n 23) 1374–86, 1391–1403; David C Donald and Mahdi H Miraz, 'Multilateral Transparency for Securities Markets Through DLT' (2020) 25 Fordham J Corp & Fin L 97; GFMA Global FX Division, 'Considerations Relevant to Initiatives and Developments in Wholesale FX Settlements' (September 2019) at 4–7 (identifying the following categories: liquidity risk, settlement risk – i.e. 'the risk that one party to a physically settled FX transaction pays out of the currency it sold

DLT-related issues also undermine its ability to enhance payment efficiency.[42] Much of the following, however, depends on *what function is distributed* (or remains with each ledger participant) in the DLT:

First, distributed ledgers are often accompanied by distributed ownership and governance;[43] in turn, organising code updates across multiple computers and engines with a plethora of different source codes and potentially divergent interests of participating institutions may become a technical, organisational and governance challenge. While these challenges are far from new to the regulators and central banks involved in streamlining their payment systems, cross-border payments often mean circumventing the jurisdictional borders of these same regulators, and by definition involve multiple regulators and central banks.

Second, DLT's increased competition feature could come with fewer revenue opportunities from the large correspondent banks as well as closed-loop systems that currently benefit from an oligopoly position; this could result in less investment in technology and compliance and thus in less efficient payments. However, new DLT-based products and services could fill the role of pacemakers in the payment services market.

Third, the distributed ledger could increase information costs if information about the ledger participants' creditworthiness and financial capabilities is not readily available; setting strict entry conditions paired with ongoing disclosure as a precondition for ledger participation could address this issue. However, the risk of errors is real. For instance, the CPMI held that 'in a possible future configuration with many automated contract tools, macroeconomic conditions could automatically trigger margin calls across [financial institutions], leading to severe liquidity demand across the financial system and creating a systemic event'.[44] Hence, data integrity and privacy can be a challenge.

Fourth, if the account itself is distributed (i.e. *if* the cash '*is on the ledger*') unless central banks guarantee its convertibility, trust will have to be vested in all actors in the network jointly; in turn the most financially capable node will effectively

but does not receive in full, when due, the currency it bought (the counter-currency) – and disruption risk, namely 'the impact of the failure of a new technology or new business model on the existing ecosystem'); *Paech* (n 12); Jonathan Rosenoer, 'Hardening the Chain: DLT and Operational Risk Management' (2018) 100 Risk Mgmt Association J 41. See also, for the evolution (*rectius*, increase) of settlement risk, as CLS and PvP share of FX turnover declined, Naveen Mallela,' Industry Initiatives on Multi-Currency, Multi-Entity Shared Ledger Infrastructure' (20 January 2021) at 3.

[42]cf *Committee on Payments and Market Infrastructures* (n 36) 17–19.

[43]While no common, predefined governance model for distributed ledgers exist, setups exploit the full range from hierarchy to non-hierarchy, including governance models that some people think are fully decentralised, i.e. controlled and influenced by no one. We examine the legal consequences of the choice of a more centralised or decentralised governance below, at D. Yet, the law requires that *someone* (either the ledger as a whole or the nodes separately) fulfils regulatory requirements, and any governance model must provide the answer as to who is responsible for doing so. For further details, see below, at E.

[44]*Committee on Payments and Market Infrastructures* (n 36) 19.

vouch for the others, potentially creating perverse incentives for the less capable ones to freeride. Unless the cash is on the ledger, synchronisation with the cash on classic accounts will be not necessarily less complex than today, as it requires strict organisation with clearing houses.[45] Also, in order to reap the benefits of DLT in a cross-border setting, any new infrastructure would need to become interoperable with existing processes and infrastructure.

Fifth, if a consensus algorithm is used to determine the purpose of the settlement, the DLT agreement may lack a strong legal basis for the exact moment when the transfer of an asset is considered final and irrevocable, as the applicable legal framework might lack a clear definition.

Further risks stem from the untested nature of DLT prompting new technology-driven operational risk, potentially triggering a new, entirely tech-based type of systemic risk.[46] Related to that, the lack of DLT-related skills and knowledge could impair the decisions of PSPs' management, PSPs' staff and the regulators.[47]

It is obvious from the challenges laid out in this section that the *architecture of* any DLT-based payment system must be carefully designed, considering both the information that can be held on the ledger and the organisation of the ledger itself.[48] We will thus lay out in the following section potential designs for specific DLT Use cases.

C. Specific DLT use cases

I. DLT as a best execution network

1. Objective

At present, the correspondent banks' point-to-point payments potentially allow for oligopolistic rents, as prices within the network rather than market forces determine payment costs.[49] DLT could be used to create competition among PSPs participating in the network by relying on the information distribution feature inherent in DLTs, similar to the order routing systems used in securities brokerage. The transparency feature of a DLT could then help to identify optimal counterparty liquidity. This process might be easier to implement in payments than in securities, since payments

[45] *van Cauwenberghe* (n 39).

[46] See Ross P Buckley and others, 'Techrisk' [2020] Singapore J Legal St 35.

[47] Marc Hamilton, 'Blockchain Distributed Ledger Technology: An Introduction and Focus on Smart Contracts' (2020) 31 J Corp Acct & Fin 7. See also Lyria Bennett Moses, 'Regulating in the Face of Sociotechnical Change' in Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (OUP 2017) section 3 (stating that 'regulators need to respond to new technologies, not because they are technological per se, but because they are *new* and law and regulation need to be changed to align with the new sociotechnical landscape, including new negative features (harms, risks, market failures, inequality, etc.) it presents.').

[48] *Committee on Payments and Market Infrastructures* (n 36) at 3 and 10.

[49] See Dirk A Zetzsche and others, 'The Case for a Best Execution Principle in Cross-border Payments' (2021) University of Luxembourg Law WPS 2021-002, UNSW Law Research Paper No. 21–45 <https://ssrn.com/abstract=3834335>.

are based on a chain of bookkeeping entries by the payer and the payee, and the transfer does not rely on a central custodian of the security to which all parties must be connected, directly or indirectly.

2. Architecture and DLT features used

Assume PSP1 located in country A wants to transfer funds to country B. PSP1 has announced an interest in engaging in a payment transfer via DLT using an announcement algorithm. Now two types of PSPs may respond (again by way of algorithms): the first group consists of PSPs with direct representation in B, interested in receiving currency A; and the second group consists of PSPs engaging in multi-aggregate transactions (e.g. PSPs in country C with links both to PSPs in A and B which are interested in swapping their position in C-currency into positions in A- and B-currency). Both the first and the second group disclose their currency transfer rates and any additional costs as well as the offered settlement time (a point in time) by way of DLT. PSP1 then accepts the offer that represents best execution. Connected via DLT, both parties can then create book positions through which cross-border payments are executed (Figure 2).

Of course, this requires a definition of what best execution in that context means. To facilitate best execution, payment regulators could change the nature of how fees may be set and allocated to clients, including by introducing a fiduciary law-style best execution principle into payments.[50]

In such a system, DLT relies on the following features, in addition to the basic elements of a payment arrangement, which include a set of instruments, procedures, and rules for transferring funds between or among participants:

- Distribution/Network function linking all PSPs together technically so that they can build up mirror account positions (nostro / vostro accounts) with little effort;
- transparency function ensuring that all nodes know where the cash is;
- immutability to ensure that bids are binding, and that failure to close may be automatically penalised; and
- these three features result in fewer compliance costs, fewer manual processes, and overall greater speed.

3. Examples

Liquidity-oriented marketplaces involving central banks are not novel, per se.[51] Also, efforts are underway to improve cross-border payments by connecting payment systems to digital identities across borders.[52] This project

[50] See ibid for additional details.

[51] For instance, the Swiss National Bank provides liquidity to market participants via a repo platform operated by Swiss infrastructure provider SIX.

[52] See, for instance, the work of the Monetary Authority of Singapore and the work of the BIS Innovation Hub, <https://www.bis.org/review/r210427c.html>. On project Dunbar, see <https://www.bis.org/about/bisih/topics/cbdc/wcbdc.htm>.

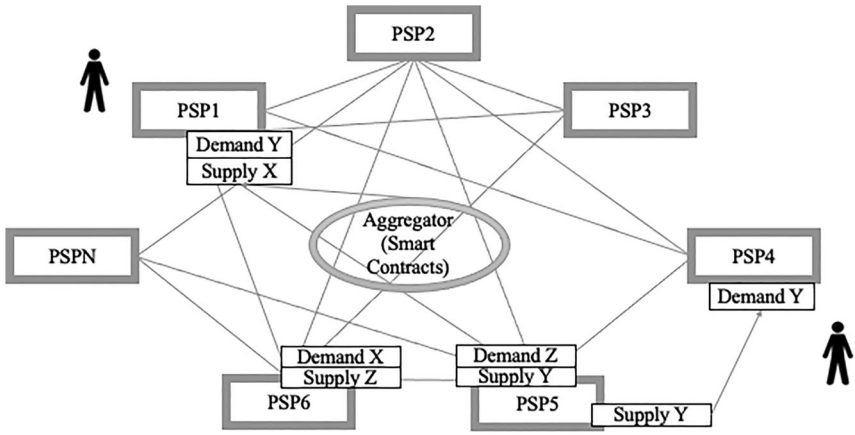

Figure 2. Best execution DLT.

could potentially implement a 'best execution' component, but in order for the Best Execution Network to operate efficiently it needs to come with amendments to payment laws in many jurisdictions.

4. Challenges

Each element of the best execution network is already available: FX aggregation software is available from various vendors (e.g. Software AG), and DLT-based marketplaces with demand and supply offers are available as a SaaS model (e.g. Google Workspace, Dropbox, Salesforce, Cisco WebEx, Concur, and GoToMeeting). The unique feature of a Best Execution DLT is DLT governance and participation.

The setting-up of a Best Execution DLT requires careful consideration as to who shall be allowed to participate in the distributed ledger as a node to prevent freeriding and reduce Herstatt risk. A ledger will function best if all participants have an interest in its proper functioning, and if the rules state that they will be held accountable if it malfunctions. Institutions with better capitalisation are targeted more easily as defendants in a lawsuit in case of malfunctions. We envision as ideal composition ledger nodes with roughly the same amount of money at risk. This can be achieved in two ways: either only institutions with roughly the same credit rating and size function as a node, or the law and regulations cut off unlimited liability for ledger participants but require a minimum capitalisation of the ledger itself.

