Explainability and operational resilience in the design of central bank digital currencies: A new generation of money-laundering deterrence software

Received (in revised form): 1st May, 2024

Israel Cedillo Lazcano
Professor of Banking and IP/IT Law, and Director of Research and Graduate Studies, Universidad de las Américas Puebla, Mexico

Israel Cedillo Lazcano

***Israel Cedillo Lazcano** is Professor of Banking and IP/IT Law, and Director of Research and Graduate Studies at Universidad de las Américas Puebla. He obtained his PhD in law from the University of Edinburgh in 2021. He has worked as an intellectual property and personal data protection adviser, and has been awarded various research prizes, including the First Prize of the Fifth Edition of the Competition of Legal Monographs for Lawyers under 35 years old in 2013, sponsored by FELABAN.*

Abstract

It has been argued that technologies such as blockchain could provide financial systems and societies with a better infrastructural solution to process information and identify illegal transactions. Building on this idea, this paper argues that if payment systems are to take advantage of the properties that define distributed ledger technologies, they must build on those models that have delivered improved trust in our economies. Accordingly, the model presented in this paper is based on a universal digital ID that could be interoperable among different jurisdictions. Such a digital ID would rely on an explainable framework structured around an understanding of the role played by central banks, intellectual property rights and personal data protection in the processing of information. Understanding the interaction between these elements may be the first step towards a better understanding of the infrastructures employed to tackle illegal activities, which could in turn contribute to the successful development of the standards on which the next generation of suspicious transaction or order reports will be based.

Keywords: CBDCs, money laundering, payment systems, operational resilience, distributed ledger technologies

INTRODUCTION

It has been argued that one of the biggest operational problems facing today's financial institutions stems from a lack of proper training and technological leadership within the domain of anti-money-laundering (AML) systems.[1] Around the world, regulatory requirements have been established to tackle money laundering and combat the financing of terrorism (CFT) by obliging financial institutions to process substantial volumes of information about their customers to ensure they know more about them than just their credit cycle. Unfortunately, technologies are being deployed in their early stages and without a proper understanding of their capabilities. As a result, institutions are increasing the number of suspicious activity reports they are filing, including many for innocuous activities — a phenomenon commonly described as 'crying wolf'. Clearly, this represents a failure to realise the benefits of Big Data.[2]

In the context of potential solutions for financial infrastructure, distributed ledger technologies (DLTs) — notably blockchain — are presently attracting substantial

*Casa 26-C (Zona de Profesores)
Ex Hacienda Santa Catarina
Martir S/N,
San Andres Cholula,
Puebla,
Mexico,
C.P. 72810*

E-mail: israel.cedillo@udlap.mx

Journal of Payments Strategy & Systems
Vol. 18, No. 2 2024, pp. 179–191
© Henry Stewart Publications,
1750-1806

attention. In addition to using the blockchain technology for the creation of digital commodities, such as Bitcoin, which is not controlled by any central authority or government, we can also assess the potential of using these technologies, DLTs, in regulated decentralised applications with different characteristics under a well-defined set of rules that allow the applications to process substantial volumes of information. Consequently, instead of arguing that DLT offers an alternative to existing payment infrastructures, this paper argues that DLT could be incorporated into the current infrastructures. In this case, the proposal is to issue a new generation of 'outside monies' in the form of central bank digital currencies (CBDCs) to improve the processing of relevant stakeholder information and address the risk of criminal action.

One could claim that this argument could lead to proposals structured around the creation of financial panopticons counter to the spirit of the technology employed, particularly considering that a CBDC system could highlight the need for on-chain and/or off-chain 'digital IDs'[3] — defined by the Financial Action Task Force (FATF) as systems that use electronic means to obtain the credentials of a unique natural person in order for them to access financial services online and/or in-person.[4] Against this background, any CBDC system must present an answer to the question of how to allow some degree of informational self-determination, while still ensuring compliance with AML/CFT regulations.

THE INFORMATIONAL NATURE OF PAYMENT SYSTEMS

As seen in Article 3(3) of the Settlement Finality Directive 98/26/EC, and in cases such as *Dubai Islamic Bank PJSC v Paymentech Merchant Services Inc.*,[5] the constitution of payment systems and the processing of funds among different infrastructural stakeholders and financial institutions are controlled by governance arrangements rather than by substantive law. This means that such transactions rely on institutional efforts of self-structuration and self-regulation, and networks of contracts that have emerged from these, which set the rules of interaction based on the particular set of circumstances faced by each system.[6] Accordingly, the primary task of a CBDC is to enable data processing with as little friction as possible, particularly in a context that relies on automation. In practice, however, this is not an easy task. As shown in Figure 1, the very structure of our payment systems relies on the interoperability among different technological solutions and providers that compete in a Wallersteinian way throughout different fragmented processing chains constituted by merchants, payment gateways, acquiring banks, acquirer processors, card networks, issuing banks, issuer processors, among others, which, in turn, will be supported by their respective value chains. [7]

As one would expect, these parties must provide and maintain the appropriate technological infrastructure to handle the various actions that lie behind a single payment order. To this end, the industry has designed standards, such as ISO 20022, which provide different message sets to allow financial institutions to process information related to account switching, payments clearing and settlement, and even to transfer information to financial authorities.

