

TOWARDS DIGITAL MONEY INTEROPERABILITY: DATA GOVERNANCE COORDINATION FOR CROSS-BORDER PAYMENTS

*Shuping Li**

ABSTRACT

Digital money interoperability will facilitate cross-border payment and capital flow, benefiting money users, but data protection concerns the regulator. Information matters for all aspects of digital money: guaranteeing payment security, finality, supervising capital flow, and establishing users' credit profiles for risk management. Due to the states' concerns about data sovereignty and data as a valuable economic resource, payment institutions' market profits, and users' privacy protection, cross-border data sharing is often impeded. Based on the political will and economic benefits of cooperation, countries may adopt multilateral or bilateral legal frameworks for data sharing. Specific data governance measures include, data classification and grading, data access, collection, processing, and erasure by the system operator, and data portability by the user, subject to operational and regulatory requirements. Legal and technical arrangements are equally important to facilitate data sharing by embedding conditional data layer interoperability in the digital infrastructure.

* Ph.D. candidate in Law from the University of Hong Kong. L.L.M. from Columbia Law School. L.L.M from the University of Cambridge. L.L.B. from Shandong University.

Keywords:

cross-border payment, data governance, data sharing, digital money, interoperability, regulation by design.

ABSTRACT	107
INTRODUCTION	109
II. DIGITAL MONEY INTEROPERABILITY AND DATA SHARING....	112
A. <i>Data in a Digital Payment System</i>	112
B. <i>Interoperability and Data Sharing</i>	114
C. <i>Information Value of Money and Payment</i>	115
III. CONFLICTS OF DATA GOVERNANCE	118
A. <i>Restrictions on Data Transfer</i>	119
1. Adequacy Decisions and Appropriate Safeguards for Data Protection	119
2. Data Localization for National Security	122
B. <i>Balance in Payment Data Sharing</i>	124
IV. COORDINATED DATA GOVERNANCE: LEGAL AND TECHNICAL PROPOSALS	127
A. <i>Institutional Bases for Data Sharing</i>	128
B. <i>Data Governance Measures</i>	131
1. Data Importance Classification.....	131
2. Data Access and Control.....	134
3. Data Portability.....	137
C. <i>Technical Proposals for Interoperability, Privacy and Security</i>	138
1. Standardized Data Formats and Protocol	139
2. Interoperable Digital Identity	140
3. Common Layer and Access Through APIs.....	141
4. Privacy and Security.....	144
V. CONCLUSION	148

INTRODUCTION

Digital money is the digital representation of money¹—something generally used as a medium of exchange, a unit of account, and a store of value. Though banks sometimes use the name ‘coin’ or ‘currency’ like Bitcoin² or central bank digital currency (CBDC),³ digital monies are just pieces of information existing as digital codes and electromagnetic waves. Payment is the movement of money.⁴ In terms of digital money, payment takes the form of data transmission to deliver certain information, e.g., information about the payer and payee, amount of payment, payment periods, and methods. Banks and central banks know the trader’s identity, account balance, time, and place of payment to verify the validity of transactions and guarantee settlement finality.⁵ In a digital payment system, money is like a memory of past debt and credit recording.⁶

Interoperability is “the capability to communicate, execute programs, or transfer data among various functional units in a manner that requires the user to have little or no knowledge of the unique characteristics of those units.”⁷ Interoperability is a critical feature of digital money to increase efficiency and realize network effects in cross-border payments. Interoperability is the

1. IMF, *A New Era of Digital Money* (2021), <https://www.imf.org/external/pubs/ft/fandd/2021/06/online/digital-money-new-era-adrian-mancini-griffoli.htm>.

2. See generally Garrick Hileman & Michel Rauchs, *Global Cryptocurrency Benchmarking Study*, CAMBRIDGE CTR. FOR ALT. FIN. 33 (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2965436.

3. Codruta Boar & Andreas Wehrli, *Ready, Steady, Go? – Results of the third BIS survey on central bank digital currency*, BIS PAPERS NO. 114, 3 (Jan. 2021); Codruta Boar et al., *Impending arrival – a sequel to the survey on central bank digital currency*, BIS PAPERS NO. 107, 1 (Jan. 2020); European Central Bank, *Report on a Digital Euro*, 3 (Oct. 2020); Raphael Auer & Rainer Böhme, *The technology of retail central bank digital currency*, BIS QUARTERLY REV.: INT’L BANKING & FIN. MKT. DEVS. 1, 85 (Mar. 2020).

4. Another Colour, *Australian Payments Network: Presenting Payments in Our Digital World* (2016), <https://anothercolour.com.au/projects/australian-payments-network-annual-report-design/>.

5. See generally Codruta Boar et al., *supra* note 3 (using general terminology to describe the processes of digital currency exchange).

6. Narayana R. Kocherlakota, *Money is Memory*, 81 JOURNAL OF ECONOMIC THEORY, 81 J. ECON. THEORY 232 (1998).

7. *Information Technology–Vocabulary ISO/IEC 2382*, INT’L ORG. FOR STANDARDIZATION (2015), <https://www.iso.org/obp/ui#iso:std:iso-iec:2382:ed-1:v2:en>.

capability of different digital monies or different payment systems to work together, with necessary information sharing and transfer to one another.⁸ The interoperability issue arises in cross-border payments where the payer and payee reside in different jurisdictions and pay with the same or different types of money. More interoperable cross-border payment is part of the G20 cross-border payments roadmap to increase data quality and straight-through processing based on coordinated regulatory, supervisory, and oversight frameworks and payment infrastructures.⁹ Countries like India are fast scaling their interoperable unified payment stack and financial account aggregator mechanism.¹⁰ Newly emerged cryptocurrencies, like Libra¹¹ or Bitcoin¹², are created, at least in part, to facilitate cross-border payment and exchange between different currencies.

Interoperability brings in concerns about data governance conflicts between countries. What accompanies cross-border payments is a data generation process, which is necessary to initiate and operate cross-border payments. Data governance involves the power and legal arrangement of managing data availability, usability, integrity, and security. The trade-off between payment interoperability and data protection will be a new paradigm in most digital public service infrastructures where the relevant social function goes along with data governance. On the one hand, data sharing will increase operational efficiency and access to financial services, save time for customers in their interactions with the financial services

8. Jorge Herrada & Angela N. Lawson, *Fit-for-Purpose Payment System Interoperability: A Framework*, FEDS NOTES (July 14, 2022), <https://www.federalreserve.gov/econres/notes/feds-notes/fit-for-purpose-payment-system-interoperability-a-framework-20220714.html>.

9. *Cross-border Payments*, FSB, <https://www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/cross-border-payments/> (last modified Nov. 17, 2022).

10. Sampath Putrevu, *IndiaStack Introduces Account Aggregator Initiative to Drive Financial Inclusion in a Fair and Equitable Manner*, YOURSTORY (Feb. 23, 2020), https://yourstory.com/2020/02/indiastack-account-aggregator-financial-inclusion-prime-knowledge?utm_pageloadtype=scroll.

11. *White Paper, LIBRA 1–2*, https://wp.diem.com/en-US/wp-content/uploads/sites/23/2020/04/Libra_WhitePaperV2_April2020.pdf (last visited Feb. 11, 2023).