Regardless of which route you take, setting up an appropriate governance scheme with multiple DLT nodes is a challenge. As such, we recommend seeking flexible governance approaches, similar to those used for property rights allocation in the SWIFT system. SWIFT is not DLT-based, but is rather

a multilateral network of institutions that addresses the long-term need to balance the divergent incentives of hundreds of shareholders and several thousand indirect participants from multiple countries; its governance issues are similar to those we are facing with regard to DLTs more generally.[53]

Another challenge is to convince private actors to participate in that Best Execution DLT. In this regard, we recommend introducing law and regulation to require best execution, taking into account customer interests on cost, speed and risk.[54]

II. DLT as a network of central banks

1. Objective

The Best Execution DLT use case faces the challenge that it lacks the central banks' credit and liquidity support[55] and thus entirely rests on the liquidity of FX markets. This, on a stand-alone basis, could create liquidity shortages in some currencies, or at some point in time. So, central bank involvement could be essential. However, the question that arises is how such involvement should be designed.

Where multiple central banks work on a single system, assigning exclusive jurisdiction to a central bank or oversight body (in the absence of interoperability of multiple single systems) necessarily leads to the fragmentation of DLT-based payment systems, as jurisdictions, for reasons of monetary sovereignty, will hesitate to cede oversight over their payment systems to a foreign central bank because they have a domestic mandate (usually to oversee the stability of the domestic payment system). Interoperability of multiple domestic systems may provide a solution.[56] Even so, the question remains how jurisdiction over the cross-border dimension of a DLT-based payment system can be assigned in a mutually acceptable manner.

As a solution, we envision the distributed ledger itself to be managed and operated by several central banks *mutually*, with a common rule book signed up to by all central banks and governance rights split over the participating central banks on a non-exclusive basis. Such governance rights would depend on (a) the volume of currency in a regulated country, (b) the

[53]See Raphael Auer and Rainer Boehme, 'The Technology of Retail Central Bank Digital Currency' (2020) <https://www.bis.org/publ/qtrpdf/r_qt2003j.pdf>.

[54]See *Zetzsche and others* (n 49).

[55]The central bank balance sheet is a public good; central bank money offers the unique features of settlement finality, liquidity and integrity. See CBDCs: 'an opportunity for the monetary system, BIS Annual Economic Report 2021' at III., 65, 69–72 <https://www.bis.org>.

[56]The question of interoperability has been discussed under the heading of 'mCBDC systems', see Raphael Auer and others, 'CBDCs Beyond Borders: Results from a Survey of Central Banks' (2021) BIS Paper No. 116 at graph 6 and 12 et seq. Yet, as we show in the following, a Central Bank Digital Currency is no prerequisite for running a multi-Central Bank payment system.

volume transacted to and from a given country, and (c) the number and nature of users of a payment system.

Yet some crucial decisions about a nation's currency must be retained for each central bank. Decisions reserved for the sovereign include: (1) the amount of liquidity supply in a country's currency, beyond the minimum amounts set as part of the general ledger setting, (2) monetary sanctions, and (3) which financial institutions have access to the central bank balance sheet. Meanwhile, central banks of other countries must retain sovereignty over central bank access.

2. Architecture and DLT features used

How should such a system be designed in Figure 3: rather than relying on market liquidity, participating central banks could step in as transactional intermediaries for each currency participating in the payment system. In addition, rather than linking PSPs as nodes in a ledger, central banks could function as nodes while all PSPs transact only with the distributed ledger; as such leaving them off-chain. This way, the nodes achieve the status of trusted authorities while we also support scaling (due to the monopoly of each central bank for its jurisdiction's currency and the lesser transaction costs when transacting with the nodes).

The ledger is set up in such a way that the supply and demand in each currency are split up and all demand/supply in each currency is exclusively settled by the central bank in charge of that currency. To ensure that central banks do not set exchange rates by virtue of this mechanism, they engage in internal rebalancing through their links within the ledger. If time and transaction costs were zero, the amount to be rebalanced would also be zero. However, even under the best technical conditions, it will take some time to rebalance, so there would be some FX risks. Given the immutability of the ledger, the entry and exit date record for each transaction can be computed and turned into a net FX deviation amount between the two dates [entry and exit].

This remaining FX balance is settled across the central bank network by way of FX swaps (traditional or tokenised), with the ledger algorithm creating FX Swaps or an amount of tokens equal to the net currency volatility during the transaction. If the token is issued by a smart contract in an automated manner across all central banks (including the nomination), that token constitutes a new settlement asset only acceptable by the participating central banks as part of the ledger rebalancing process. Yet it is crucial to provide for such a neutral settlement device, as all other ways would lead to rebalancing in one currency that one of the central banks may not have in the quantity needed for settlement. (Over time, however, if rebalancing amounts pile up in one way, it may be necessary to rebalance the outstanding amount by some type of asset transfer to ensure that the debt owed by one central bank does not become too high).

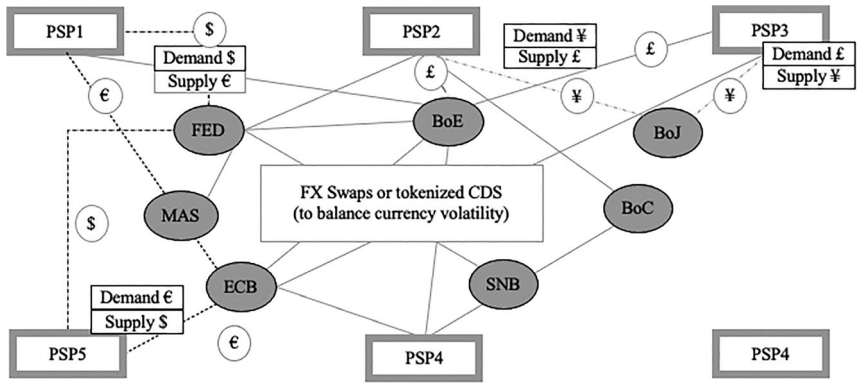

Figure 3. DLT as a network of central banks.

By relying on a safe settlement asset, the DLT Network of Central Banks benefits from a digital transfer of assets across borders – something that could not be done so easily if it was only currency that was transferred: cash-on-ledger concepts are still in their infancy, and difficult to maintain in a multi-currency framework where then different central banks would either be exposed to some other country's currency, or gain some leverage over another country's currency. Hence, a neutral settlement asset with securities and/or derivatives features allows for rebalancing where cash/money lacks transferability – for reasons of legal and monetary sovereignty.

For a Network of Central Banks, the liquidity provision in each currency remains concentrated as this is the original central bank function for each currency. But we distribute the transactional information across all ledger participants and use the network function for settlement. Trust among participating central banks and users is created by immutability and smart contracts undertaking rebalancing across the system.

3. Examples

We are aware that the core functionality, to the extent that derivatives are used instead of money, has similarities with the mCBDC bridge project and the Dunbar project that explore the potential of DLT for an international settlement arrangement involving multiple CBDCs.[57] However, to our knowledge, our DLT Network of Central Banks, with its split liquidity provision, introduces a different division of functions and a novel rebalancing mechanism. Further, the BIS Innovation Hub works on connecting central banks using DLT in an effort to create a new foundational infrastructure interlinking existing payment systems as well as creating an international

[57]See ibid at graph 6 and 12 et seq.

settlement system. Our Central Bank model pursues the second of these directions.

A working model connecting central banks using DLT could eventually be found in 'CLS NET', yet on a paid-upfront basis. While providing a settlement mechanism without counterparty risk and potentially creating new liquidity pools, CLS Net does not make use of two of the key benefits that the use of DLT could result in, which are (1) reducing FX risk between the point in time a transaction is initiated and settled, and (2) that prepayment is not necessary. Of course, if CLS Net would result in a settlement time approaching 0, the FX risk is minimal.

Further, the company Wakandi aims to connect eight African countries and their respective central banks by way of DLT.[58] At the heart stands Wakandi Core with one standard Application Interface that allows multiple formal and informal payment providers to connect by way of DLT. While connecting private entities seems to work quite effectively, it remains to be seen how the project succeeds to moderate the jurisdictional conflict among multiple central banks. As a solution, we envisage that all central banks involved in the project assign private entity Wakandi as service provider, thus each central bank retains formally the governance rights over its currency.

4. Challenges

Again, governance is a challenge when multiple central banks cooperate given that each central bank has a domestic mandate and is subject to legislative constraints. At the same time, certain central banks already have experience with deep cooperation in the field of payment systems, and experience with aligning technical aspects.

For the Network of Central Banks, we recommend the following stipulations:

(1) A DLT as a network of central banks functions best with as many functions as possible automated through smart contracts, as this type of automation addresses the issue that central banks often have very limited staff, and automation can help to ensure that a system can be run with relatively little overhead. At the same time, such an embedded RegTech approach reduces uncertainty for all participating central banks.
(2) For a network of central banks, the central banks need to agree on an arbitration mechanism *ex ante*.

Theoretically, our central bank network, if truly well-functioning, could potentially wipe out FX markets; if all or most of the liquidity flows through the network there is little room for market-based currency prices. If this

[58]See <https://www.wakandi.com/>.

were to happen, the rebalancing mechanism we propose lacks a reference point. To avoid wiping out our FX markets, the Network of Central Banks could come with a marketplace component, such as limiting prices for the respective currency, implicitly creating market prices. Further, we could foresee central banks taking a more active role in setting currency prices based on the liquidity flows they see over their system and transaction disclosures (including intra-closed loop netting) from payment systems. Yet as the establishment of the super-efficiency of the Network of Central Banks is still far away, we leave these fundamental questions regarding the function of central banks for future research.

III. DLT for AML/KYC utilities

1. Objectives

A recurring challenge in the domain of cross-border payments is the scope of KYC procedures for financial institutions and other regulated entities.