From the structure of these message sets we can confirm that most payment systems 'transfer' money by sending messages that comply with these standards, as observed by Staughton J in *Libyan Arab Foreign Bank v Bankers Trust Co*,[8] who argued that the word 'transfer' could be considered misleading, possibly even an abuse of language. Consequently, the differences that we find throughout the history of payment systems lie in the technology employed to record the balances distributed among different parties,

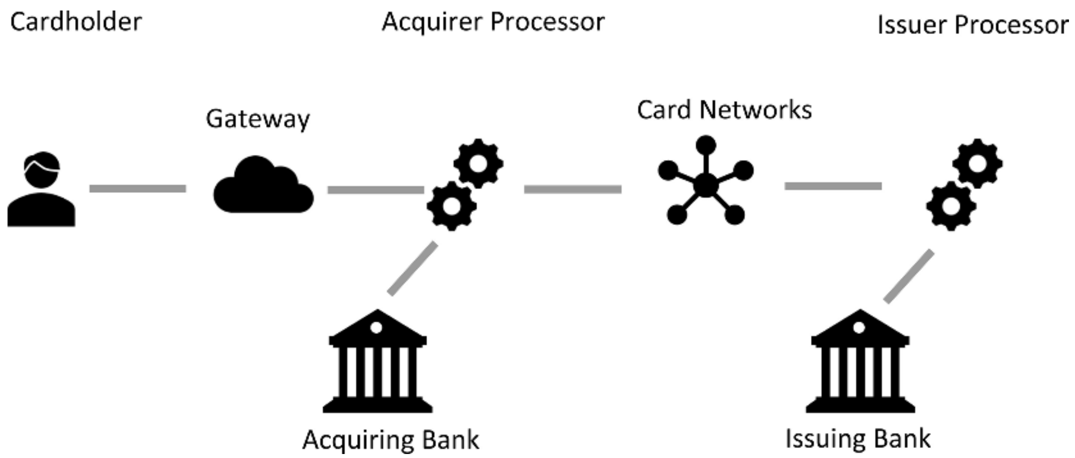

Figure 1: Payments processing chain

and one may conclude that payment systems can be understood and defined as dynamic systems designed for the processing of personal data.

Tackling money laundering

Money laundering tends to be defined as the process of making the financial proceeds of criminal activity appear legal through a process of dilution that involves the mingling of legal and illegal money through different instruments, contracts, institutions and financial infrastructures. The process is commonly associated with organised crime, such as drug trafficking, the illicit sale of arms and explosives, and terrorist activities,[9] and is vital for identifying the illegal movement of money.

Efforts to address financial crimes have been developed for many decades; however, the global focus on AML grew out of the collapse of the Bretton Woods system, as described in *Miliangos*,[10] which eased the dilution of liquidity through different currencies and markets, prompting international efforts to restrict global criminal activities in the late 1980s.

Financial crime legislation is structured around two cornerstones: (1) a strategy focused on criminalisation; and (2) a regime of reporting and regulation.[11] Unfortunately, as exemplified by the 'crying wolf' problem, the effectiveness of these measures tends to be hindered by the quality and the quantity of available data, the underdeveloped technological leadership found within the financial industry, and the state of the normative framework, which tends to be rigid and adjusted only during times of financial turmoil.

To be effective, AML/CTF laws and practices must be improved on an ongoing basis. To this end, it is now possible to employ a technology-neutral approach and implement RegTech strategies to improve data processing and, consequently, reduce the effort required to detect illegally acquired money and determine its origins.

Selecting the infrastructural design of our payment systems

There is no universal formula to explain the creation and the circulation of money: the level of decentralisation in one central bank may vary from that in another; similarly, there is nothing to prevent free-banking models from differing in their design and implementation. What is required, however, is that the stakeholders responsible for processing data within in any given infrastructure comply with regulatory requirements such as the EU General Data Protection Regulation (GDPR).

In this context, the processing of personal data is an emerging area of debate. Per Article 88 of the Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA), we must decide who will be in charge of the design and management of the processing model that will act as the cornerstone for the payment systems of the future. On the one hand, given that new payment solutions are being developed around operational smart contracts (not smart (legal) contracts), decentralised applications are looking to create a link with the sovereign nominal reference to stabilise the elements that constitute those payment systems based on 'stablecoins' as they are described in the introductory part of MiCA. Despite their apparent novelty, it is possible to draw similarities with an existing model developed by the private sector by which we can *reify* sovereign currencies and personal data, namely, the issue of banknotes within Scotland and Northern Ireland. If we read Regulation 127 of the Banking Act 2009 and the Scottish and Northern Ireland Banknote Regulations 2009, particularly Regulation 6(2), we will find that a bank that has been authorised by the Bank of England to issue notes within these jurisdictions must constitute an underlying source of liquidity through backing assets such as Bank of England banknotes, current coins of the United Kingdom and funds placed on deposit in sterling in an account held by the Bank of England. Considering these elements, it would be interesting to see if the institutions — particularly commercial banks — that act as stakeholders in some stablecoin projects could eventually obtain a licence to issue regulated cryptographic *reifiers* backed by central bank money, under a variation of the referred regulation.