12. Satoshi Nakamoti, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN 1, <https://bitcoin.org/bitcoin.pdf> (last visited Feb. 11, 2023) (explaining the benefit of the uniformity of using Bitcoin rather than physical currency when making transactions).

provider, and improve product options. On the other, states have various de jure and de facto restrictions on data transfer, such as local data mirroring, explicit or implicit local data storage and processing, and exclusion of foreign firms from managing and processing local data.¹³ The root cause may be states' monetary sovereignty and national security concerns, payment operators' competition for the data source in the market, users' privacy, and technical incompatibilities worldwide.¹⁴

This article examines the data governance issue of digital money, exemplified by the CBDC. Central banks and governments have made some efforts for cross-border payment coordination, such as the mCBDC Bridge,¹⁵ Dunbar initiatives coordinated by the BIS Innovation Hub,¹⁶ Project Stella,¹⁷ and Project Jasper,¹⁸ among others.¹⁹ These proposals are still in their infancy and await to be specified for detailed requirements, including data protection measures. Cross-border data sharing is crucial in the international proliferation and acceptance of CBDC, but it needs legal and technical support. Digital infrastructure operators should be regulated to the extent that they do not interfere with the privacy of individual users and businesses nor threaten a

13. Nigel Corey and Lunch Dascoli, *How Barriers to Cross-Border Data Flows are Spreading Globally, What They Cost, and How to Address Them*, INFO. TECH. & INNOVATIONFOUND., <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/> (July 19, 2021).

14. Andrew D. Mitchell and Jarrod Hepburn, *Don't Fence me in: Reforming Trade and Investment Law to Better Facilitate Cross-border Data Transfer*, 19 YALE J. L. & TECH. 182, 186 (2017).

15. *Joint Statement on the Multiple Central Bank Digital Currency (m-CBDC) Bridge Project*, Hong Kong Monetary Authority (Feb. 23, 2021), <https://www.hkma.gov.hk/eng/news-and-media/press-releases/2021/02/20210223-3/>.

16. Bank for Int'l Settlements [BIS], *Project Dunbar: International Settlements Using Multi-CBDs*, at 3 (Mar. 2022), <https://www.bis.org/publ/othp47.pdf>.

17. STELLA (Joint Rsch. Project of the Eur. Cent. Bank & the Bank of Japan), *Synchronized Cross-Border Payments*, at 1–2 (June 2019), <https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical190604.en.pdf>.

18. The Bank of Canada & Monetary Auth. of Singapore, *Jasper-Ubin Design Paper: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies*, at 4 (2019), <https://www.mas.gov.sg/-/media/Jasper-Ubin-Design-Paper.pdf>.

19. Bank of Canada, Bank of England, & Monetary Auth. of Singapore, *Cross-Border Interbank Payments and Settlements: Emerging Opportunities for Digital Transformation*, at 6 (Nov. 2018), <https://www.mas.gov.sg/-/media/MAS/ProjectUbin/Cross-Border-Interbank-Payments-and-Settlements.pdf>.

state's national security and public interest. Data governance rules for digital money issued by private entities can be similar as these money issuers and operators undertake similar regulatory tasks for public reasons.

To explore the chances of data governance coordination, Section II reviews the data flow of cross-border payments and explains the information value of money. Section III examines legal and factual restrictions on cross-border data transfer and reveals the deeper conflict between data security, privacy, market competitiveness, and digital money interoperability. Section IV suggests that data sharing for cross-border payments needs international cooperation for different data types at different levels. It also introduces technical solutions such as standardized data formats, APIs, cloud computing, and encryption that make the scheme possible. Finally, Section V concludes that designing an interoperable CBDC will depend on the relative benefits of the new payment system and data protection strategies by countries. Governments and central banks should weigh the costs and benefits of the international use of CBDC, differentiate the importance of data for the public and businesses, and then decide on the scope of data access and control from foreign entities. Furthermore, data governance arrangements should be embedded in the digital infrastructure so that in the beginning, data is conditionally available to operators and users of the system. Technology, in this sense, is not a passive implementation of the legal rules but proactive embeddedness that affects social behaviour beforehand.

II. DIGITAL MONEY INTEROPERABILITY AND DATA SHARING

A. *Data in a Digital Payment System*

CBDC is a digital form of central bank money different from balances in traditional reserve or settlement accounts; it is a digital payment instrument denominated in the national unit of account.²⁰ CBDCs are intended for various cross-border payments, such as trade settlement, insurance payment,

20. Bank for Int'l Settlements [BIS], *Central Bank Digital Currencies: Foundational Principles and Core Features*, at 2 (2020), <https://www.bis.org/publ/othp33.pdf>.

commercial payment, wealth connect settlement, corporate bond issuance, low-value aggregation services, e-commerce, supply chain finance, and settlement of tokenized dual-currency instruments.

For countries that lack private payment provisions, the central bank could perform the issuance, management, and all other functions of the CBDC. Yet for countries with various payment participation by the public and private actors, the CBDC is better operated on a two-tier issuance and transaction system in which the central bank acts as the primary issuer and payment service providers perform periphery tasks. The central bank is responsible for currency issuance, destruction, and settlement, monitoring and controlling transactions by enforcing capital controls based on accurate data of onshore and offshore holdings. While the public pays for goods and services through retail payment institutions, these institutions carry out large-value transactions between them through wholesale payments.

The policy and technical design of digital money determine access to data in a payment system. CBDC is expected to operate like physical cash, which is highly private to all parties except the payee, who often sees the payers' identity. At the retail point, payment service providers can access user's data for transaction verification, authorization, and settlement. They also need customers' identification and records of transactions for anti-money laundering (AML) and counter-financing of terrorism (CFT).²¹ Payment service providers may be required to submit transaction data to the central bank and other regulatory authorities via asynchronous transmission on a timely basis.²²

21. People's Bank of China, *Progress of Research & Development of E-CNY in China*, at 10 (July 2021), <http://www.pbc.gov.cn/en/3688110/3688172/4157443/4293696/2021071614584691871.pdf>.

22. Fan Yifei, *Some Thoughts on CBDC Operations in China*, CENT. BANKING (Apr. 1, 2020), <https://www.centralbanking.com/fintech/cbdc/7511376/some-thoughts-on-cbdc-operations-in-china>.

B. Interoperability and Data Sharing

Interoperability is the technical and legal compatibilities that enable a payment system to be used with others.²³ Interoperability allows participants in different systems to conduct, clear, and settle payments or financial transactions across systems without participating in multiple systems.²⁴ Higher levels of interoperability will increase payment efficiency by creating economies of scale, e.g., better serving risk management, encouraging competition by lowering the entry threshold, releasing consumer lock-in, and increasing market competition.²⁵ With respect to retail linkages, CBDCs should be interoperable with other payment means so that they can be exchanged freely with bank deposits and cash. As for wholesale linkages, an interoperable CBDC platform could allow for the issuance of CBDCs by a central bank, the exchange between different CBDCs, and the redemption of CBDCs from a commercial bank at the central bank.²⁶ Interoperable CBDCs are expected to link to existing large value transfer systems, including foreign payment systems.²⁷

As the interoperability of digital money requires the communication and cooperation between different payment institutions,²⁸ data sharing and transfer are essential to keep units in the payment system running. Designing the scope of data sharing involves trade-offs between cost, efficiency, and security.

23. Committee on Payment and Settlement Systems of the Bank for Int'l Settlements [BIS], *A Glossary of Terms Used in Payments and Settlement Systems*, at 10, <https://www.bis.org/cpmi/publ/d00b.htm?&selection=177&scope=CPMI&c=a&base=term>.

24. Org. for Econ. Coop. and Dev. [OECD], *Data Portability, Interoperability, and Digital Platform Competition: OECD Competition Committee Discussion Paper*, at 48 (2021), <https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf>.