DLT could be used to reduce the risk of suspicious transactions and the identification of beneficial owners through embedded RegTech, that is automating certain contractual terms and conditions merged with legal requirements. This can be done for beneficial owner identification, where legal requirements demand the financial institution to know the ultimate beneficial owner of a transaction, and for assessments of suspicious transactions.[59]

Financial institutions' ability to assess and investigate the full route of a transaction across multiple intermediaries, which could in its entirety be classified as a suspicious transaction, is in fact limited. Assessments of ultimate beneficial owners are particularly challenging (i.e. costly) in times where links between individuals and entities are created through alternative modes of corporate control such as tailor-made derivatives, smart contracts, and private DLT platforms, respectively.[60]

2. Architecture and DLT features used

As we show in detail in Figure 4, DLT can be instrumental in addressing said challenges. For AML purposes, transactional information across all ledger participants can be shared and connected with information on beneficial owners. If all PSPs connected to the same individuals share transaction data on a common platform, transactions can be assessed from a life-cycle perspective, and not on a singular basis.

[59]See Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing [2018] OJ L156/43, Arts 30(1) and 44.

[60]Linn Anker-Sørensen, *Corporate Groups and Shadow Business Practices* (CUP forthcoming).

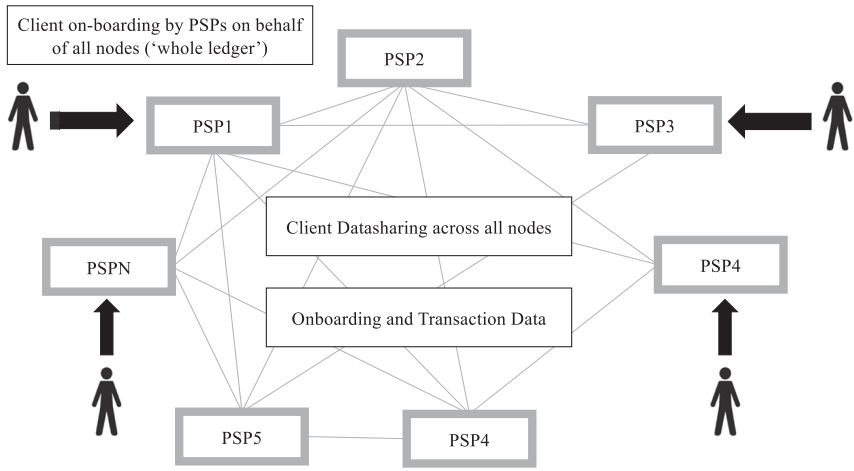

Figure 4. DLT as an AML/KYC network.

Data shared on the platform are locked and cannot be tampered with. A system-wide AML/KYC utility requires careful consideration of which data are stored on-chain and which are stored off-chain.

3. Examples

For now, most systems rely on third-party service providers to allow for in-system AML/CTF checks. Examples include the multi-currency Buna payment-platform operated by the Arab Regional Payments Clearing and Settlement Organization, a subsidiary of the Arab Monetary Fund. Buna is cooperating with Refinitiv[61] to provide comprehensive anti-money laundering compliance through World-Check Risk Intelligence, screening millions of transactions each month.[62] Compared to systems such as that, a DLT utility would directly tap into the databases of all nodes connected to it.

Deutsche Bundesbank 'Amplus' proposes – among other modules – a KYC scheme to support the automation of compliance processes in cross-border payments based on a KYC identifier and supported by a DLT infrastructure where local competent authorities would operate the nodes.[63] The proposed

[61] Refinitiv is one of the world's largest providers of financial markets data and infrastructure, serving over 40,000 institutions in approximately 190 countries. It provides leading data and insights, trading platforms, and open data and technology platforms that connect a thriving global financial markets community – driving performance in trading, investing, asset management, regulatory compliance, market data management, enterprise risk and financial crime fighting. For more information, see www.refinitiv.com.

[62] Additional information is available at <https://www.refinitiv.com/content/dam/marketing/en_us/documents/brochures/world-check-risk-intelligence-brochure.pdf>.

[63] See David Ballaschk and Marcus Härtel, 'The "Amplus" Initiative – A Modular Approach to Improving Cross-Border Payments' (2021) <https://www.bis.org/events/cpmi_ptfop/proceedings/paper6.pdf>.

governance model would allow for the inclusion of national solutions while at the same time ensuring a sufficient international minimum standard.

4. Challenges

A system-wide KYC utility faces a number of challenges.

First, the coding of smart contracts and algorithms that will connect individuals with their payments and transaction history across the ledger must take into account data privacy regulations, and other data-sharing restrictions. This could be solved by data partitioning, for instance, by virtue of zero-knowledge proofs,[64] where only parts of individuals' information are shared on the platform. Zero-knowledge proofs could provide the nodes on the platform with a green/yellow/red indicator on the risks related to the beneficial owner, thereby reducing challenges relating to data protection and cyber-attacks.[65]

Further challenges to overcome include the system risks that may lie in a centralised entity pursuing AML functions, the degree of locked information on the platform in rapidly changing identity cases, and integration into existing AML compliance systems.[66]

In order to overcome these challenges, we propose:

- Introducing a labelled risk categorisation using risk-related identifiers associated with beneficial owners in the system, based on existing KYC procedures in financial entities as nodes. An algorithm may facilitate labelling which is updated on-chain, based on new information on the client gathered by financial institutions which is stored off-chain.
- Using zero-knowledge testing in the transition of on- and off-chain information to decrease/eliminate GDPR[67] risks.

Using algorithms on the DLT platform capable of detecting alternative control modes as far as relevant for AML/KYC purposes.

IV. DLT for financial inclusion (identity tool)

By reversing the function of DLT-based client diligence, DLT could result in granting financial identities to customers who do not have them for multiple

[64] *Yang and Li* (n 38).

[65] Such categorisation resembles the country codes used today where certain codes signal the need for additional due diligence.

[66] Dirk A Zetzsche, Ross P Buckley and Douglas W Arner, 'Digital ID and AML/CDD/KYC Utilities for Financial Inclusion, Integrity and Competition' (2018) J Econ Transformation 133; Douglas W Arner and others, 'The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities' (2019) 20 Eur Bus Org L Rev 55.

[67] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1.

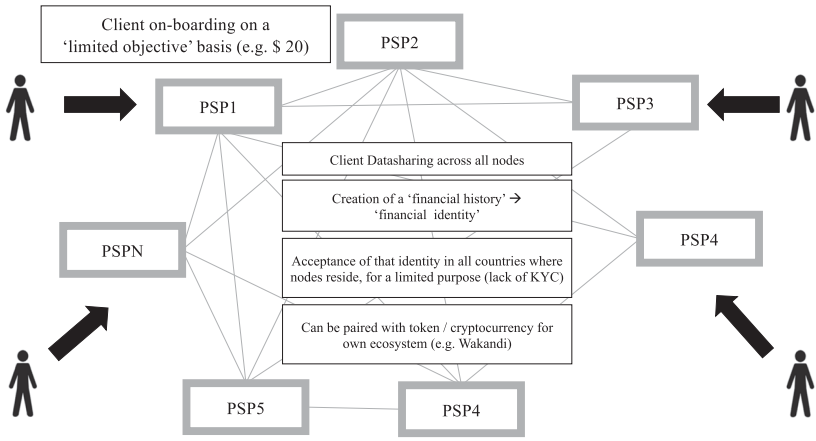

Figure 5. DLT as an identification network.

social and economic reasons. In this case, DLT could actually improve financial inclusion. We depict such a design in Figure 5.

1. Objective

Rather than defining clients by who they are based on official documents, over time an individual is identified just as securely by tracking data about what they are doing, paired with their personal features such as biometric data. DLT's inherent feature of locking in information and making it transparent continuously on the ledger may therefore provide solutions to the problem of customer identification. The data stored via DLT could be turned into a client identification tool based on the financial transactions the clients enter into paired with additional user data taken from their cell phone and e-commerce transactions.

2. Architecture

DLT as an identify tool could assign an identification number on-chain based on multiple data points linked together, thereby creating a client e-identity. After the client is identified this way, an e-ID number substitutes for the pool of data assigned to that individual which together describe the individual's activities. This e-ID number can be used in the chain for payments, banking and non-financial services and functions. The central bank could operate this network in areas of low official identity, add credit data as part of a built-in credit register and checks on the credit institution's interest rates, thereby assisting in limiting the shadow banking market.

3. Examples

While the identity-creating data collection function is at the core of many systems (including India's Aadhaar and Deutsche Bundesbank's Amplus), few payment systems make explicit use of DLT for this purpose.

One example that comes to mind is the 'UBU' project run by Global Voice which makes use of DLT-based identities within a financial ecosystem drawing on a barter system created by virtue of the virtual currency unit 'UBU'.[68] In addition, some projects that aim to financially include refugees and migrants are also DLT-based.

4. Challenges

The perennial concern regarding cyber-attacks and operational malfunctions in particular relate to DLT as an identification tool. However, the main possible promising feature of a DLT-based identity platform is that the identity is stored on an immutable platform, which makes it more difficult to manipulate the ID. However, customer due diligence without relinking 'banking IDs' to formal identity systems will render participants in such networks incapable of large financial transactions for a long time, meaning that a DLT-based identity works only as a mere starting point.

V. DLT as a messaging board for small-value systems

1. Objective

Using DLT for micropayments has been advocated for some time.[69] With regard to micropayments (to be defined), the costs related to SWIFT are high, as SWIFT charges a per-message fee; negligible for wholesale payments, but expensive for small payments if we assume there are no 'bundling banks' (i.e. correspondent banks). Further, individual assessments and accounting for large numbers of small transactions are time-consuming, as a number of assessors are required to evaluate the transactions where both the time and costs related to the valuers' function are not commensurate with the ordinary risks of small-value payments. DLT may serve as *a* means to improve efficiency, reduce costs, and, at the same time, maintain transparency and traceability of transactions. We depict the DLT design for that purpose in Figure 6.

[68] See <https://www.ventureburn.com/2019/04/ubu-startup-universal-basic-income/>.

[69] cf Alexander Bechtel and others, 'The Future of Payments in a DLT-Based European Economy: A Roadmap' (18 December 2020) <https://ssrn.com/abstract=3751204>; Volodymyr Babich and Gilles Hilary, 'Blockchain and Other Distributed Ledger Technologies in Operations' (19 November2018) <https://ssrn.com/abstract=3232977>.