On the other hand, a different and more traditional model is being considered by approximately 95 per cent of central banks in the world — one related to the development of CBDCs.[12] CBDCs are possible thanks to the analyses related to their potential to reduce the costs and risks of using them following the evolutionary approach developed by Kahn, Quinn and Roberds.[13] As illustrated in Figure 2, this means that current projects are looking for paradigms that will allow stakeholders to reduce costs — taking advantage of new paradigms like open source software — while they reduce risks like those analysed in the present work.

As an illustration of these projects, it is worth mentioning Article 4 of the regulatory proposal for the digital euro, which states that 'in accordance with the Treaties, the European Central Bank shall have the exclusive right to authorise the issue of the digital euro, and the European Central Bank and the national central banks may issue the digital euro'. This means that the referred CBDC would be a direct liability of the European Central Bank or of the national central banks, depending on the design selected.

As seen in Article 37 of the referred regulation, to transform AML regulatory reporting, users in a payment system potentially developed within a CBDC ecosystem need to be identifiable. However, as has been analysed by the FATF[14] and the Financial Stability Board (FSB),[15] the notion of privacy required to address this need is not

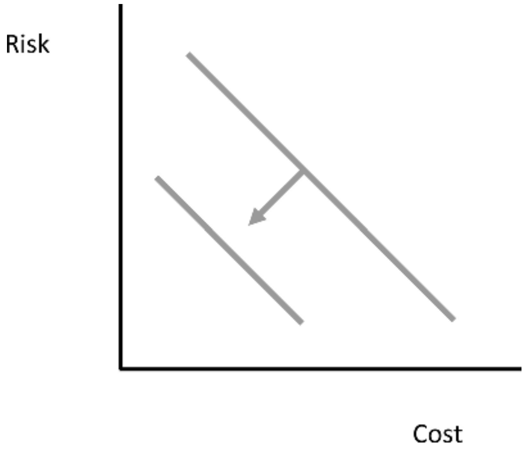

Figure 2: Payment systems evolution

consistent across the globe, and privacy preferences, policies and laws vary significantly by culture and region. Accordingly, some processing principles like collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability[16] must be considered in light of the disclosure requirements of policies aimed at combating money laundering and terrorism.[17]

Taking advantage of the rapidly decreasing cost of information storage and sorting, any data-processing strategy designed to face the challenges posed by international criminals must be segmented into four main phases, each with its own risks, namely: (1) the collection of data; (2) the analysis of said data; (3) the use or implementation of the data; and (4) the erasure and recycling of the data.[18]

Looking at Figure 3, we can see how each phase poses different potential problems for the regulatory and supervisory strategy to address, building on the principles discussed previously. When we collect personal data from data subjects, we must recognise that the imbalance of power could act as a foundation for the creation of digital panopticons, which could in turn lead to social and legal actions against the agenda of the sovereign stakeholder, thus increasing the resistance to our efforts to tackle the 'crying wolf' problem. Furthermore, this lack of understanding could lead to the introduction of technologies, such as machine learning and DLT, which could include biases where the outputs conflict with the interests of data subjects (and even of those of society) and dilute the consent throughout the processing chain among controllers and processors. Finally, in the final stages of processing, controllers and processors could forget to block and eliminate the data that are not being processed under a contractual relationship or the terms set out in AML/CFT legislation.[19]

This increased complexity and the resultant product variability pose challenges not only for regulation, but also for institutions like the FATF, the FSB and the Bank for International Settlements (BIS), which deal with the challenges posed by new instruments and technologies. Consequently, if we want to improve the monitoring of suspicious activities within our payment systems, we must pay particular attention to: (1) the selection of explainable technology, with the aim of simplifying or standardising algorithmic finance to minimise the risks that could emerge from its complexity; and

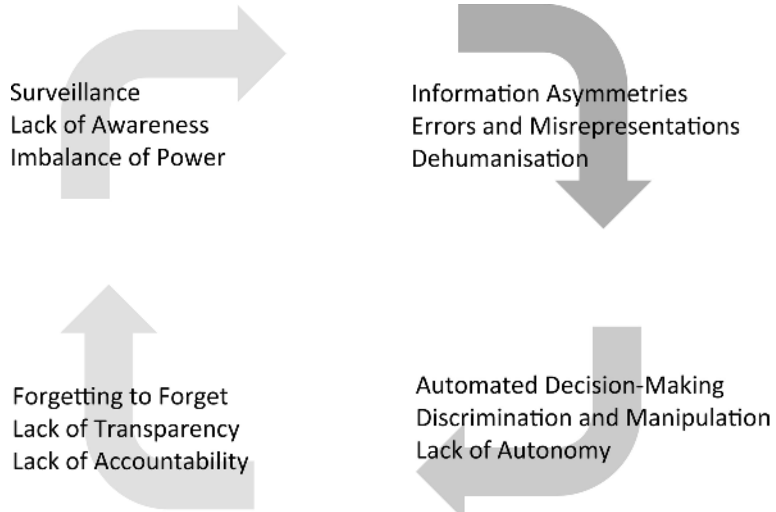

Figure 3: Risks associated with the various phases of data processing

(2) the introduction of differential privacy guarantees to reduce the risks associated with re-identification that could emerge from complex data processing chains, and to help improve the regulatory reporting developed by financial institutions.