25. Ian Brown, INTEROPERABILITY AS A TOOL FOR COMPETITION REGULATIONS 6 (2020).

26. Raphael Auer et al., *Multi-CBDC Arrangements and the Future of Cross-Border Payments*, BANK FOR INT'L SETTLEMENTS [BIS] PAPERS NO. 115, at 5–6 (Mar. 2021).

27. Raphael Auer et al., *Rise of the Central Bank Digital Currencies: Drivers, Approaches, and Technologies*, BANK FOR INT'L SETTLEMENTS [BIS] PAPERS NO. 880, at 28 (Aug. 2020).

28. *Information Technology—Vocabulary ISO/IEC 2382*, INT'L ORG. FOR STANDARDIZATION (2015), <https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:ed-1:v2:en>.

Security, or risk management considerations, includes fraud risk (AML and CFT), liquidity risk (the risk that a financial institution cannot settle at the designated time due to insufficient funds available at the time of individual transaction), and credit risk (the risk of loss by payment institutions that owed funds by the defaulting institutions where payment institutions are required to make final payments to their customers instantly). The information value of money and payment should be clearly understood to uncover the incentives of data sharing so that the interests of all stakeholders can be aligned to build an interoperable system.

C. Information Value of Money and Payment

The payment system records monetary transactions and reflects the financial status of transacting parties. The information value of money perches in a hierarchy where different interests have different priorities, as is presented in Figure 1 below.²⁹

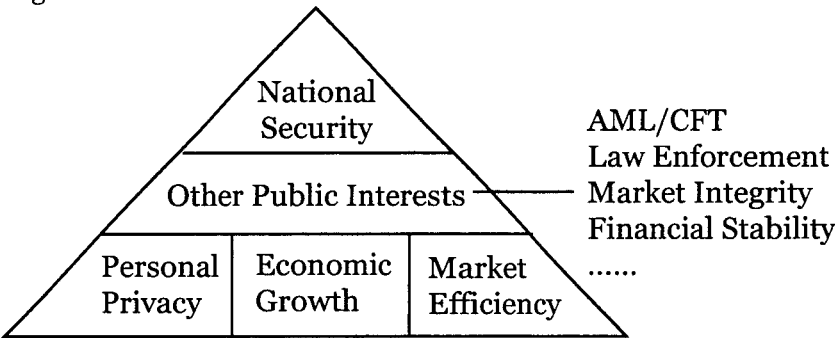


Figure 1: Hierarchy of the Information Value of Money

Among these values, national security comes first. Here, national security particularly refers to economic security that can be understood as the smooth operation of monetary systems, which

29. See generally Andrew D. Mitchell & Jarrod Hepburn, *Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*, 19 YALE J. L. & TECH. 182, 186, 188–193 (2017) (explaining the rationale behind restricting cross-border transfers to protect various interests).

matters for people's welfare and daily transactions.³⁰ For the state, the money and banking system is part of its financial sovereignty, which is the state's power to exercise exclusive legal control over its currency. The public nature of money³¹ suggests that money is a macro moderator used by governments to support their economy, achieving policy goals such as full employment and price stability. As an important part of the money supply, CBDCs will affect monetary policy implementation and transmission, hence the monetary policy's effectiveness. The CBDC ecosystem will be a high-value target once deployed, causing greater impacts on the economy and the financial system. The central bank will have to put suitable controls and processes in place to mitigate the risk of large-scale attacks from these advanced persistent threats. Congregate transaction data in a payment system provides crucial information about the quantity of money (the amount of transaction, leverage ratio of large financial institutions) and its value (price level, interest rate, and exchange rate). The government and central bank can accordingly take effective measures (e.g., imposing fees, taxes, tolls, and tributes on the transaction) to affect money circulation.

Specific public interests such as market integrity, financial stability, transparency, and so on are ranked second.³² Hidden information and opaqueness may breed illegal activities.³³ Anonymity can be abused by ill-intentioned individuals to engage in criminal activities, such as counterfeits, double spending, financial terrorism, money laundering, and tax evasion.³⁴ Less fraud and deception will lower the risk premium in the market by reducing the risk of issuers and the cost of capital, both pre-trade

30. See generally DICK K. NANTO, *ECONOMICS AND NATIONAL SECURITY: ISSUES AND IMPLICATIONS FOR U.S. POLICY*, CONG. RSCH. SERV., R41589 1 (Jan. 2011) (explaining that national security is very closely related to economic security because citizens prosper and economies grow when people can reside without fear and can take part in a vibrant and secure economic system).

31. See CHRISTIAN FELBER, *THE BASIS: MONEY AS A PUBLIC GOOD*, 29–30 (2017).

32. See BANK FOR INTERNATIONAL SETTLEMENTS, *CBDCs: AN OPPORTUNITY FOR THE MONETARY SYSTEM*, 70 (2021).

33. *Id.* at 82.

34. *Id.* at 74, 82.

and post-trade.³⁵ Additionally, transparency and disclosure protect investors and help achieve financial stability.³⁶ The call for transparency comes with the neo-liberal belief that uncertainties surrounding market information's availability, reliability, and comparability distort financial market participants' decision-making, leading to contract deficiencies and market volatility.³⁷ The significance of authentic and comprehensive information disclosure was partly revealed in the financial crisis, where the way-off valuation book of most financial institutions masked the risks, triggering a worldwide financial crisis.³⁸ The disguised book helped to gloss over disturbing facts and resulted in the crisis by changing the character of many financial relationships.³⁹ These chain reactions are aggravated by digital money, which is more susceptible to high leverage and procyclicality.⁴⁰ Governments need payment information to enhance the power of discipline and regulation of monetary transactions.

Ranked third are personal rights such as privacy and other legitimate interests, benefits from market efficiency, and economic growth, among which there is no absolute preferential order. Privacy can be defined as the capability of individuals to control access to information about themselves.⁴¹ The recognition of privacy shows respect for an individual's inviolate personality, including one's spiritual nature, feelings, and intellect.⁴² As a

35. Dan Dhaliwal et al., *Corporate Social Responsibility Disclosure and the Cost of Equity Capital: The Roles of Stakeholder Orientation and Financial Transparency*, 33 J. ACCT. & PUB. POL'Y 1, 3 (2014).

36. See BANK FOR INTERNATIONAL SETTLEMENTS, *supra* note 32, at 77.

37. See INTERNATIONAL MONETARY FUND, *REFORMING THE INTERNATIONAL FINANCIAL ARCHITECTURE—PROGRESS THROUGH 2000* (2001).

38. See Rosalind Wiggins et al., *The Lehman Brothers Bankruptcy A: Overview*, 1 J. OF CRISES 39, 44 (2019).

39. See AMAR BHIDÉ, *A CALL FOR JUDGMENT: SENSIBLE FINANCE FOR A DYNAMIC ECONOMY* 13 (2010).

40. See SIRIO ARAMONTE ET AL., *DEFI RISKS AND THE DECENTRALISATION ILLUSION* 29, 33 (2021).

41. See Julie E. Cohen, *What Privacy is For*, HARV. L. REV. 1904, 07 (2013) (commenting on the general definition of Privacy as understood by modern privacy theorists).

42. See Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

mode of social ordering, privacy reserves space for social individuals to engage in the processes of boundary management through which they define and refine themselves as subjects.⁴³

At a social level, data has become a key factor of production, the exploitation of which will boost productivity and growth in the long run.⁴⁴ For instance, information about borrowers' risk of default is particularly important for banks to decide whether a user can meet its payment obligations to reduce the credit risks and increase the quality of bank assets. Data is also essential when the payment system is designed for automatic payment upon predetermined conditions.