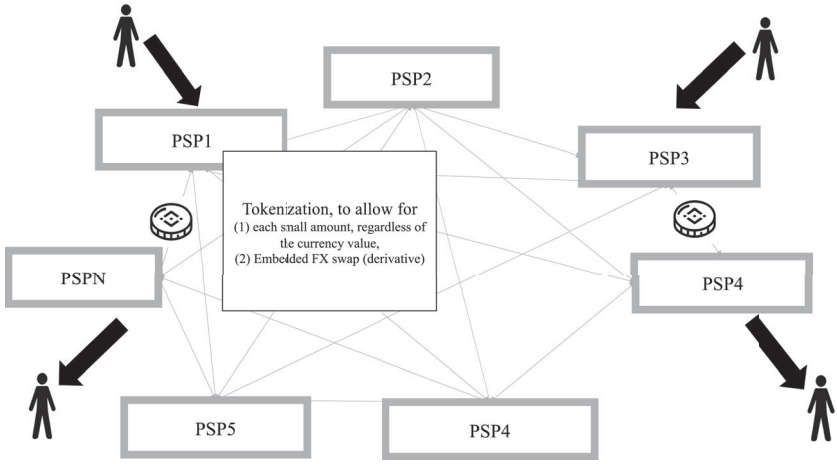

Figure 6. DLT for Small-Value Payments.

2. Architecture

A DLT platform for micropayments does not distribute any functions, but rather operates as a messaging board where network participants have access to near real-time sales or usage data.

For micropayments, DLT would be useful not only for its improved transparency and immutability, but also for its ability to automatically collect and disburse payments to participants on the platform.

3. Examples

Various providers have created platforms for micropayments. Pertinent examples include Microsoft's Ethereum-based platform for royalty payments for their Xbox gaming platform to enhance efficiency in the gaming industry. These platforms pursue their own efficiency gains alongside benefits for their network partners and participants. Microsoft's platform relies on digital contracts between Microsoft and industry participants, where the legal terms of their contractual relations are encoded in smart contracts. In addition to automated royalty payment calculations, the DLT platform provides contributors with almost real-time disclosure of digital content sold on the Xbox platform, so that each contributor can see their own royalty income derived from the sales. The time for calculations is said to decrease from 45 days to 4 min as a result, and no manual processes are necessary due to the self-executing features encoded in the smart contracts.

4. Challenges

Of course, these small payment platforms are not a panacea. On the one hand, they create lock-in effects, *de facto* replacing one silo (that of

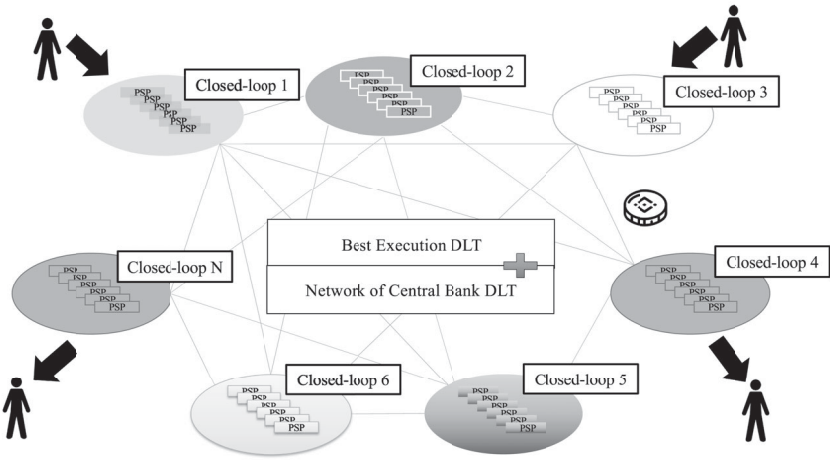

Figure 7. Interoperability DLT.

correspondent banks) with another silo (that of closed-loop systems run by unsupervised commercial entities). Further, the underlying financial risks are not addressed. Particularly noteworthy here are the FX risks on the consumer's side, as well as risks from market concentration and reliance on one entity which could be understood as a form of systemic risk.

VI. DLT as an interoperability network of closed-loop systems

1. Objective

DLT can be instrumental to build new foundational financial infrastructure that avoids the negative effects of silos (regardless of whether that silo stems from a network of correspondent banks or closed-loop systems) while maintaining the benefits of the silos, which come from technical standardisation across countries, by providing an interoperability framework for many different closed-loop systems.

Rather than rebuilding legacy systems, DLT could provide a connector among existing closed-loop systems. Further, we may understand the technical integration provided by some banking groups (such as S&L institutions in Germany and Norway) as the development of *regional* closed loops. We further expect, given the costs of creating and maintaining IT infrastructure, that more and more partially-integrated closed loops will develop over time. From this perspective, it is desirable to reach a state in which these hundreds or so of technically-integrated closed circuits (in each of which multiple PSPs participate) interact, to the benefit of the payee and the payer and the financial system and the economy at large.

2. Architecture

Such an interoperability framework could rely on the DLT use cases we have outlined above: we would propose combining the Best Execution DLT (above, at C.I.) to ensure that closed loops have all payment gateways at their disposal, with the Network of Central Bank approach (above, at C.II) being applied to ensure unlimited liquidity resulting in the design displayed in Figure 7.

The Interoperability DLT combines the DLT features of the two models and all four DLT advantages as outlined above in III.2, namely immutability to build trust, technical standardisation to achieve speed, network feature that ensures transparency, and access.[70]

3. Challenges

The challenge associated with the interoperability framework is to ensure that closed loops and correspondent banks participate. We propose relying on laws and regulations to provide incentives. To this end, regulators should require:

- 'Best execution' as part of payment laws (including rules on how to allocate infrastructure costs to payment transactions);
- Detailed pre- and post-execution disclosures to regulators;
- As part of the licensing conditions for any intermediary PSP (closed-loop operator or correspondent bank), participation as a node in the Interoperability DLT;
- As part of the licensing conditions for all PSPs (and in particular PSPs participating in a closed-loop system), a (indirect) connection to the Interoperability DLT by way of a flow-through process, so that tapping into the interoperability framework is as standardised as tapping into payment services in the closed loop.

If DLT now provides better terms with regard to cost, risk and speed than rates offered within the closed circuit or correspondent banking network, regulation would require the intermediary PSP to channel execution through the Interoperability DLT.

The Interoperability DLT faces the challenges with respect to ensuring that liquidity is actually flowing through the Interoperability DLT, at least initially; for quite some time, the closed loop will appear to operate at lower costs, as past technology investments are sunk costs in that cost calculation, while the costs of maintaining the connection to the Interoperability DLT are ongoing and high per each transaction, if few transactions are processed via the Interoperability DLT.

[70]We are so far not aware of live interoperability frameworks. However, the joint Dunbar project by the BIS Innovation Hub and the Monetary Authority of Singapore (MAS) moves towards multi-CBDC settlement, including the exploration of a wide variety of governance, implementation, and policy issues.

Thus, the involvement of central banks as providers of unrestricted liquidity is essential to the functioning of the Interoperability DLT. In addition, strict enforcement of best execution coupled with standardised disclosure to regulators who analyse the data with advanced algorithms will enhance pressure over time to comply with the best execution principle.

D. The legal challenge: the ledger or the node perspective?

How can the use cases explained above be best reflected in law? In this section, we will argue that adjusting existing laws to DLTs – which by definition are based on some degree of distribution of functions – will require, for *any single* legal, regulatory, contractual and other right and obligation, a decision as to whether the technical distribution of functions across ledgers should be acknowledged by law, that is whether the law shall adopt what we call herein '*the ledger perspective*' or whether it should retain '*the node perspective*' where the law requires each node to comply with applicable laws and regulations.[71] While this decision is crucial for any DLT-based payment system, the matter is even more pressing for the cross-border provision of payment services.

I. Introducing the ledger and node perspectives

PSPs and payment infrastructures involved in cross-border payments are subject to the legal and regulatory regimes of multiple jurisdictions. Payer and payee intermediaries must meet the different legal and regulatory requirements[72] of two or more jurisdictions.

In principle, the law and regulation of payments is contingent on the assumption that ownership, governance, accountability and responsibility for legal rights and obligations is concentrated in *one* legal entity. In turn, the law so far looks at each node separately, establishing the duties and obligations of that node; for that view (herein referred to as '*the node perspective*') the perspective of the ledger – whether it functions well as a whole, and how all the nodes interact – is derived from the individual rights and obligations of each node and is thus of secondary importance. For instance, we could understand the books of a settlement bank used by a payment system as central ledger; in this case, the node's duties and obligations can be established directly and are not derived from the individual rights and obligations

[71] We acknowledge that the multilateral regulatory approaches for regulating Financial Market Infrastructure established by the BIS/CPMI Principles for Financial Market Infrastructure seek to move in the direction of the ledger perspective, yet stop short of going 'all in': Even with regard to financial market infrastructure where regulation clearly acknowledges the need for interoperability of many entities as a system, each entity is subject to its own rules and regulations established in its home country, and can thus meet its own compliance requirements, in principle, independent of other system participants.

[72] *Financial Stability Board* (n 1) at 12.

of the payment system participants in the case of a traditional payment system. A ledger, from the node perspective, is the product of multiple entities cooperating, and the law governing such cooperation, including the rules of delegation, determines the conditions and outcomes of that cooperation.

Even when the law takes the node perspective, the ledger relationship must be considered in terms of the setup of each participant, which is no easy feat: typically, each ledger participant alone has no influence over the ledger and cannot secure its operations on a standalone basis, given that the very nature of a DLT is its distribution across various nodes. This influences the cybersecurity risk and requires modified operational resilience plans; such a plan could consider, for instance, whether the overall ledger setup and governance is robust, and whether other ledger participants are well capitalised, regulated and supervised. In addition, outsourcing rules that require the ledger participant to ensure compliance with all laws and regulations and to terminate the relationship in cases of non-compliance make little sense when the DLT is monopolistic, as capital market infrastructure often is; terminating participation is equal to getting out of service. Allocating responsibility in a DLT-based payment scheme is also becoming increasingly difficult.

Further, asking who among several participants issues a payment instrument if the instrument is issued via a DLT that is not controlled by anyone leads to challenges in the application of the law. Thus, as an alternative, financial regulation could look at the DLT as a whole. Under this contrasting concept, for *any single* rule, obligation and/or right, the node perspective is replaced by the *ledger perspective*. Under the ledger perspective, the technical distribution of functions among ledgers is acknowledged by law; the ledger perspective assigns rights and obligations to the ledger as a whole. From a legal standpoint, the ledger perspective is close to assigning entity status to the ledger, albeit – as we will show – not for all of the functions, rights and obligations that the law foresees.