DESIGNING EXPLAINABLE CBDCS

Documents such as 'The Riksbank's E-Krona Project',[20] 'The digital pound: A new form of money for households and businesses?',[21] and even the proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro,[22] provide a variety of analyses and proposals regarding projects based on DLT aimed at incorporating emerging technologies to improve the exercise of the *lex monetae*, and adjust it to the spirit of our time.

This should not be surprising. As was witnessed through the introduction of expert systems in our financial systems during the 1960s, using technology to foster greater transparency of internal systems can foster agreements among regulators, supervisors and regulated entities with respect to risks and metrics, as seen with the operational resilience disclosures described in the Basel III revisions published in 2017.[23] Accordingly, the introduction of CBDCs, could be considered a RegTech strategy that, in practice, would be based on a new category of money-laundering deterrence software that is being diffused around the transition towards more centralised protocols such as proof-of-authority, which may be defined as an algorithm created to deliver faster transactions through a consensus mechanism based on digital IDs, which configures the authority of the nodes.[24] Based on the evolutionary trend highlighted by these protocols, we argue that, building on the spirit of projects such as Project Aurum,[25] it is possible to design a permissioned network in which regulated institutions would act as nodes with access to our sovereign blockchain.

On this line, and considering that governments affect financial intermediation as market participants, industry competitors or benefactors of innovation, legislators and enforcers, negotiators and unwitting intervenors,[26] to issue a CBDC, we would discard any fully decentralised protocol whose source code could eventually empower a 'shadow bank' to act as the paymaster of the entire system. Accordingly, our payments system would be structured around a network of licences and transfers of economic rights under the work-for-hire doctrine, through which well-defined technology providers would deliver the source code and the rights necessary to put the respective payments system in place. These systems would work through a pipeline based on a core ledger and an API layer in which four types of nodes assigned to a single or multiple parties at the same time (participants, doormen, notaries and oracles)[27] can connect with the aim to provide services to users who would have access to a digital ID.

Building on the use cases referred above, the organisation of these nodes and infrastructures under a 'two-tier' model would not require substantial normative creation or reform. It would be based on a technology-neutral interpretation of the constitutional prerogatives and the macro prudential regulations that are currently in place to combat money laundering and terrorist financing. For instance, following the developments presented by UBS[28] and J.P. Morgan,[29] under the 'two-tier' paradigm, participant nodes could be assigned to regulated intermediaries covered by regulations like the Financial Services and Markets Act 2000 and the Banking Act 2009 to allow them to transact with each other and manage the 'off-chain' transactions developed by consumers, as verified through the execution of the pilot Phase 4 of the e-Krona.[30]

Additionally, within this category one could assign a unique issuer node to the central bank based on their constitutional mandates, or even foster the creation of free-banking models, like the one covered by the Scottish and Northern Ireland Banknote Regulations 2009, by which certain nodes could be empowered to issue new instruments structured around a sovereign unit of account,[31] as one can see with the case of PayPal USD.[32] In both cases, all these activities would be monitored by regulator nodes assigned by the state, probably to the same regulated intermediaries and/or even to those financial intelligence units described in Article 7(1) of the United Nations Convention against Transnational Organized Crime, with the aim of receiving and processing reports relating to legal and illegal transactions developed in the network by individual digital IDs. On this last point, we are going to find the relevance of the digital IDs. In traditional payment systems that run through the infrastructure of our commercial banks, the processing of data, particularly in the context of customer due diligence, is decentralised and asymmetric given that each institution conducts independent analyses of a single individual based on its own crime solution (which could be based on different paradigms like scenario-modelling approaches and inference-based approaches).[33] Before this problem, a CBDC could present an option to leverage digital IDs to improve the processing of personal data, as required by AML/CFT regulations.[34]

If we create a network that is interoperable with other networks given the characteristics provided by common infrastructural stakeholders (for instance, in most documents that support the development of CBDCs common we will find common names like CORDA), we will be able to create a more universal form of digital ID that could be recognised by different nodes in different networks. Thus, if a user wants to employ this payments system, he/she will need to present his/her information to one of these nodes, which will perform the due customer due diligence to support the issuance of the digital ID that will reflect the two tiers of the system. That ID will allow the customer to interact with different banks based on a single informational basis, while the regulated nodes will be able to identify more efficiently on the chain any suspicious interactions associated to that piece of information. In simpler terms, we will not a have a global coin, but we can have a global digital ID.

The second category of nodes would be structured around a doorman service based on the spirit of regulations, such as Chapter 2 of Part 1A of the UK Financial Services Act 2012 and Article 8 of the Mexican Credit Institutions Law, by which the central bank and/or other sovereign institution would receive, study and, if applicable, approve the addition of a new node in the network. Following the content of the same regulations, these nodes could provide certain services for the arrangement, including dispute resolution, standard-setting, regulatory reporting, and even those provided by the third category of nodes: the notary nodes. Under this paradigm, the central bank would operate a service within the network with the aim of easing the safe execution of transactions by verifying that each transaction is unique and does not represent double spending,[35] as set in Articles 28–34 and Annex 1 of the Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market, and Articles 89–98 of the Mexican Commercial Code.