Unlike other resources, data can be used by many people and entities simultaneously without being depleted. As the self-reinforcing data-network-activities loop incorporates more users into the payment system, it may lead to entrenched market power and data concentration.⁴⁵ Data governance rules affect the availability of information in the market and the costs and benefits of relevant activities. Since different types of data bear different political, social, and economic significance, states impose different data protection and security rules.⁴⁶

III. CONFLICTS OF DATA GOVERNANCE

Data generation, collection, processing, and transfer run parallel to cross-border payments. Frictions occur when the transfer is impeded for technical and legal reasons. Payment infrastructures worldwide are often developed to run on proprietary communications, security, and data standards and protocols, resulting in a lack of interoperability between different systems. Incompatible data standards across payment networks adversely affected transnational payment processing at payment

43. See Judith A. Swanson, *Private Friends and Public Citizens* 186-87 (1992); see also Julie E. Cohen, *Privacy Autonomy, and Information* 2 (2012).

44. See NIGEL CORY & LUKE DRISCOLL, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION, HOW BARRIERS TO CROSS-BORDER DATA FLOWS ARE SPREADING GLOBALLY, WHAT THEY COST, AND HOW TO ADDRESS THEM 15 (2021).

45. See BANK FOR INTERNATIONAL SETTLEMENTS, *supra* note 32, at 66.

46. See Bo Zhao & Yang Feng, *Mapping the Development of China's Data Protection Law: Major Actors, Core Values, and Shifting Power Relation*, 40 COMPUT. & SCI. SEC. REV. 1, 4 (2021).

institutions. Furthermore, explicit or implicit restrictions on foreign access and control of data are prevalent in data protection laws and regulations. Some restrictions are alike for all participants, such as the risk profile of cross-border payments. Whereas home states of payments may focus on operational resiliency, governance, and liquidity management; host states will pay more attention to investor and consumer protection, and monetary and financial stability. Other obstacles are state-specific, such as restrictions on cross-border data transfer and data localization policies.⁴⁷ These restrictions interfere with foreign governments' businesses and individuals' access and usage of the data concerned.

A. *Restrictions on Data Transfer*

1. Adequacy Decisions and Appropriate Safeguards for Data Protection

Current legal bases for cross-border data transfer include whitelist jurisdictions (e.g., EU's adequacy decisions), certifications (e.g., APEC CBPR, certification under GDPR, privacy shield), safeguards (e.g., model contract clauses, binding corporate rules), consent by the data subject, and necessity (e.g., for the conclusion or performance of the contract).⁴⁸ Some jurisdictions, such as Hong Kong, combine these measures to have elastic decisions.⁴⁹ Specifically, data transfer may be

47. See John Selby, *Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?*, 25 INT'L J. OF L. AND INFO. TECH. 213 (2017) (commenting on measures within the Trans-pacific partnership meant to prevent data localization); see also Paul M. Schwartz, *The EU-US Privacy Collision: A Turn to Institutions and Procedures*, 126 Harv. L. Rev. 1966, 89 (2013) (noting the EU's commitment to for cross-border flow of data to bolster international trade); Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU?*, 8 PA. ST. J. OF INT'L L. & AFFS. 50, 103–04 (2020) (highlighting the differences between data sharing regimes of China, U.S., and EU, and the preference to avoid data localization).

48. Aida Kaloci, *Guide to the Cross-Border Transfer of Personal Data in the GDPR*, DELOITTE, <https://www2.deloitte.com/al/en/pages/legal/articles/gdpr.html> (last visited Feb. 13, 2023).

49. Hong Kong Personal Data Privacy Ordinance, (1997) Cap. 486, § 33 <<https://www.elegislation.gov.hk/hk/cap486!en>> accessed 13 December 2021 (laying out multiple exceptions under which users may transfer personal data out of Hong Kong).

permitted if the data is transferred to places in the whitelist; there is an adequate data protection regime in the destined jurisdiction; there is written consent by data subjects; it is transferred for avoidance and mitigation of adverse action against data subjects; the use of personal data is exempted from use limitation; or data users take reasonable precautions and due diligence.

These rules are often applied in a sequence of considerations. According to Articles 45, 46, and 49 of the GDPR, adequacy decisions should carry out data transfer outside the European Economic Area, have appropriate safeguards where there is no adequacy decision, or be exempted for specific situations if there are neither adequacy decisions nor appropriate safeguards.⁵⁰ In the *Schrems II* case⁵¹, the Grand Chamber of the European Court of Justice (CJEU) invalidated the Commission's decision on the adequacy of data protection provided by the EU-US privacy shield.⁵² The Court's invalidation of the privacy shield was built on the following reasons: the primacy of US law enforcement requirements over those of the privacy shield;⁵³ lack of necessary limitations and safeguards on the power of the authorities under US law, particularly in consideration of the proportionality requirements;⁵⁴ lack of an effective remedy in the US by EU data subjects;⁵⁵ and deficiencies in the privacy shield ombudsman mechanisms.⁵⁶

50. General Data Protection Regulation, Art. 45, Transfers on the Basis of an Adequacy Decision (Eur. Union); General Data Protection Regulation, Art. 46, Transfers Subject to Appropriate Safeguards (Eur. Union); General Data Protection Regulation, Art. 49, Derogations for Specific Situations (Eur. Union).

51. Case C-362/14, *Schrems v. Data Prot. Comm'r*, ECLI:EU:C:2015:627 (Oct. 6, 2015).

52. Xavier Tracol, "Schrems II": *The Return of the Privacy Shield* (2020) 39 COMPUT. L. & SEC. REVIEWREV., November 2020, at 1, <https://doi.org/10.1016/j.clsr.2020.105484>.

53. *Id.* at 6.

54. *Id.*

55. *Id.* at 7.

56. *Id.* at 6.

Following the Schrems II case, the EU and the US adopted the EU-US Data Protection Umbrella Agreement 2016⁵⁷ for regulating the transatlantic flow of personal data,⁵⁸ which imposes stronger obligations on the US side for data protection. The European Commission also revised its Standard Contractual Clauses for cross-border data transfer⁵⁹ and adopted final recommendations on supplementary measures for transfer tools.⁶⁰ The supplementary measures highlighted a six-step roadmap to assist with assessing third countries, and identifying and implementing appropriate supplementary measures.⁶¹ The six steps require that data controllers identify the transfer conditions (adequacy decisions, appropriate safeguards, derogations), assess whether the transfer tool is effective in view of transferring factors, receive the country's laws, and transfer outcomes, take supplementary measures and procedural steps, and re-evaluate at appropriate intervals.⁶² It can be found that the EU paid much attention to protecting personal data at an individual level, with fewer national concerns about the significance of aggregate data. But even this rigorous personal data protection puts forward a high standard for other countries to observe.

Despite these restrictions on data transfer, payments and transactions in a digital payment system are processes of data generation, collection, and processing, not purely data transfer. In Lindqvist⁶³, the CJEU held that there is no transfer of data to a third country within the meaning of Article 25 of Directive 95/46, where an individual loads personal data onto an internet

57. Agreement between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offences, 2016 O.J. (L 336) 3.

58. European Commission Press Release IP/16/2461, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 12, 2016).

59. Commission Implementing Decision 2021/914, 2021 O.J. (L 199) 31, 32, 37.

60. Recommendations 01/2020, of the European Data Protection Board on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data (Adopted version for public consultations, 10 November 2020).