The node perspective applies the law as if an individual PSP were the sole subject of a given regulation. Here, we look at the exposure, costs, and risks of each node as such. In contrast, the ledger perspective refers to a state where the whole network is subject to regulation and each participating entity is subject to regulation only as a kind of reflection through its participation in the network; in the latter case, liability is intermediated through the network and responsibility is distributed among network participants. Here, we look at the participants only to the extent that they are exposed as network participants.

Example: let us assume there are two DLT participants: A (with an AAA rating) and B (with a junk rating). The node perspective would measure counterparty risk separately, resulting in one very good rating and one very poor rating. If third-party clients are exposed to counterparty risk

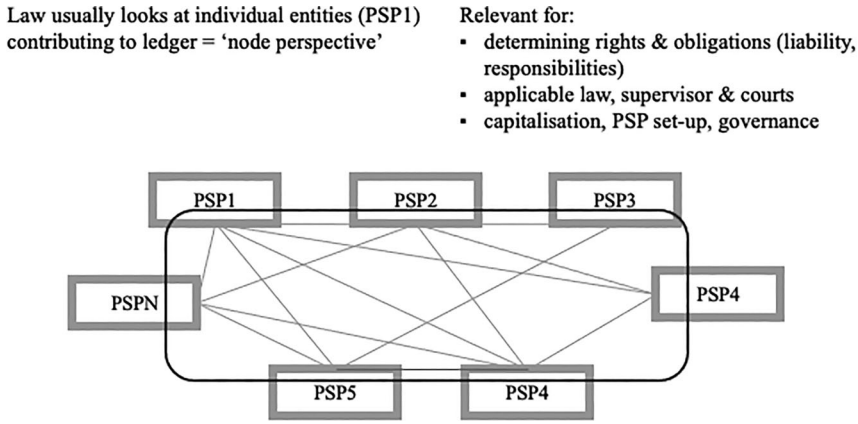

Figure 8. Legal view: ledger or node perspective?

with respect to A, they put less capital at risk than clients exposed to B. From the perspective of the ledger, the rating mix of A and B would determine the outcome. If A is much larger and much stronger than B, the result may be much closer to A's rating than to B's, and vice versa if B's exposures exceed A's capitalisation.

Given that payments are in the end a point-to-point transfer of funds from one institution to another, there is an implicit limit to the ledger perspective, i.e. the distribution of functions: any distribution of the underlying accounts would result in the socialisation of an institution's capital. In turn, only *a part* of the functions of a payment system provider can be distributed; however, which of these functions are distributed is of the utmost importance from a legal perspective.

The latter case particularly concerns DLT, as DLT relies on the cooperation of multiple nodes in order to jointly operate a DLT-based system. As we have discussed elsewhere in more detail, the result of this cooperation by virtue of DLT may be some type of joint liability for the obligations and debts incurred by being involved in the operations of the DLT.[73] In turn, for legal purposes, it is crucial to clarify which functions of a payment system are performed via the distributed ledger (with all nodes contributing to its functions) and which functions are retained by the institutions connected to the DLT and booked on their very own balance sheet (Figure 8).

To take this further, from a legal perspective the distribution of a function of financial intermediation, resulting in a kind of shared responsibility and accountability, and prompting the need for shared supervision by several regulators, is an abnormal state of affairs and is as such costly: since Aristotle's

[73]See *Zetzsche, Buckley and Arner* (n 23).

times[74] it has been well known that an asset or service owned by many is essentially owned by none; if no one is truly entitled to its proceeds no one will invest in maintaining the asset or service a state wellknown from (other) public goods and dubbed 'the tragedy of the commons'.[75] We have examined the effect of decentralisation on financial services in general elsewhere in more detail.[76] Suffice it to say here that distribution of payment functions does not improve efficiency per se, but it *could* improve efficiency *if the scope of the DLT is limited and its functions are properly designed so that the benefits of distribution outweigh the additional transaction costs it generates*.

Hence, from a legal policy perspective, what we need when adopting the ledger view is a justification as to why the ledger perspective results in an improvement in efficiency in light of the four features of DLT (data security, technical harmonisation and integration, transparency, and access under equal terms) – and where this justification is lacking, retaining the node perspective seems to be the most plausible default option in law.

As such, we see the need for regulators to analyse each individual legal stipulation and to decide whether adopting the ledger view for that function in fact increases efficiency. For this decision, the perspective of the law needs to be taken into account. This perspective differs depending on the particular area of law we are talking about; specifically, financial regulation differs from private law.

II. Why it matters: financial regulation and public law

Examples of (broadly defined) financial regulation include areas such as: licensing and authorisation, prudential supervision (including risk management, cyber security and other operational risks), financial integrity (e.g. anti-money laundering and countering the financing of terrorism and proliferation (AML/CFT)), transparency (including transaction tracking and disclosure of costs and fees), consumer protection and protection of customer funds, transaction limits, foreign exchange regulations, and the law governing the cross-border provision of services. In all these fields it matters whether we ask the ledger as such or each individual node to comply with the law, and ensure proper enforcement.

[74] As *Aristotle* said about children, and *Milton Friedman* adapted for the overall economy, 'when everybody owns something, nobody owns it, and nobody has a direct interest in maintaining or improving its condition.' See Milton and Rose Friedman, *Free to Choose – A Personal Statement* (Mariner Books 1990) 24.

[75] See, on the original concept, William Forster Lloyd, *Two Lectures on the Checks to Population* (OUP 1833). The concept became widely known after being used by Garrette Hardin, 'The Tragedy of the Commons' (1968) 162 Science 1243.

[76] See Dirk A Zetzsche, Douglas W Arner and Ross P Buckley, 'Decentralized Finance (DeFi)' (2020) 6 J Fin Reg 172.

Other areas of public law in which adopting the ledger or node perspective is important are:

- data collection, protection and transfer rules;
- capital controls;
- sanctions regimes; and
- tax reporting requirements.

Last but not least, adopting the ledger or node perspective makes a difference particularly for enforcement purposes: should the ledger as a whole or each node be fined for cases of non-compliance, and if so under what conditions? Which directors will be disqualified by financial regulators in cases of non-compliance?

The decision between the node or ledger perspective is even more relevant in a cross-border setting. Financial regulation recognises three types of conflicts of law rules:[77]

(1) *Incompatibility*: country A prohibits conduct that is permitted in country B. This configuration incurs the greatest costs for intermediaries, as they need to devise alternative solutions, typically involving separate legal entities licensed in different jurisdictions and connected by a contract;
(2) *Restricted eligibility*: country A establishes additional requirements that may or may not be compatible with the institution's setup and business model in country B. This setup requires an additional layer of law/regulation and oversight/enforcement in A that comes with additional costs;
(3) *Eligibility subject to mutual recognition*, which is usually based on a substituted compliance/equivalence test: country A recognises that the law/regulation and supervision/enforcement in country B is, in substance, equivalent to and as effectively enforced as in country A.

Against this background, it becomes important which regulator holds jurisdiction over conduct. Financial law has several ways to connect the jurisdiction of a regulator. One category often used for prudential regulation, the organisation of financial institutions and standard compliance requirements is the headquarters and/or registered office of the financial institution. Distribution rules often ask where the institution offers or markets its services, while a third category asks where the effects of an institution's actions are felt. The focus on effects is the consequence of so-called risk-based regulation, which asks where risks are likely to materialise; the latter category can be found for example in market abuse, data protection and AML/CTF rules, systemic risk oversight, but also in state sanctions laws.

[77] See Eddy Wymeersch, 'Challenging the Prudential Supervisor: Liability Versus (Regulatory) Immunity' (February 2003) <http://www.law.ugent.be/fli/wps/pdf/WP2003-03.pdf>. See also, in the context of Brexit, Matthias Lehmann and Dirk A Zetzsche, 'Brexit and the Consequences for Commercial and Financial Relations Between the EU and the UK' (2016) 27 Eur Bus L Rev 999 at II.A.

In turn, a payment institution can be subject to the financial regulation of several different countries at the same time: the laws of the country's headquarters for prudential regulation and operational requirements, the laws of the countries where it offers payment services (if only as a correspondent bank), and the laws of all those jurisdictions whose (a) citizens' data are stored, and (b) currencies are booked in a payment institution's account.

Since violations typically result in (severe) penalties, any payment institution's legal counsel must evaluate its potential involvement with each new country. The PSP's compliance organisation must organise and process on a steady basis the data on sanctions, black-listed individuals and firms. Further, the PSP's data systems must link to the reporting interfaces of each national regulator to which it is bound to report.

III. Private law

The node or ledger perspective also matters for private law. In particular, who is the party to the payment services contract? Each node or the ledger as such? Who is the proper defendant in a lawsuit with customers? Who is liable for damages? If we take the ledger perspective: what are the conditions for piercing the 'veil of the ledger' (i.e. applying a 'look-through' perspective)? The question of governance is pertinent here: who is in charge, who has voting rights, and who can make decisions about ledger operations and technological revamps/updates?

Again, the ledger or node perspective are important legal determinants in a cross-border setting. Meanwhile, private law includes contracts, property and tort relationships between private actors (i.e. payment institutions and their clients), and also intra-corporate matters such as legal relationships between DLT nodes. However, we provide herein examples only on conflict of law rules for contracts. As a matter of principle, entities involved in wholesale business (such as a PSP's relationships with other PSPs) can choose in many cases the jurisdiction whose laws shall apply and which courts shall be responsible for deciding whether one institution owes the other damages from breaches of a contract between them.[78] However, some mandatory public law rules of a jurisdiction require recognition even if the private law is otherwise freely chosen. In addition, there are certain fundamental principles of private law (called *ordre public*) that always require recognition. In contrast, when it comes to retail clients and consumers, in principle, the mandatory consumer protection law of one country applies as a minimum standard even if the law and courts of another country govern the legal matter; in some cases, to protect consumers, the choice of law and courts is even void.

[78]cf John HC Morris (ed), *The Conflicts of Laws* (6th edn, Sweet & Maxwell 2005), chapters 1–5; Peter Hay, *Conflict of Laws* (6th edn, West 2018); Arian Briggs (ed), *The Conflict of Laws* (Clarendon 2019).