Finally, considering that our network and its applications would be developed through smart contracts, it would need to incorporate regulated and non-anonymous oracle nodes; after all, despite the denomination of these agreements, they would not be complete agents able to access information found ‘off-chain’.[36] Replicating the paradigm introduced by Barclays in 1959 with the rollout of the EMIDEC 1100 computer, in which less powerful machines transferred, through communication cables, information processed by branches with the aim of supporting institutional processes,[37] our system would require mediators to provide market information related to the contract code execution, but, just as in the case of regulator nodes, they would not be in position to make changes on the ledger.[38]

Operational risk and ID monitoring

Given the current state of DLT, one might ask what happens if the algorithms involved in the development of these payment systems are suboptimally designed and/or if the persons in charge of deploying them are not properly trained. In this respect, important — and potentially systemic — stakeholders should put in place measures to certify their technological leadership and the training of the staff involved in the selection and operation of the systems to be deployed, the integrity of their premises, equipment, software, hardware, and other critical structural elements, in line with regulatory instruments, such as the FCA's REC 2.5 (Systems and Controls, Algorithmic Trading and Conflicts). This builds on the fact that criminal actors can exploit the vulnerabilities of the code, the lack of experience among staff, and the soft and hard legacy systems that currently exist throughout the industry. Consequently, we must consider that the development of a payments system similar to the one presented in this paper will require the identification of infrastructural stakeholders that will play a role in the processing of data, including the pieces of information related to criminal activity. Accordingly, one first parameter that could be considered for the creation and operation of a CBDC, can be found in the Principles for Operational Resilience issued by the BIS[39] and the Digital Operational Resilience Act (DORA) 2023.

The principles found in these documents, certainly, reflect the spirit of our context and they are relevant for, on the one hand, the optimal monitoring of activities and money flows associated with money laundering and terrorist financing, and, on the other, the protection of informational infrastructures from criminal activity and preparing them to operate under different stress scenarios. This relevance can be verified in the third consultation paper related to the draft technical standards and guidelines specifying certain requirements of MiCA on the detection and prevention of market abuse, investor protection and operational resilience, published by the European Securities and Markets Authority (ESMA). [40]

Given that payment systems (including peer-to-peer systems) rely on global value chains, we can find some interesting elements on the draft prepared by ESMA that could complement the principles described earlier and be extrapolated in the context of AML/CFT monitoring and reporting, particularly building on the model of the suspicious transactions or orders reports (STORs), which are compatible with ISO 20022. Within our financial markets, intermediaries can be identified as the main stakeholders; behind them, however, we are going to find hierarchies structured around the power held by certain companies that exercise a certain level of infrastructural control based on their ownership of intellectual property rights (IPRs) and their power to process of data, including personal data, through algorithmic black boxes.

Based on this, the principles developed by the BIS and ESMA, and found in DORA, recognise that one of the greatest challenges derived from the adoption and diffusion of technologies like DLT and artificial intelligence throughout our financial infrastructures is their lack of explainability. This increased complexity and the resultant product variability pose challenges not only for regulation, but also for those institutions that create and deal with new instruments and technologies, such as 'crypto assets'. Consequently, if we want to improve operational risk management, Principle 2 of the

BIS Principles for Operational Resilience and Article 28 of DORA could include or highlight a subprinciple based on the selection of explainable technology with the aim of simplifying or standardising algorithmic finance to minimise the risks (including those related to criminal activity) that could emerge from its complexity, while we put in place effective and ongoing monitoring of the operation of the technology.

One of the normative elements that could emerge from this subprinciple could be an integral part of a constitutive charter by which the incorporation of certain explainable applications would require financial institutions to be licensed to do so.[41] Of course, those applications that could not comply under well-defined explainability requirements — particularly during their stay in a regulatory sandbox — should be banned from their incorporation within our financial infrastructures, including our payment systems, unless reasonable explanation for their operation is presented.[42]

To support this effort, and the gradual materialisation of new STORs, it is possible to argue that Principles 4 and 5 of the BIS Principles for Operational Resilience, and Articles 28 and 29 of DORA are very relevant to: (1) identify the stakeholders involved; and (2) set the agreements by which intermediaries will have to answer for the failures of their systems and the flow of information that runs throughout them. In other words, independently of the existence of the networks of stakeholders and agreements, intermediaries must have the control of their infrastructures. Consequently, this argument presents a complementary proposal to identify the relevance of the stakeholders and refine the requirements set for the agreements referred within the referred instruments.

Selected infrastructure

Figure 4 illustrates the interaction between multiple stakeholders within a single technology infrastructure covered by three regulatory areas (intellectual property law, personal data protection and AML/CFT). This may be useful for materialising the mapping described in DORA Articles 28 and 29 and for the development of a more appropriate STOR regime. On the first level are the intellectual property rights holders, to include primary owners (particularly in the context of work-for-hire) and third-party providers. Within this level, we must identify/separate: (1) the owners of moral and economic rights related to copyright elements such as software; and (2) the owners of the intellectual property rights related to the inventions and innovations protected by patents, utility models, and other figures that support the technology in question. With the exception of those intermediaries that develop and control their own infrastructures, we must verify that financial intermediaries have the rights that will allow them to control the selected infrastructures, particularly if they rely on smart applications, such as DevOps, to develop their in-house products and services.