61. *Id.* at 8–19.

62. ONETRUST DATAGUIDANCE, THE DEFINITIVE GUIDE TO SCHREMS II 7 (2022).

63. Case C-101/01, *Lindqvist v. Jönköping*, ECLI:EU:C:2002:513 (Sep. 19, 2002).

page that is stored with his hosting provider, which is established in that State or another state, making the data accessible to anyone who connects to the internet, including people in a third country.⁶⁴ Instead, data transfer entails technical means needed to access the internet and make information available to people who did not intentionally seek access to that information. Moreover, as most data protection laws allow for lawful processing and transfer, carve-out and exception provisions can be properly used to justify data transfer. Special arrangements may trigger potential regulation and censorship and thus constitute de facto data-sharing burdens.

2. Data Localization for National Security

States carry out data localization policies because they have increasingly realized the importance of data as a strategic political and economic resource. Data localization requirements are enforced in many ways, such as local data mirroring, explicit or implicit local data storage and processing, discriminatory licensing, certification, and other regulatory restrictions to exclude foreign firms from managing and processing local data.⁶⁵

Under the ideology of national security, technology nationalism, and the balance between industrial benefits and individual privacy, China views data localization as part of its internet sovereignty.⁶⁶ Following the centralized state control over data management, China has established a series of data protection laws and regulations, represented by the Cybersecurity Law, Data Security Law, and Personal Information Protection Law. Protected data includes the digital form of personal information and important data the internet operator collects and produces in China. The overall approach to data transfer in China is “local storage, outbound assessment.”⁶⁷ The rules apply to important data collected and generated in China by critical information infrastructure operators, data handlers, and

64. *Id.* ¶¶ 21, 46.

65. Corey & Dascoli, *supra* note 13.

66. Jinhe Liu, *China's Data Localization*, 13 CHINESE J. OF COMM'C'N 84 (2020).

67. *Id.* at 87.

personal information handlers.⁶⁸ Critical information infrastructure operators should store personal information and important data generated from critical information infrastructures in mainland China.⁶⁹

China's classification scheme distinguishes different data types based on their risks, importance, and impacts. In the Draft Guidelines for Data Cross-Border Transfer Security Assessment in China, regulated objects include personal information and important data in electronic form collected and generated by network operators during their operations within the territory of China. Important data includes but are not limited to (i) security information of financial institutions;⁷⁰ (ii) financial information of natural persons, legal persons, and other organizations;⁷¹ and (iii) working secrets not involving state secrets generated during the work of the central bank, financial regulatory authorities, and foreign exchange regulatory authorities. To clarify how "important" data is, the People's Bank of China issued the industrial standard, the Financial Data Security—Security Specification of Data Life Cycle,⁷² which provides detailed requirements for the collection, transmission, use, deletion, and destruction of different grades of financial data based on the financial data's safety grades.

If firms are to transfer personal and important data abroad, principal requirements include business necessity, customer's written authorization, associated institutions as data recipients, signed agreement, and compliance with laws and regulations. Security assessments and approval from regulatory bodies are required for data transfer outside mainland China.⁷³ Different

68. *Id.* at 88.

69. Cybersecurity Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Nov. 7, 2016, effective June 1, 2017), art. 37.

70. Guidelines for Data Cross-Border Transfer (promulgated by Standardization Admin. China) art. A.19.1.

71. *Id.* at art. A.19.2

72. "Financial data security—Security specification of data life cycle" financial industry standard officially released, CHINA FIN. STANDARDIZATION TECH. COMM. (May 15, 2021), <https://www.cfsc.org/en/2932554/2980189/index.html>.

73. Shuju Chujing Anquan Pinggu Banfa (数据出境安全评估办法) [Measure for Data Export Security Assessment] (promulgated by the State Internet Info. Off., May 19, 2022, effective Sept. 1, 2022), art. 4.

control measures are taken in line with the characteristics of different data usage and transfer stages, including data collection, processing, storage, distribution, and destruction.⁷⁴ The state shall exercise export control over data defined as controlled items related to safeguarding national security interests and fulfilling international obligations.⁷⁵ Multi-level cybersecurity protection measures are required for critical information infrastructure operators whose data breach activities may seriously damage national security and public interest.⁷⁶

B. Balance in Payment Data Sharing

As stated above, various obstacles exist in cross-border data sharing for payment interoperability. Payment institutions are either restricted for privacy protection or national security considerations. Indeed, data governance arrangements affect privacy, market competitiveness, and profitability. The current situation is that the state, business, and individual interests outweigh the common good of data sharing, and these restrictions on data sharing impede the interoperability of digital money in cross-border payments.

In a payment system, data access and control are necessary for clearing and settlement between payment institutions, without which payment cannot occur. Data collection and processing are essential for guaranteeing the security and certainty of payments. States should allow data sharing for payment security and finality for AML and CFT purposes. Moreover, the interoperable digital money will run with fewer fees, fewer operational complexities, fewer foreign exchange settlement risks, higher transparency, and lower reporting burden, because data and information are available to all

74. Zhonghua Renmin Gongheguo Shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of China] (promulgated by the Standing Comm. Nat'l People's Cong., Jun 10, 2021, effective Sept. 1, 2021), arts. 3, 27.

75. *Id.* at art. 25.

76. *Id.* at art. 31 (requiring the security management protocol for critical information operators to be formulated by the national cyberspace authority alongside the State Council); see also *id.* at art. 36 (requiring Chinese individuals and organizations to go through multiple levels of government authorization to provide data stored in China's borders with any foreign judicial or law enforcement body).

operators in the network. The clearing and settlement system will be able to net trades and mitigate obligations that continue beyond an end-of-day settlement period. This system is more efficient as it internalizes the network effects of adding more users through type-specific contracts. The system may reduce payment costs that can take away 1% or more of the GDP annually.⁷⁷ It is estimated that economies that embrace data sharing for finance could see GDP gains of between 1–5% by 2030, with benefits flowing to consumers and financial institutions.⁷⁸ The sharing of payments data also enables the execution of smart contracts and integration of payment instruments and infrastructures with other information systems for businesses such as accounting or liquidity management. Therefore, central banks and regulators should coordinate their data governance policies for mutual social economic benefits.

This does not mean that data sharing should go as far as possible. Data sharing is good insofar as it enhances the security and efficiency of payments, not at the cost of distorting the market. This coordination is worth more consideration because market fragmentation may enhance the informativeness of prices, relative to a centralized market where all trade flows are consolidated, and hence improves allocative efficiency where prices are closer to being a random walk.⁷⁹ When the market is more fragmented, transactions costs can be lower and executions speeds are faster.⁸⁰ In other words, fragmentation can improve allocative efficiency and price informativeness in some cases.⁸¹

On the other hand, collective action problems arise in cross-border payments because states have diversified incentives,

77. See Heiko Schmiedel et al., *The Social and Private Costs of Retail Payment Instruments: A European Perspective*, EUR. CENT. BANK, Sept. 2012, at 4; David Humphrey et al., *What Does it Cost to Make a Payment?*, 2 REV. OF NETWORK ECON. 159, 159 (2003).

78. Olivia White et al., *Financial Data Unbound: The Value of Open Data for Individuals and Institutions*, MCKINSEY & CO. (June 24, 2021), <https://www.mckinsey.com/industries/financial-services/our-insights/financial-data-unbound-the-value-of-open-data-for-individuals-and-institutions>.