In turn, payment institutions among themselves can be subject to the law and courts of one jurisdiction (A) while the law applicable to their relations with their customers is subject to the law and courts of another jurisdiction (B). If the jurisdiction of country A is inconsistent with the jurisdiction of country B, no adjudicating body will address the gap. For instance, if the law of country A in charge of an inter-bank relationship awards the payee institution damages for the payer's revocation of a payment order (after a certain time limit), but the law of country B in charge of the relationship between the payment institution and the payer does not grant the same claim in the PSP's relationship to its client, the payment institution in B needs to internalise the damages (i.e. by paying them out of their own pocket). Add to that the fact that it is often uncertain *ex ante* whether or not the law in country B will grant damage claims. Both the damage itself and the costs of assessing legal risk (legal advice) will end up as 'costs' of a cross-border payment system.

Where the mandatory legal background is harmonised, on a public and private law level, standardised agreements may achieve essentially the same results and thus could reduce costs; in the absence of mandatory law harmonisation, however, even if the contract wording is similar, the outcome may diverge. This is particularly true with regard to DLTs where the legal environment in many countries is still, in many respects, uncertain.[79]

IV. Use of DLT as a risk-increasing feature of payment systems

Against this background, it is easy to understand why DLT 'can increase legal risks'[80] in an environment where it is difficult to identify the applicable jurisdiction or relevant laws. While according to the former in most cases the law assigns exclusive jurisdiction with regard to one rule to *one* country, two difficulties remain: first, the economic actors to whom the law applies come from different jurisdictions; second, in different fields of law, conflicts of law rules may allocate jurisdictions differently – most notably, it may be that the law of one country applies to contracts, that of another to torts, and the law of a third country to matters of financial regulation (including payments regulation, data protection and AML/CTF rules). In turn, we may see the private law of countries A and B simultaneously applying at the same time that the public law of country C regulates certain aspects of a transaction.

The former does not present a particularly complicated scenario, but rather the *ordinary* life of a PSP involved in cross-border payments. In turn, we may understand that PSPs move out of certain smaller and less profitable

[79] *Committee on Payments and Market Infrastructure* (n 36) at 16.
[80] ibid, 16–17.

markets to reduce their costs and risks, often referred to as 'de-risking'.[81] At the same time, regulatory cooperation in a DLT-based setting is under-developed, due to the decentralised performance of services,[82] which further increases complexity.

Regional harmonisation projects that include both private and public law dimensions could provide a solution:[83] public law harmonisation resulting in substituted compliance reduces legal risks stemming from financial regulation, while private law harmonisation ensures a harmonised approach to damages for revoked or nullified transactions within a payment chain, so that PSPs do not need to internalise damages resulting from an inconsistent harmonisation of laws.[84] Yet, in reality, harmonisation is rarely achieved, and the issue remains how to achieve legal consistency across several regionally integrated regions.

Hence, in the absence of distinctive policy steps which remedy whether a given law allocates rights and obligations to either the ledger as a whole or each node, the use of DLT increases legal risks, which will reduce the attractiveness of DLT as a technology for payment systems.

E. Policy considerations (steps *de lege ferenda*)

The previous undesirable state can be improved through a clear allocation of rules applied to either the node or the ledger as a whole, and in turn a clear allocation of jurisdiction and supervisory powers based on that. At the same time, mandatory regulation limits innovation. In this section we examine how to bridge this gap.

I. Enabling an approach to financial regulation: opting for either the ledger or the node perspective

1. The plan of operations as a determinant of the ledger or node perspective

We have already shown (above, at C.) that the distributed part of a payment system can take entirely different forms and functions depending on the use case envisaged. At the same time, regulators have little experience with DLT arrangements; this is particularly true in the payments context. This makes, in principle, any rule undesirable that presupposes either compliance to be

[81] *Financial Stability Board* (n 1) at 12.
[82] *Zetzsche, Arner and Buckley* (n 76).
[83] See Douglas W Arner and others, *Building Regional Payment Systems: Towards a Single Rule Book* (forthcoming).
[84] For instance, in the case of the EU where 27 countries of different sizes are tied together under one uniform payment regulation and a payments law directive harmonizing private law, consumers and PSPs benefit from huge costs reductions and depth of cross-border services retained through the European Passport for payment institutions – the most intense form of substituted compliance.

performed by the ledger as a whole, or by each node individually. For the time being, we suggest refraining from imposing binding standards and guidelines that cement either the ledger or the node perspective for certain functions.

Rather, we recommend that financial regulations be drafted in a way that allows for the adoption of the ledger *or* node perspective with respect to each legal right and obligation, but requires that the nodes collectively, as part of the licensing process, submit a plan of operations showing whether compliance with a provision will be performed by each of the nodes separately, or by the ledger as a whole.[85]

Under this approach, applicants will be required to put in place an agreement based on private law devices (contract, corporate or partnership law, secured transactions) that establishes which entity or entities will assume responsibility for compliance with specific provisions of financial regulations. Regulators are supposed to review the plan of operations and assess whether the proposed arrangement ensures effective compliance. As a default rule (subject to the exceptions discussed below in V.3), all rights and obligations not expressly assigned to the ledger as a whole will remain the responsibility of each node separately; this default rule reflects, in principle, the doctrinal basis of existing financial regulation.

The enabling approach should, in principle, apply to all parts of payment processes subject to supervision and regulatory approval of any kind, i.e. where a review by a supervisory authority ensures that the plan of operations aims at rigorous compliance rather than the circumvention of the rules.

A provision could be formulated as follows:[86]

> Operators of DLT payment infrastructures, and in the absence of an operator of all nodes collectively, shall establish a clear and detailed plan of operations describing how they intend to carry out their services and activities, including a description of critical staff, technical aspects, the use of the DLT and information on how they carry out their functions, services and activities and how functions, services and activities are performed, including the type of DLT used and the function, responsibilities and liability of each node in that DLT.

[85]While, in principle, a plan of operations is in line with the governance agreement required by Principle 2 of the CPMI-IOSCO Principles for Financial Market Infrastructures, its content and nature may go beyond what is set out in Principle 2. cf Principle 2 of the CPMI Principles for Financial Market Infrastructures requires that '[a]n FMI should have governance arrangements that are clear and transparent, promote the safety and efficiency of the FMI, and support the stability of the broader financial system, other relevant public interest considerations, and the objectives of relevant stakeholders.'

[86]Inspired by, but modified from, Article 6 draft EU PilotR on DLT market infrastructure. See Dirk A Zetzsche and Jannik Woxholth, 'The DLT Sandbox Under the EU Pilot Regulation' (2021) University of Luxembourg Law WPS 2021-001 <http://www.ssrn.com/abstract=3833766> (highlighting that the PilotR Proposal 'foresees a regulatory sandbox approach for the European Single Market, offering firms a set of exemptions from EU financial law allowing them to test distributed ledger technologies (DLTs) in certain activities related to trading, clearing, and settlement. Besides offering room for experiment, the PilotR Proposal supports the education of EU regulators about DLTs in this context, which may come to form the basis for foundational changes to EU law').

> They shall also have up-to-date, clear and detailed publicly-available documentation on their website at all times, defining the rules under which the DLT payment infrastructure shall operate, including the agreed-upon, associated legal terms defining the rights, obligations, responsibilities and liabilities of the operator of the DLT payment infrastructure, as well as those of all nodes, members, participants, issuers of payment instruments, and/or clients using the DLT payment infrastructure. Such legal agreements shall specify the applicable law, pre-litigation dispute resolution mechanism and jurisdiction to bring an action.

2. Examples

All in all, the more the Plan of Operations deviates from the default state, the more peculiar the arrangements required, and the more rigorously the substitute arrangements need to be scrutinised by regulators. Given the tendency of regulators to prefer proven concepts, we acknowledge some pressure to adopt the default rule, yet if supervised entities provide good reasons to deviate from the default rule, they may receive permission to do so.

A few examples may demonstrate how the Plan of Operations works. *First*, the rules on the safeguarding of clients' funds shall ensure that clients' funds are isolated from PSP default risk, but also provide safety in terms of certain operational risks; for instance, safeguarding rules usually require some 'safe' investment policy on non-volatile and central bank deposits. Given that Payment DLTs take on different forms, any rule anticipating 'cash-on-ledger' would be premature. Most use cases will not require that client funds be held permanently on the ledger itself. Thus, in principle, the default rule is for nodes to meet the provisions on the safeguarding of clients' funds. However, the default rule concept also allows for a Plan of Operations that requires that all customer funds of all PSPs functioning as nodes be held in an account in the name of the DLT on behalf of all PSP nodes. Then, the Plan of Operations must also come up with additional safeguards (e.g. the omnibus account could be created as a trust account and held by one or several central banks in the name of the ledger). Further, if client funds are held on the ledger, the Plan of Operations must adjust clients' rights; for instance, in addition to a claim against their PSP (which stems from the clients' payment services contract with the PSP), the trust arrangement between the ledger and the trustee must be set up to ensure that it benefits the PSPs' customers (i.e. the payee and the payer) as third-party beneficiaries in the event of ledger (if any) and/or PSP insolvency.

Second, capitalisation and own funds requirements serve to ensure a buffer against a PSP's adverse operational and business developments, such as unexpected damage or reduced profitability for a limited period of

time. They also ensure that each PSP has some skin in the game, incentivising the PSP to maintain operations. In principle, this logic holds even if several PSPs cooperate through a DLT. However, we could imagine that the ledger itself, if provided with entity status and capital or capital substitutes (insurance), would function as a risk buffer. Thus, the default rules approach allows for innovation, depending on the function and configuration of each ledger.

Third, the PSP's own governance and conduct of business rules[87] serve to ensure proper participation of the PSP in the DLT. For instance, we would require a PSP to ensure that its management, as a whole, has the skills necessary to make qualified decisions on how to best participate in the DLT (a distributed view, in contrast, would look at whether all PSPs together meet this test). Again, the default rule approach allows a different allocation for cases in which the ledger itself usurps the function of client contact (as potentially encountered in a small-value payments DLT).