At the second level are the controllers and processors of personal data, who may be identified via the chain of IPR transfers. For instance, a financial institution that acquires a licence to use the components of a technological infrastructure to process personal data for the purposes of customer due diligence will be considered the controller for the purposes of regulations such as the GDPR. At the same time, if the infrastructure in question is supported/controlled by a third party, this latter party would be considered as a processor.

So, how does this paradigm help to address the ‘crying wolf’ problem? First, where a blockchain controlled by a central bank is interoperable with similar sovereign blockchains, users, banks and authorities can benefit from a universal digital ID, thus facilitating and standardising know-your-customer checks and compliance with

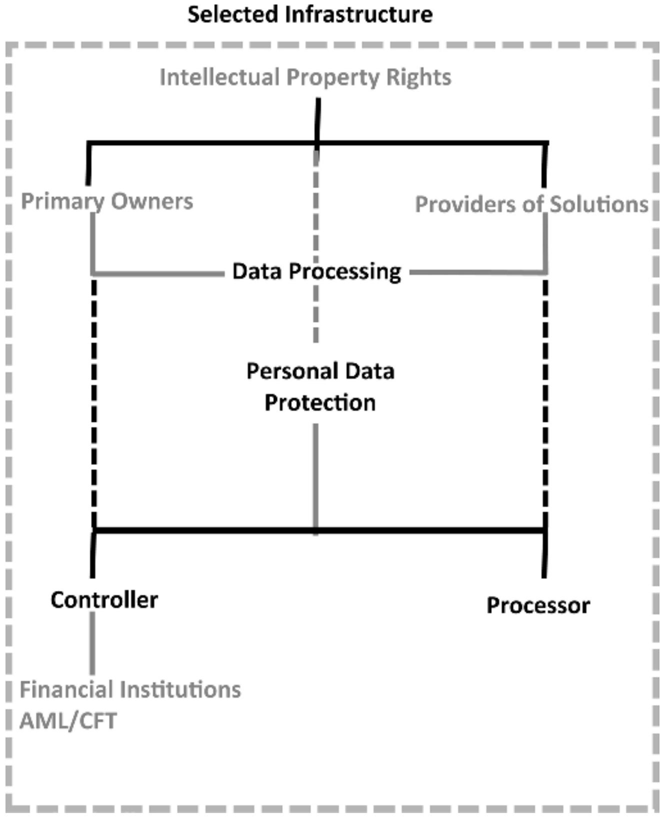

Figure 4: Interaction between infrastructural stakeholders exercising their Intellectual Property Rights (IPRs) and the controllers and processors of data

AML regulations. Secondly, the transparency and the standardisation that define this paradigm will allow us to go beyond the simple arguments related to the anonymisation of data. This means that, to address some concerns related to the re-identification of users, under the standards needed for the deployment of our CBDCs, we can design and implement a model of differential privacy[43] that could allow us, on the one hand, to assemble large datasets to train a new generation of smart applications for identifying suspicious patterns, while, on the other, we introduce a new set of practices related to the addition of 'noise'.

In other words, as seen in Figure 5, in a differential privacy model we could set different privacy parameters based on the characteristics of certain behaviours. For instance, the system would add more noise to those transactions that would be labelled as 'low-value' and 'low-risk', reducing the accuracy of the information. However, if the transactions are considered suspicious, the noise added would be minimal and it would allow us to identify concrete nodes in the system that could be of interest for authorities. At the same time, the parameters employed to create these differentials, could be useful for the design of our STORs, building on the cornerstones established by ISO 20022 and institutions like ESMA.

CONCLUSION

As this work has discussed, if we are to address the informational challenges that result in the 'crying wolf' problem, we must first understand the infrastructure employed and count with properly-trained staff capable

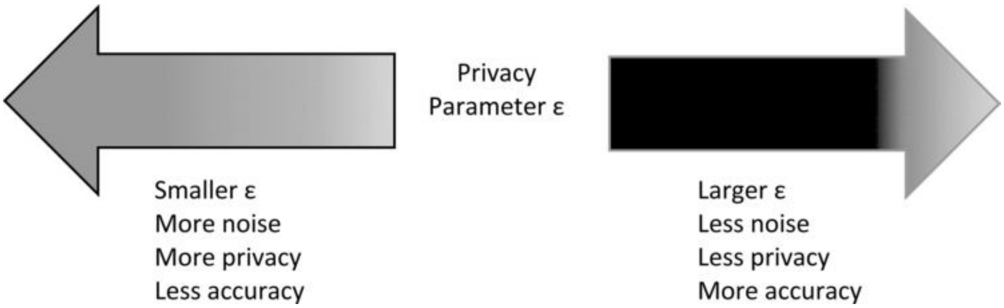

Figure 5: Impact of the privacy parameter ε: the privacy-utility trade-off

of employing the new infrastructures to process the data in an optimal way. To this end, this paper has presented a proposal that builds on a paradigm structured around the incorporation of DLT in our regulated financial systems, specifically, in the form of CBDCs with the aim of developing a new category of money-laundering deterrence software.