79. Daniel Chen & Darrell Duffie, *Market Fragmentation*, 111 AM. ECON. REV. 2247, 2247 (2021).

80. Maureen O'Hara & Mao Ye, *Is Market Fragmentation Harming Market Quality?*, 100 J. OF FIN. ECON., 459, 460 (2011).

81. Chen & Duffie, *supra* note 79, at 2247.

strategies, and even conflicting interests in data sharing. Some of these problems are comparable, such as the state's sovereignty concerns and individual's valuation of personal privacy, which can be solved by shaping trust and respect for digital sovereignty and regulatory compliance. Other policy disparities are fundamental, such as the EU's strong personal data protection, China's national security and big data development strategy, and the US upholding extraterritorial data regulation for its domestic legal interest and judiciary power application. In 2018, the US enacted the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which empowers federal law enforcement to legally require US-based technology companies, by means of warrants or subpoenas, to disclose requested data stored on servers, irrespective of whether the data is located domestically or in foreign countries.⁸² The CLOUD Act was inspired by the case of *United States v. Microsoft Corp.*⁸³ Now, firms can no longer refuse to deliver their data stored in a data center in another country.⁸⁴ Similar to extraterritorial judiciary and legal power conflicts in data usage, protection, and regulation can be more commonplace when countries want to extend the power of their domestic laws and regional agreements.⁸⁵ In jurisdictions with weak AML regulations, accessing a bank account needs only limited information as an identifier rather than identification.⁸⁶

82. U.S. DEPT OF JUST., PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 3 (2019).

83. *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018).

84. See U.S. DEPT OF JUST., *supra* note 82, at 7 (explaining that "the second part of the CLOUD Act clarifies that U.S. law requires that [communication service providers] subject to U.S. jurisdiction must disclose data that is responsive to valid U.S. legal process, regardless of where the company stores the data.").

85. See Mark A. Prinsley et al., *English High Court Considers Limits of the Extraterritorial Reach of the GDPR in Relation to an Overseas Website*, MAYER BROWN (Feb. 15, 2021), <https://www.mayerbrown.com/en/perspectives-events/publications/2021/02/english-high-court-considers-limits-of-the-extraterritorial-reach-of-the-gdpr-in-relation-to-an-overseas-website> (analyzing a U.K. case that contemplated the extraterritorial reach of an E.U. data protection law outside of the borders of the European Economic Area.).

86. See FED. DEPOSIT INS. CORP., RISK MGMT. MANUAL OF EXAMINATION POLICIES, 8.1-1 to -2 (describing the extensive identification requirements in jurisdictions with strong AML).

In the digital era, states will have a wider range of cooperation on digital trade and investment, which necessarily involves digital payments and payment with CBDCs where possible. For example, China has formally applied to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, a multilateral trade pact, to facilitate digital trade.⁸⁷ Despite the existing restrictions on cross-border data flow, China is expected to actively adjust its domestic laws and regulations and leave more space for data sharing. If countries want the common good of payment efficiency and economic growth, international coordination of data governance is needed to reduce barriers in data transfer and minimize the negative impacts of domestic actions. While countries may undergo a process of skepticism, experimentation, and adaptation to data sharing, they should step toward more aligned data governance standards to facilitate cross-border data use.

IV. COORDINATED DATA GOVERNANCE: LEGAL AND TECHNICAL PROPOSALS

To address states' concerns about monetary sovereignty, national security, economic profits, and consumer privacy, countries need to establish trust, common will, and reciprocity through international rules and standards. There is no common standard as to what extent should data be shared. The degree of privacy protection could vary from country to country depending on the governance, regulations, and implementation of the system. It depends on the political will and social benefits of payment and monetary cooperation. Some legal and technical solutions are suggested to reconcile countries' unwillingness to share data with other countries and the desire for an interoperable digital payment system. In an interoperable payment system, the level of privacy would default to the lowest common level of privacy used.

87. Xinmei Shen, *China to Pursue Digital Trade Expansion Under New Five-Year Plan as Cross-Border Data Flow Restrictions Remain in Place*, S. CHINA MORNING POST (Oct. 21, 2021), <https://www.scmp.com/tech/policy/article/3153196/china-pursue-digital-trade-expansion-under-new-five-year-plan-cross>.

A. *Institutional Bases for Data Sharing*

To coordinate data sharing and transfer, states need to establish clear and consistent legal foundations for their governmental regulation and enforcement. Many national and regional data protection laws provide the legal foundation of international cooperation for the protection of personal data.⁸⁸ At the end of 2020, the EU proposed a Data Governance Act which seeks to set up solid mechanisms to facilitate the reuse of certain categories of protected public-sector data, increase trust in data intermediation services, and promote data altruism across the EU.⁸⁹ Under the idea of data altruism, individuals and companies are encouraged to share or donate their data for the common good.⁹⁰ The proposal creates a new business model—data intermediation services—to provide a secure environment for data sharing.⁹¹ Companies can share their data on the platform and undertake data sharing and protection obligations therein, without fearing the misuse of data or loss of competitive advantage.⁹² Individuals can exercise their rights under the GDPR, control their data, and share the data with the companies they trust.⁹³ In the US, the Consumer Financial Protection Bureau's initiative attempts to facilitate a consumer-authorized

88. See, e.g., 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, and Repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter GDPR] (providing various measures and requirements for protecting personal data via international cooperation.); Renmin Xinxu Baohu Fa (人民信息保护法) [People's Information Protection Law] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021, effective Nov. 1, 2021), arts. 12, 38 (stipulating that China must actively develop rules for protecting personal information data through "international exchanges and cooperation.").

89. Council of the EU Press Release, EU Looks to Make Data Sharing Easier: Council Agrees Position on Data Governance Act (Oct. 1, 2021), <https://www.consilium.europa.eu/en/press/press-releases/2021/10/01/eu-looks-to-make-data-sharing-easier-council-agrees-position-on-data-governance-act/>.

90. *Id.* (explaining that a proposed European Union law would encourage data altruism by "mak[ing] it easier for individuals and companies to make data voluntarily available for the common good.").

91. *Id.*

92. *Id.*

93. See Council of the EU, *supra* note 89.

data-sharing market, while the Financial Data Exchange consortium attempts to promote common, interoperable standards for secure access to financial data.⁹⁴ Brazil's central bank has drafted guidelines on data access, technical standards, and consumer consent that will require financial institutions to give open-data access to nonbank third parties, and other countries in the region are following closely behind.⁹⁵

Yet these rules are quite inconsistent, fragmented, and enforced through unilateral measures that hurt exports and investment in data-based and data-related products and services. Also, mutual recognition and enforcement of data protection rules often involve much time and effort from both sides. Thus, it is crucial to establish international rules and standards of data governance. This can take the form of multilateral, plurilateral, and bilateral agreements, or soft law guidance. It can be a special data governance convention binding on its signing parties.⁹⁶ For greater integration into global economic institutions, data governance provisions can be added to current and future agreements on trade, investment, or payment between countries, as an essential part of the digital economy. These two methods of the multilateral agreement will not only provide a bargaining platform for countries to negotiate their common interests in exchange for one another but also help ensure that data governance arrangements do not discriminate against and are open to participation by other countries. Provisions on the transaction of CBDCs may include exchange rates, contract bases of the transaction (e.g., for trade or investment), and clearing and

94. *CFPB Outlines Principles for Consumer-Authorized Financial Data Sharing and Aggregation*, CONSUMER FIN. PROT. BUREAU, (Oct. 18, 2017), <https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-principles-consumer-authorized-financial-data-sharing-and-aggregation/>; see also *Financial Data Exchange (FDX) Adds 18 New Members*, FIN. DATA EXCH., (May 4, 2021), https://www.financialdataexchange.org/FDX/FDX/News/Press-Releases/FDX_Adds_18_New_Members.aspx.