Fourth, any payments regulation must set rules and procedures to clearly define the point at which settlement is final. It has been argued that, to ensure that DLT-based payments can be integrated into the financial systems, regulators must (be amended to) ensure that DLT-based platforms qualify as 'designated systems' for the purposes of settlement finality, 'because the technical finality of transfer orders processed in a DLT environment need not match the commonly-shared legal understanding of the concept of finality'.[88] Finality of transactions processed in distributed ledger environments may be understood to be probabilistic only (rather than deterministic, as in the case of centralised ledgers), which raises concerns regarding the determination of title transfer thus giving rise to warranted reservations in terms of title transfer.[89] Further, in the absence of an identifiable entity to operate the platform, doubt emerges with regard to which entity is to guarantee (that is: who is liable for) the finality of transactions.[90]

[87] Including requirements on the fitness and properness of key staff, the requirements to act honestly, fairly and professionally with a view to the best interest of the clients, conflicts of interest rules as well as board and firm-internal governance arrangement (including lines of defence and reporting lines).

[88] See e.g. in the context of Directive 98/26/EC of the European Parliament and of the Council of 19 May 1998 on settlement finality in payment and securities settlement systems [1998] OJ L166/45 (Settlement Finality Directive, SFD), Art 2(a): Phoebus Athanassiou, 'Impact of Digital Innovation on the Processing of Electronic Payments and Contracting: An Overview of Legal Risks' (30 October 2017) at 29–30 <http://www.ssrn.com/abstract=3067222>.

[89] London Stock Exchange Group, 'Response to ESMA Discussion Paper on The Distributed Ledger Technology Applied to Securities Markets' (September 2016) at 2; see also Randy Sams, 'Bitcoin Blockchain for Distributed Clearing: A Critical Assessment' (2015) 4 Capco Institute J Fin Transformation 39, 44, 39–46, at 44; Juan A Garay, Aggelos Kiayias and Nikos Leonardos, 'The Bitcoin Backbone Protocol: Analysis and Applications' (14 August 2020) at 4–5 <http://www.eprint.iacr.org/2014/765.pdf>.

[90] See *Athanassiou* (n 88) at 29–30. For that purpose existing legislation for securities settlement mandates that a CSD or another system participant will assume responsibility for the irrevocability of

Our proposal, if adopted broadly for selected parts of financial law, would solve this problem: in the Plan of Operations, the consensus method relying on probabilistic means could be defined as the definitive one, for legal purposes. In the end, it matters most which entity may stand up for settlement finality with its balance sheet (i.e. every decision in the end is a matter of accountability). Obviously, when DLT has entity status, all nodes collectively could function as an 'entity' (more precisely; a group of enbtities) in charge of settlement for this purpose. However, even a group of entities cooperating through the DLT could provide more financial support than a centralised ledger, except for those that are better funded or the central banks themselves. The same Plan of Operations stipulating that the group (if any) assumes responsibility also needs to stipulate the legal consequences, particularly what type of responsibility is assumed; to ensure the purpose of settlement, unlimited liability is the strongest type of responsibility, of course, but separating liability could also be effective if the formula of separation and the amount are clearly defined.

3. Three accompanying rules

Such an enabling approach must be accompanied by *three rules*.

First, it must be clarified by way of law that the Plan of Operations defines not only rights and obligations, but also describes what sanctioning powers regulators have with respect to the rights and obligations laid out in the plan. That is, the ledger as a whole or the node will be sanctioned based on the responsibility assigned by the plan. This division of sanctioning power, to be effective, will need to be accepted by various regulators across boundaries. Of course, sanctioning the ledger as a whole means sanctioning the nodes that rely on it as well, in principle, so the details of the sanctioning power must be carefully considered.

Second, cases of non-compliance shall trigger a review of the Plan of Operations, with regulators entitled to request changes to that plan.

Third, a Plan of Operations approach as proposed herein works best if an entity is in charge of applying for supervisory approval (called herein the 'operator' of a DLT payment system). DLT would enable systems without an operator, as in fully distributed public ledgers such as Bitcoin. Yet, those DLT systems raise significant governance issues. Hence, we propose that in principle each DLT is required to have one operator, or a group of operators, respectively, who jointly assume responsibility for the initial filing. The law shall stipulate that in the absence of one operator fulfilling the legal filing requirements, all nodes shall be *jointly* liable for compliance with all rules

the transactions. A similar argument applies to cross-border payments with the need to determine the point in time where the accounts of the banks involved are matched and thus settled.

and regulations applicable to the DLT.[91] This will provide a strong incentive to ensure that an operator, or a group of operators, is put in place.

Over time, this approach will lead to better practice regarding certain functions that could then become the basis for default arrangements (to reduce costs) or even binding rules.

4. Technical implementation

All rules governing payment processes must be reformed to enable the plan of operations approach to ensure openness to innovation. Technically, this can be done with a piece of legislation in the general part of a regulation that overrides existing rules and regulations, clarifying that the entity addressed by the financial regulation could also be *multiple* legal entities (nodes) connected through DLT that together ensure compliance with some, or all, of the provisions as further described in a Plan of Operations and where private agreements exist that bind all nodes in the manner prescribed. Our proposal is developed further in the following sections (E.II. to E.V.).

II. Cross-border supervision and cooperation

Cross-border supervision and cooperation between payment regulators and central banks are key to ensuring effective supervision and financial system stability. DLT, as part of decentralised finance, comes with significant barriers: all established means of cooperation tend to be too slow and ineffective, while intensive forms of cooperation such as mutual recognition schemes and substituted compliance based on equivalence assessments tend to be difficult to establish politically across a wide range of jurisdictions.[92]

However, in the world of payments, and specifically for cross-border payments where cross-border cooperation is indispensable, the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMI) provide a solution. The principles require that payment regulators and supervisors should 'cooperate with each other, both domestically and internationally, as appropriate, in promoting the safety and efficiency of FMIs'.[93] Under these principles, the US Federal Reserve System has accepted primary oversight responsibility for the CLS system, in a Cooperative Oversight Arrangement with the ECB and national central banks of various countries. Within the Eurosystem, the ECB has primary responsibility for the settlement of

[91] For a similar proposal, see CPMI-IOSCO, 'Consultative Report Application of the Principles for Financial Market Infrastructures' (October 2021) at 13 et seq.
[92] *Zetzsche, Arner and Buckley* (n 76).
[93] See 'CPMI-IOSCO Principles for financial market infrastructures (PFMI)' (April 2012) at 133, Responsibility E.

euro-denominated payments by CLS, in close cooperation with other Eurosystem central banks.

The most intensive form of cross-border cooperation – the supervisory college – may also be appropriate for dealing with DLT-based payment systems. Since we require each DLT to appoint an operator, the supervisory authority responsible for the DLT operator as well as any node supervisor should participate in that college. This leaves open the question of how to determine the chair of the college. This function could be assigned based on (a) volume processed, (b) entities involved, and/or (c) settlement currency. Depending on the configuration, we could also provide for different colleges for different parties, with the authority of the DLT operator participating in all of them.

As a result of the establishment of the supervisory college, regulators need to secure the DLT's license to operate in any given country where the DLT's activities are subject to licensing, given the DLT's specific setup. This can be achieved by a rule embedded in the financial regulation of all participating countries that any license granted under this scheme by the supervisory college provides automatically for the right to perform that service in any country participating in the supervisory college under the conditions stipulated by that college.

III. Reversed default rule in certain instances

Our proposal is based on a default rule concept in which all rights and obligations not expressly assigned to the ledger as a whole will remain the responsibility of each node separately. However, in certain instances reversing the default rule, that is rendering the ledger perspective the default rule and the node perspective the contractual option (albeit subject to regulatory approval), could enhance efficiency.

1. Systemic risk prevention

Systemic risk controls seek to shed light on interconnectedness. For DLT payment systems as multilateral networks, taking a joint view on the DLT as such increases supervisory oversight and is, in principle, preferable.

Yet, there are limits to the ledger perspective: the PSP's individual operational risk (in particular, tech risk[94]) from the use of DLT must be assessed separately to incentivise the institution to invest in the best technology and staff to reduce these risks. However, if the ledger protects these types of risk, the tech risk on the node level can be disregarded for systemic risk purposes.

[94]See *Buckley and others* (n 46).

2. DLT governance

DLT governance requirements, that is the decision-making mechanism which decides the design and all changes to the DLT design,[95] make little sense if they do not find their counterparts in all participants, so the evaluation of ledger governance must be based on the ledger perspective.

3. AML/CTF

Applying AML/CTF rules to the general ledger as a whole could improve cost efficiency and reduce duplicate compliance checks. That is inherent in using the DLT as an AML/CTF Network (above, at C.III.).

The nexus of AML/CTF legislation is often a legally defined term such as 'payment service provider' or 'intermediary payment service provider'.[96] Attached to that term are multiple reporting and documentation duties, including that each PSP and intermediary PSP must add their own tracking numbers to enable transaction tracking, report suspicious transactions and establish a compliance organisation to ensure such reporting. The ledger perspective for AML/KYC purposes would allow for centralised AML/KYC checks, efficient intra-ledger processes and operations and the pooling of reporting requirements.

Beyond simplifying reporting to regulators, the ledger perspective allows for the following efficiency gains:

(1) Within closed-loop DLT systems, regulators could consider moving from front-end to back-end AML checks, since most relevant transactions stay in the system; this is true at least as long as cash transfers are limited to smaller amounts;
(2) Identification of ultimately beneficial owners could be stored and mitigated on the DLT platform, where algorithms can ensure the accuracy of the information in light of the various modes of enterprise control mechanisms being applied;
(3) Auditable data trails could enable regulators to access the entire setup of a transaction to assess whether and to what extent a specific individual or market actor fulfils compliance requirements.

[95] *Committee on Payments and Market Infrastructure* (n 36) 3.3.4, at 17.

[96] See Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds [2015] OJ L141/1, Art 3 No. 5 'payment service provider' means the categories of payment service provider referred to in Article 1(1) of Directive 2007/64/EC, natural or legal persons benefiting from a waiver pursuant to Article 26 thereof and legal persons benefiting from a waiver pursuant to Article 9 of Directive 2009/110/EC of the European Parliament and of the Council, providing transfer of funds services; No. 6 'intermediary payment service provider' means a payment service provider that is not the payment service provider of the payer or of the payee and that receives and transmits a transfer of funds on behalf of the payment service provider of the payer or of the payee or of another intermediary payment service provider.