One might argue that DLT is not the only potential solution to address this informational problem. Nevertheless, it benefits from certain traits that could be used to facilitate our efforts to tackle money laundering and terrorist financing. First, it offers a transparent solution that allows us to identify in the ledger the interactions between different nodes and their respective characteristics. Secondly, the existence of few relevant infrastructural stakeholders eases the creation of standards that will help us to develop uniform requirements for the design of STORs and to create a universal form of digital ID. Thirdly, as with any other technology, DLT does not exist in isolation. To fulfil its potential, it must work as an integral part of more complex dynamic systems in which DLT will be complemented with machine learning, which in turn, will be trained on the patterns generated by the networks supporting the existence of our CBDCs to identify suspicious transactions. At the same time, it will help us protect privacy through the inclusion of differential privacy models.

Finally, considering that money laundering and terrorist financing must be included as integral elements of our macro prudential regulations, the constitutive elements of our payment systems must be analysed from an operational perspective, recognising the relevance of IPRs and personal data protection on the design of the framework for our payment systems. Accordingly, CBDC systems will have to comply with different governance paradigms and international standards, such as the NIST framework, ISO 20022 and the CPMI-IOSCO guidance for cyber resilience of financial market infrastructures, and learn from institutions such as ESMA about safeguards to prevent market abuses in the cryptoassets market. These standards could ease the transfer of knowledge and improve best practices by helping embed a common understanding of concepts, terms and definitions to help prevent errors like those associated with the 'crying wolf' problem.[44]

References

(1) Jensen, R. I. T. and Iosifidis, A. (2023) 'Qualifying and raising anti-money laundering alarms with deep learning', *Expert Systems with Applications*, Vol. 214, pp. 1–12.

(2) Takáts, E. (2011) 'A theory of "crying wolf": The economics of money laundering enforcement', *Journal of Law, Economics & Organization*, Vol. 27, No. 1, pp. 32–78.

(3) Sullivan, C. (2011) 'Introduction', in: *Digital Identity*, University of Adelaide, South Australia, pp. 5–17.

(4) Financial Action Task Force (2020) 'Digital Identity', available at: https://www.fatf-gafi.org/

content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity.pdf.coredownload.pdf (accessed 24th October, 2023).

(5) [2001] 1 Lloyd's Rep. 65 (UK), at 517-8.

(6) Cranston, R., Avgouleas, E., Zwieten, K., Hare, C. van and Sante, T. van (2017) *Principles of Banking Law*, Oxford University Press, Oxford.

(7) Ching, J. (2020) 'Credit Card Payments Processing 101', Medium, available at: https://chingjon.medium.com/credit-card-payments-processing-101-f90f3b843a41 (accessed 19th March, 2024).

(8) [1989] Q.B. 728 (UK), at 750.

(9) Satapathy, C. (2003) 'Money laundering: New moves to combat terrorism', *Economic and Political Weekly*, Vol. 38, No. 7, pp. 599–602.

(10) [1976] A.C. 443 (UK), at 460–70.

(11) Alldridge, P. (2008) 'Money laundering and globalization', *Journal of Law and Society*, Vol. 35, No. 4, pp. 437–463.

(12) Bank for International Settlements (2023) 'Making Headway — Results of the 2022 BIS Survey on Central Bank Digital Currencies and Crypto', available at: https://www.bis.org/publ/bppdf/bispap136.pdf (accessed 10th July, 2023).

(13) Kahn, C., Quinn, S. and Roberds, W. (2014) 'Central Banks and Payment Systems: The Evolving Trade-off between Cost and Risk', Norges Bank, available at: https://www.norges-bank.no/contentassets/3fba8b3a3432407d929ae9218db1ffc4/10_kahn_quinn_roberds2014.pdf (accessed 1st June, 2023).

(14) FATF, see ref. 4 above.

(15) Financial Stability Board (2023) 'Stocktake of International Data Standards Relevant to Cross-Border Payments', available at: https://www.fsb.org/wp-content/uploads/P250923.pdf (accessed 27th October, 2023).

(16) World Economic Forum (2019) 'The Global Risks Report 2019', available at: https://www.weforum.org/reports/the-global-risks-report-2019 (accessed 2nd April, 2019).

(17) Hildebrandt, M. (2015) 'The fundamental right of data protection', in: *Smart Technologies and the End(s) of Law*, Edward Elgar Publishing, Cheltenham, pp. 186–213.

(18) Tamò-Larrieux, A. (2018) 'Setting the Stage', in: *Designing for Privacy and its Legal Framework. Data Protection by Design and Default for the Internet of Things*, Springer Nature, Cham, pp. 1–17.

(19) Tamò-Larrieux, see ref. 34 above.

(20) Sveriges Riksbank (2017) 'The Riksbank's E-Krona Project. Report 1', available at: https://www.riksbank.se/globalassets/media/rapporter/e-krona/2017/rapport_ekrona_uppdaterad_170920_eng.pdf (accessed 7th December 2018).

(21) Bank of England (2024) 'Response to the Bank of England and HM Treasury Consultation Paper − The digital pound: A new form of money for households and businesses?', available at: https://www.bankofengland.co.uk/paper/2024/responses-to-the-digital-pound-consultation-paper?sf185838246=1 (accessed 25th January, 2024).

(22) European Commission (2023) 'A proposal for a Regulation of the European Parliament and of the Council on the Establishment of the Digital Euro', available at: https://finance.ec.europa.eu/system/files/2023-06/230628-proposal-digital-euro-regulation_en.pdf (accessed 5th July, 2023).