95. See *Open Finance*, BANCO CENT. DO BRAZ., https://www.bcb.gov.br/en/financialstability/open_banking (last visited December 13, 2021).

96. See Douglas W. Arner et al., *The Transnational Data Governance Problem* 37 BERKLEY TECH. L. J. 623, 634–635 (2021).

settlement rules, as a foundation of data governance arrangements.

A less mandatory approach is to add data governance rules in existing international standards on financial markets, such as the Principles for Financial Market Infrastructures,⁹⁷ General Principles for International Remittances,⁹⁸ FATF Recommendations,⁹⁹ and the Basel III framework.¹⁰⁰ Sector-specific regulations coalitions will allow for a more detailed balance between data value and governance autonomy and are more flexible when technologies and market patterns change to call for different governance arrangements.

To better design and implement these rules, an international data governance institution can be established to work on best practices by member states' authorities, advise on the governance of cross-sectoral data governance arrangements, and deal with potential conflicts and disputes related to data sharing and control. This data governance institution needs to coordinate its relationship with other international organizations and dispute settlement forums such as WTO, ICSID, UNCITRAL, etc. Panel experts, arbitrators, or judges may work on a rotation basis to guarantee the updating and fairness of the rules.

States may set up a data protection office under the ministry of trade or commerce to decide on and execute better-informed data policy decisions. Such an office will improve interagency clearance, help illustrate the government's situation in international settings, and coordinate cross-border arrangements.¹⁰¹ Data administration officers should carefully weigh data privacy and security concerns with other competing policy objectives and values. Besides, the creation of a central

97. See THE BANK OF INTERNATIONAL SETTLEMENTS, PRINCIPLES FOR FINANCIAL MARKET INFRASTRUCTURE 5 (2012) ("The Standards in this report harmonize, and, where appropriate, strengthen existing international standards. . .").

98. See THE BANK OF INTERNATIONAL SETTLEMENTS, GENERAL PRINCIPLES FOR INTERNATIONAL REMITTANCE (2007).

99. See INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATIONS, FATF, 7 (2021).

100. See *International Regulatory Framework for Banks*, The Bank of International Settlements (2017), <https://www.bis.org/bcbs/basel3.html> (last visited Mar. 3, 2023).

101. See Peter Swire, *Why the Federal Government Should Have a Privacy Policy Office*, 10 J. ON TELECOMM. & HIGH TECH. L. 41, 50 (2012).

dashboard enables users and regulators to closely monitor and control the flow of data. This will facilitate the effective enforcement of legislation for the protection of personal data, provide international mutual assistance in the enforcement of this legislation, and promote the documentation and exchange of data protection legislation and practice.

B. Data Governance Measures

Data governance measures cover all aspects of data generation and circulation: collection, access, correction, processing, transfer, and erasure.¹⁰² The degrees to which these activities are permitted vary, depending on the importance of data, the purpose, context, and method of use, and other reasons.¹⁰³ There are also regulatory requirements on notice and transparency, purpose limitation, data minimization, security, records of processing, risk assessment, data breach notification, and registration with authorities.¹⁰⁴ These legal and regulatory measures should be predesigned and embedded in the digital payment system.

1. Data Importance Classification

The first step of data sharing is to identify the category of data and its importance. Data protection is not a one-size-fits-all solution that applies to all data in all situations. In a payment

102. See *What is Data Governance and Why Do You Need It?*, TALEND (last visited Feb. 13, 2023), <https://www.talend.com/resources/what-is-data-governance/> (“Data governance is a collection of processes, roles, policies, standards, and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.”).

103. See NAT’L INST. OF STANDARDS AND TECH., U.S. DEPT. OF COMM., SPECIAL PUB. NO. 800–53, SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS 7, 113, 114 (2020) (“Data actions are system operations that process personally identifiable information. The processing of such information encompasses the full information life cycle, which includes collection, generation, transformation, use, disclosure, retention, and disposal. . . provides a number of contextual factors that are important to assessing the degree of privacy risk created by the system. . .”).

104. See Standards for Safeguarding Customer Information 16 C.F.R. § 314.1 (2023) (“...sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.”).

system, protected data includes personal information about the payer, payee, the payment itself (content and purpose), and the relationships between the two parties.¹⁰⁵ It is important to identify the differential significance of data to different subjects.

States' willingness to share data is partly determined by the value of data in a specific field and the benefits of sharing it.¹⁰⁶ Risk management, such as AML, CFT, credit risk, and other prudential requirements, entails the sharing of information with competent authorities across jurisdictions.¹⁰⁷ Data classification will carve out space for data-fueled economic development under different regulatory obligations.¹⁰⁸ It also helps better understand and sort out data resources to leverage their social and economic value, enhance the standardization of datasets and increase the efficiency of data sharing.¹⁰⁹ The goal is to restrict the collection and transfer of sensitive data in some given sectors and free up other data to circulate in the economy with fewer restrictions.

The importance of data depends on the context and purpose of the transmission, considering its impact on economic and social

105. See Electric Funds Transfer Act, 15 U.S.C. § 205.9(a) (1978); see also *PCI Data Security Standards*, BOSTON UNIVERSITY, <https://www.bu.edu/cfo/comptroller/departments/cashier/resources/pci-data-security-standards/> (last visited Mar. 3, 2023) ("Cardholder Data/ Payment Card Data is all personally identifiable data about the cardholder. . .").

106. See *Enhancing Access to and Sharing of Data : Reconciling Risks and Benefits for Data Re-use across Societies*, OECD, <https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en> (last visited Feb. 13, 2023) ("This chapter describes the major challenges facing policy makers when enhancing access to and sharing of data. These include balancing its benefits and risks. . . . Balancing the benefits of enhanced data access and sharing with the risks while considering legitimate private, national and public interests.").

107. See FINANCIAL STABILITY BOARD, *ENHANCING CROSS-BORDER PAYMENTS STAGE 1 REPORT TO THE G20: TECHNICAL BACKGROUND REPORT*, 19, 24 (2020) ("Cross-border supervision and oversight requires the sharing of information with competent authorities in other jurisdictions and effective risk management requires sharing of information within a financial group that may span multiple jurisdictions. AML/CFT rules, for example, require cross-border information sharing within financial groups for the purposes of AML/CFT risk management.").

108. See Samm Sacks et al., *With Auto Data, China Buckles In for Security and Opens Up for Future Tech*, STAN. DIGICHINA, CYBER POL'Y CTR. (June 10, 2021), <https://digichina.stanford.edu/news/auto-data-china-buckles-security-and-opens-future-tech>.

109. *Id.*

development, national security, public interest, lawful rights, and legitimate interests, if the data is falsified, destroyed, leaked, or illegally acquired, or illegally used. The scope of data sharing should also consider the potential degree of harm (serious damage, ordinary damage, minor damage, no damage) caused in the event of information leakage or tampering.