However, the former is subject to the condition that within the distributed ledger all *relevant* data are accessible for compliance purposes; this creates potentially large pools of unwanted data. Moreover, involving the ledger for AML/CTF only makes sense if the nodes are themselves relieved of their customer due diligence duties. Hence, our proposal is to adopt the ledger perspective for that field as a reversed default setting. In such a setting, the *ledger* is the primary recipient of AML/CTF rules that rely on the various PSPs to perform client due diligence as delegates through outsourcing arrangements for the ledger. Such an arrangement would facilitate clear responsibilities and sanctions: the mandated ledger operator would be responsible and liable, and regulators would require adequate resources, capital and governance arrangements as a precondition for licensing.

However, we could envisage many intermediate arrangements, in particular 'traffic light' systems in which PSPs and intermediary PSPs rely on client due diligence performed by one node on behalf of the others. As such, the default setting allows for different arrangements, by setting up the Plan of Operations accordingly.

4. Data protection and governance

DLT rests on shared data, hence any node perspective creates costs and barriers in that regard.[97] In terms of data governance, the ledger perspective (disregarding the many nodes) would decrease costs. At the same time, DLT is particularly good at protecting against data corruption and ensuring ongoing data access. Data protection legislation imposes most obligations and responsibilities to the data controller and data processor.[98] To each of these terms is attached a number of information, documentary and compliance requirements. When many ledgers are connected, as in the case of a distributed ledger, these duties multiply if each of the nodes is subject to full GDPR compliance expectations. Adopting the ledger perspective for the data processor and data controller could simplify compliance and reduce costs.

However, data protection and privacy rules may limit the ability to save resources. For instance, at present, the EU GDPR and Australian data protection framework are reported to be among the strictest globally.[99] A DLT-

[97] See *Committee on Payments and Market Infrastructures* (n 36) 3.3.5, at 17.

[98] Pursuant to GDPR, Art 4 No. 7: 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; Pursuant to GDPR, Art 4 No. 8: 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

[99] 'Australian Entities and the EU General Data Protection Regulation (GDPR)' (8 June 2018) <https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation>. A general comparison is also available at <https://www.insights.comforte.com/12-

based payment system may therefore need to consider and accept these local standards. In essence, this may ask any DLT including the EU and Australia, to *de facto* adhere to EU and Australian data protection and privacy laws as a precondition for global reach.[100] Technology may provide a solution to this undesirable state: we discussed the option above (C.III.). of making use of a so-called 'zero-knowledge proof' for particular parts of information that are locked down in the DLT platform we refer to.

Yet, it will be difficult to implement the ledger view for data governance. In the current state of legal diversity, the lack of data-related equivalence may prompt the segregation of client data on a per-country basis; for instance, the EU does not deem the data governance of US federal laws to be equivalent to the EU's GDPR. In addition, some countries have instituted regulatory requirements for data localisation,[101] i.e. key customer data residing in a given country must be stored and processed in that country. While these data localisation rules are intended to ensure operational resilience, they also hinder, from a legal perspective, the ability to treat DLT as a single entity, ensuring the smooth flow of data across all ledger participants.

IV. Sanctions

It goes without saying that both the ledger and the node perspective come with their own incentives for financial institutions participating in the DLT; compliance must be ensured by appropriate sanctions. For legal and political reasons, agreeing on a harmonised catalogue of sanctions is a challenge, yet *some* harmonisation of sanctions is crucial, as a different level of sanctions provides incentive for regulatory arbitrage and thus undermines the effectiveness of any *legal* ordering cross-border: law is all about sanctions.

To clarify, in order for the Plan of Operations approach to function, we do not need 'full' harmonisation of sanctions, but sanctioning along certain previously agreed principles within a certain catalogue of sanctioned conduct. In the absence of such minimum harmonisation of sanctioning powers, only the node perspective works from – which means we lose enormous scale potential inherent in adopting the ledger perspective. Hence, we encourage to invest the political capital to achieve some joint approach to sanctioning.

countries-with-gdpr-like-data-privacy-laws>. cf Elizabeth Englezos, 'A New World Standard?: Why Australian Businesses Should Be Ensuring Their Compliance with the EU 'General Data Protection Regulation'' (2019) 115 Intellectual Property Forum 39.

[100]See also *Englezos* ibid; Charlie George, 'Privacy Predicaments: How the New EU General Data Protection Regulation (GDPR) Affects Australian Companies' (8 June 2018) Mondaq business briefing.

[101]See IRSG & DAC Beachcroft, How the trend towards data localisation is impacting the financial services sector (December 2020) 13–46 (providing an overview of data localisation requirements across the Globe, taking a critical perspective).

V. Private law

Our general approach, where the Plan of Operations determines whether compliance is owed by each node separately, or by the ledger as a whole, works less well with regard to private law matters. One of the reasons is that the Plan of Operations can easily adopt the perspective of the payment system, while private law must consider the perspective of each PSP participating in the system, and the relations of that PSP to its clients.

The difficulties here stem from three aspects: (i) private actors have an incentive to create liability arrangements in their favour, and thus to the detriment of third parties not subject to the contract; (ii) usually, the jurisdiction of payment regulators does not extend to private law relationships; and (iii) courts deciding on private law are not bound by regulators' approval of these schemes. At the same time, private law liability impacts the operations and setup of each PSP. Thus, private law arrangements deserve special attention.

1. Wholesale v retail clients

We propose that wholesale and retail clients be distinguished. In principle, wholesale clients can negotiate terms with their PSPs and have the means to protect their interests through a contract.

Consumer and SME clients, by contrast, do not have the negotiating power to do so. At the same time, harmonisation of consumer protection laws across countries is not yet feasible. Instead, we propose an approach in which PSPs are subject to contracting for a large number of items, and submitting these contracts for approval by the authorities. In principle, this could lead to some harmonisation by way of contract despite the divergence of national laws.[102]

2. Private international law

We have set out the difficulties in assigning applicable law and competent courts. For greater clarity, we propose that a private international law provision specific to multilateral payment systems be introduced.[103] Such a provision could subject the rights and obligations relating to a distributed ledger (the intra-ledger perspective) to the laws and courts of a country, or relating to the ledger's head office (if any) or the country stipulated in the contract underlying the ledger, addressing the respective legal uncertainties in private international law.[104]

[102]For our proposal we take inspiration from a similar approach in payment laws. See for instance PSD2, Art 52.

[103]Our proposal is inspired by Regulation (EC) No. 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6, Art 6(4)(d) and (e), providing specialised conflict of law rules for multilateral trading platforms.

[104]See Matthias Lehmann, 'Who Owns Bitcoin? Private Law Facing the Blockchain' (2019) 21 Minn JL Sci & Tech 93, 124–27.

3. Insolvency law

One field in which the law, so far, takes the node perspective is in the field of insolvency law. Insolvency proceedings are concentrated in one court proceeding. In many countries, the proceeding takes place at the debtor's 'centre of main interests'.[105] In a DLT situation, where the DLT itself assumes entity status, it can be difficult to determine the debtor's 'centre of main interests'. At the same time, insolvency laws exclude certain regulated entities subject to tailor-made resolution regimes from the 'main interest' test, particularly credit institutions and payment systems.[106] This exemption applies, however, only if the DLT itself is a licensed entity within that definition, requiring its own capitalisation, reporting and governance. In the absence of the former, the 'principal interest' test applies, creating significant legal uncertainty regarding the applicable insolvency law.

One solution to this insolvency conundrum is to assign a prudential status to the 'ledger', that is, to adopt the ledger perspective for that part of the DLT-based payment system. Our proposal above, requiring an 'operator' to be appointed for the ledger, does not got that far, but we acknowledge that as soon as 'the ledger' turns into some organisation, this may have repercussions with regard to the forum in 'the ledgers' insolvency'.

F. Conclusion

Financial law and regulation to date assume that regulated activities and functions are concentrated in a single legal entity that is responsible and accountable for operations and compliance. This regulatory paradigm is under pressure in the world of DLT-based payment systems where *some* ledgers are distributed. While the function of payments as a point-to-point transfer of funds seems to place an implicit limitation on DLT-based distribution of technical functions, DLT-based systems allow for the creation of foundational infrastructure linking existing systems rather than merely new designs on the front-end. As such, we identify the Best Execution DLT, the DLT as Network of Central Banks, the DLT as AML/KYC Utility, Identity Platform, Small Payments Platform and Interoperability Platform connecting multiple closed-loop and proprietary banking systems.

From a legal perspective, the distribution of functions in DLTs comes with new risks, and the need for additional agreements, and ongoing coordination across, and governance arrangements among the nodes. Further, in a cross-border context multiple regulators and courts in various countries (demanding compliance with their own set of rules and regular reports) will be

[105]See, for instance, Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings [2015] OJ L141/19, Art 7(1).
[106]See Regulation (EU) 2015/848, Arts 1(2) and 12.

involved. All of these must decide whether for compliance with the law and regulations they look at the DLT as a whole (herein called 'the ledger perspective') or each individual node (that is each institution participating in the DLT, herein called 'the node perspective'). Further, financial and private law must provide for allocation of risks, liability, responsibility and accountability for all legal obligations related to each function and activity.

The key decision in the legal design of DLT-based payment systems is for which rights and obligations regulators adopt the ledger perspective, and for which they adopt the node perspective. In this article, we propose what we call an enabling approach to be adopted for payment systems: ledger operators must specify in an operational plan subject to regulatory approval to which rights and obligations the ledger perspective applies; in the absence of such a stipulation, the rules apply based on the node perspective. However, for systemic risk controls, AML/CTF, data protection and governance, as well as DLT governance and, to some extent, insolvency proceedings, we propose an inverted default rule in which the ledger perspective prevails. Finally, in private law matters where we need to focus on the perspective of the PSP rather than the system as a whole, we propose that consumer customers and SMEs are protected through a standardised payment services contract.

Acknowledgement

We are grateful for funding support by the Bank for International Settlements as well as the NORFACE Joint Research programme on Democratic Governance in Turbulent Ages, co-funded by AEI, AKA, DFG, FNR and the European Commission through Horizon 2020, under the Grant Agreement No 822166.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the Bank for International Settlements through its workstream 'Enhancing cross–border payments' as well as the NORFACE Joint Research programme on Democratic Governance in Turbulent Ages, co–funded by AEI, AKA, DFG, FNR and the European Commission through Horizon 2020, under the Grant Agreement No 822166.

ORCID

Dirk A. Zetzsche http://orcid.org/0000-0003-4051-7699
Linn Anker-Sørensen http://orcid.org/0000-0003-3348-8033
Maria Lucia Passador http://orcid.org/0000-0002-1884-4979