(23) Bank for International Settlements (2017) 'Basel III: Finalising Post-Crisis Reforms', available at: https://www.bis.org/bcbs/publ/d424.pdf (accessed 21st April, 2017).

(24) Kozak, T. (2018) 'Consensus protocols that serve different business needs. Part II', Intellect Soft, available at: https://blockchain.intellectsoft.net/blog/consensus-protocols-that-serve-different-business-needs-part-2/#Proof-of-Authority (accessed 29th April, 2019).

(25) Bank for International Settlements (2022) 'Project Aurum: A Prototype for Two-Tier Central Bank Digital Currency (CBDC)', available at: https://www.bis.org/publ/othp57.htm (accessed 10th July, 2023).

(26) McMyn, A. and Sim, M. (2017) 'Networks in Trade Finance: Balancing the Options', R3, available at: https://www.r3.com/wp-content/uploads/2018/04/Networks-in-trade-finance.pdf (accessed 17th November, 2018).

(27) Bank of England (2023) 'The digital pound: Technology Working Paper', available at: https://www.bankofengland.co.uk/paper/2023/the-digital-pound-technology-working-paper (accessed 12th July, 2023).

(28) Noonan, L. (June 2019) 'Top banks push ahead with digital coins for 2020', *Financial Times*, available at: https://www.ft.com/content/9fd8e8ea-83e5-11e9-b592-5fe435b57a3b (accessed 3rd June, 2019).

(29) Son, H. (2019) 'JP Morgan Is Rolling out the First US Bank-Backed Cryptocurrency to Transform Payment Business', CNBC, available at: https://www.cnbc.com/2019/02/13/jp-morgan-is-rolling-out-the-first-us-bank-backed-cryptocurrency-to-transform-payments--.html (accessed 15th February, 2019).

(30) Riksbank (2024) 'The e-krona pilot phase 4: Offline payments with e-krona', available at: https://www.riksbank.se/en-gb/press-and-published/notices-and-press-releases/notices/2024/the-e-krona-pilot-phase-4-offline-payments-with-e-krona/ (accessed 27th March, 2024).

(31) Bank for International Settlements (2017) 'Distributed Ledger Technology in Payment, Clearing and Settlement. An Analytical Framework', available at: https://www.bis.org/cpmi/publ/d157.pdf (accessed 1st April, 2018).

(32) Asgari, N. (August 2023) 'PayPal pushes deeper

into crypto payments with stablecoin launch', *Financial Times*, available at: https://www.ft.com/content/fd072b20-f9c7-4e2b-b274-b2f13cbeae07 (accessed 26th March, 2024).

(33) Cox, D. (2014) 'Money-laundering deterrence software', in: *Handbook of Anti-Money Laundering*, Wiley, Chichester, pp. 277–284.

(34) Mahari, R. Z., Hardjono, T. and Pentland, A. (2022) 'AML by design: Designing a central bank digital currency to stifle money laundering', *MIT Science Policy Review*, Vol. 3, pp. 57–65.

(35) Bank for International Settlements, see ref. 31 above; McMyn and Sim, see ref. 26 above.

(36) Bank for International Settlements (2023) 'The crypto ecosystem: Key elements and risks', available at: https://www.bis.org/publ/othp72.htm (accessed 12th July, 2023).

(37) Sweetman, A. (2022) 'The London Clearing Banks and Computer Security: 1960-1977', in: *Cyber and the City. Securing London's Banks in the Computer Age*, Springer Nature, Cham, pp. 25–65.

(38) McMyn and Sim, see ref. 26 above.

(39) Bank for International Settlements (2021) 'Principles for Operational Resilience', available at: https://www.bis.org/bcbs/publ/d516.htm (accessed 6th June, 2021).

(40) European Securities and Markets Authority (2024) 'Draft technical standards and guidelines specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA) on detection and prevention of market abuse, investor protection and operational resilience — third consultation paper', available at: https://www.esma.europa.eu/sites/default/files/2024-03/ESMA75-453128700-1002_MiCA_Consultation_Paper_-_RTS_market_abuse_and_GLs_on_investor_protection_and_operational_resilience.pdf (accessed 29th March, 2024).

(41) Kahana, E. (2020) 'Quantum Computing and AI Algorithmic Bias', Stanford Law School (SLS), available at: https://law.stanford.edu/2020/02/06/quantum-computing-and-algorithmic-bias/ (accessed 7th February, 2020).

(42) Schemmel, J. (2020) 'Artificial Intelligence and the Financial Markets: Markets as Usual?' in Wischmeyer, T. and Rademacher, T. (eds) *Regulating Artificial Intelligence*, Springer Nature, Cham, pp. 255–276.

(43) National Institute of Standards and Technology (2023) 'Guidelines for Evaluating Differential Privacy Guarantees', available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-226.ipd.pdf (accessed 10th January, 2024).

(44) Peng, S. (2018) 'Cybersecurity standards. cyberspace governance, multistakeholderism and the (ir)relevance of the TBT regime', *Cornell International Law Journal*, Vol. 51, No. 2, pp. 445–469.

Copyright of Journal of Payments Strategy & Systems is the property of Henry Stewart Publications LLP and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.