As explained in the hierarchy of the information value of money, the importance of data can be roughly categorized into three levels.¹¹⁰ The first level is national security and the public interest which are the prioritized interests.¹¹¹ For instance, governmental authorities should have access to transaction data for AML and CFT regulations.¹¹² This data involves user identity and transaction verification information such as account passwords, KYC information, bank magnetic track data, chip information, card verification codes, card validity periods, and personal biometric identification information.¹¹³ The second level is financial privacy—personal information about a specific financial consumer, such as his or her financial status, the leakage of which may result in indirect property damage, discriminatory treatment, or harm to information security.¹¹⁴ Other examples of private financial matters are account

110. See Mitchell & Hepburn, *supra* note 29 (“The proffered justifications for such restrictions include policy concerns like safeguarding privacy and security, but digital protectionism may also be at play, entailing for example the promotion of the local information and communications technology industry either directly by providing preferential treatment in government procurement to domestic cloud computing companies, or indirectly by coercing foreign companies to locate their servers domestically. These restrictions tend to reduce market access for foreign suppliers of digital services, impeding trade and investment opportunities and increasing the costs and service choice of individual businesses.”).

111. *Id.* at 189.

112. See Rodrigo Coelho, *FSI Insights on Policy Implementation No 18: Suptech Applications for Anti-Money Laundering* 1, 3 (2019).

113. Irma Šlekytė, *What is Identity Verification? Process, Methods, and Benefits*, NORDVPN (Nov. 15, 2022), <https://nordvpn.com/blog/identityverification/#:~:text=Digital%20identity%20verification%20is%20the,%2C%20a%20password%2C%20etc.>

114. See *GDPR Personal Data – What Information Does This Cover?*, GDPR, <https://www.gdpreu.org/the-regulation/key-concepts/personal-data/>; see also *Data Classification Policy Best Practices*, STRONGDM, <https://www.strongdm.com/blog/dataclassificationpolicy/#:~:text=Data%20classification%20generally%20includes%20three,protecting%20your%20most%20critical%20information> (last visited Feb. 9, 2023).

information, personal identification information, personal property information, transaction history, home addresses, and more.¹¹⁵ The third level, which is of less significance, is the information used internally by financial institutions for working and record-keeping purposes, general business activities of financial institutions, or disclosed and accessible by the public.¹¹⁶ Information on digital wallets, such as the wallet ID, wallet type, wallet level, wallet name, wallet operating institution, opening-up date and wallet state, should bear the importance no lower than the third level.¹¹⁷

2. Data Access and Control

Data governance coordination should specify the conditions and scope of data access and control. Whatever the specific techniques adopted, there are some common standards that should be used to guarantee data security during the processes of data collection, transmission, storage, usage, sharing and destruction. Conditions and scopes of data access and control are linked to the design of the payment system.¹¹⁸ This is determined by the need for a secure, privacy-preserving, and efficient payment system.¹¹⁹ Participating institutions can access different types of data depending on their verification and regulation tasks.¹²⁰ Such data governance in public infrastructure is

115. *Id.*

116. *Data Classification*, IMPERVA, <https://www.imperva.com/learn/data-security/data-classification/> (last visited Feb. 9, 2023).

117. *See id.*

118. *See* Richard Rohena, *Understanding PCI DSS Scope: Definition and Guide*, GLOBAL PAYMENTS INTEGRATED, <https://www.globalpaymentsintegrated.com/en-us/blog/2020/03/18/understanding-pci-dss-scope> (last visited Feb. 9, 2023).

119. *See* Craig Stedman, *What is Data Governance and Why Does it Matter*, TECH.TARGET, <https://www.techtarget.com/searchdatamanagement/definition/data-governance> (last visited Feb. 9, 2023).

120. *See generally* Federal Trade Commission, *How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm Leach Bliley Act*, FEDERAL TRADE COMMISSION, <https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act>. (last visited Feb. 9, 2023); *see also* U.S. Government Accountability Office, *Why Do Banks Share Your Financial Information and Are They Allowed To?*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, (Dec.

different from the data transfer between businesses because the social, economic and even political function of these public facilities necessarily depends on the data sharing of all operators and stakeholders.¹²¹ The payment ledger is a public good which streamlines key financial, economic, and regulatory activities among central banks, commercial banks, exchanges, and other payment institutions.¹²²

The principle of data access and control is that the scope of access and control should correspond to the secure operation of the digital payment system. Whereas transactions at a small value may remain anonymous, large-amount transactions should be disclosed to the central bank and other payment service providers. Users should be able to transact outside of KYC regulations if the amount of transaction is small. The payer's identity should be hidden from a merchant, like paying with cash. But law enforcement should be able to determine a person's holding, even if only approximately.

The information about transaction details available to a payer's payment service provider shall depend on the situation. Closely cooperating central banks and payment institutions may work on a common ledger.¹²³ If a central operator is governing, regulating, and processing cross-border payments and settlements between central banks and payment institutions, it should simultaneously be responsible for managing the data. The central operator could bring more efficient organizational structure and dispute resolution mechanisms with the central payment operator grasping the whole scene of cross-border payments. With less centralization, the central overseer may not perform the payment and clearance function, but only to ensure

9, 2020), <https://www.gao.gov/blog/why-do-banks-share-your-financial-information-and-are-they-allowed>.

121. See generally Douglas J. Elliot et al., *Rethinking Data Governance*, OLIVER WYMAN, <https://www.oliverwyman.com/our-expertise/insights/2020/apr/risk-journal-vol-9/emerging-risks/rethinking-data-governance.html> (last visited Feb. 9, 2023).

122. See Tobias Adrian et al., Comment, *A Multi-Currency Exchange and Contracting Platform* 6, International Monetary Fund, Working Paper No. 22/117 (forthcoming Nov. 2022).

123. Tobias Adrian & Tommaso Mancini-Griffoli, *Bullet Train*, INT'L MONETARY FUND-FINANCE & DEV. (Sept. 2022), at 23.

that the payments are carried out effectively and diligently. In both situations, the central ledger keeper will play a decisive role in managing the ledger and the data. The data will be kept secret and properly stored at a centralized database for digital currency service providers to evaluate risks regarding the integrity, security, and finality of payments.

Below the overarching payment operator, central banks can validate transactions on the ledger, perform key regulatory tasks such as monitoring banks wallets and transactions in real-time, set threshold limits for their currency, and reduce the balance of commercial banks with holdings above the limits. Central banks can view or collect the data for regulation and policymaking purposes. Previous transaction data can be used to develop AML and CFT detecting models to impose more efficient, accurate, and automated blockage of illegal transactions.

Authorized banks and other financial institutions can act as settlement agents on behalf of their clients for retail transactions and use the same or alternative infrastructure for wholesale payments. Commercial banks and exchanges submit transactions to the ledger, provide automated reporting to comply with local regulations, and verify transactions submitted to the ledger. In cross-border trade settlements, remittance banks also have the obligation to screen AML, and hence they should understand the underlying trade details such as sales contracts, invoices, and proof of delivery. Other involved institutions, like a third-party aggregator, will offer merchants and customers the connection to payment service providers who have no agreements between them. Merchants or customers can submit and request transactions to the ledger, but the access to data is limited to their own transactions.

Other requirements include that the collection of data should remain confidential. The storage of data should provide adequate data availability on demand. Data sharing should be limited to the specific use and be verifiable by the receiver. Data transmission should guarantee data integrity.

3. Data Portability

The third important aspect of data sharing is users' right to data portability,¹²⁴ which empowers data subjects to control their data. Data subjects can ask the current data controller to transfer the data gathered, stored, and processed to another controller in a structured, commonly used, and machine-readable format without hindrance from the current controller.¹²⁵

Under the GDPR, data portability only applies to personal data that is processed by automated means, excluding additional information created from the information provided and pseudonymized data.¹²⁶ Nor does data portability apply to controllers whose lawful basis for processing is necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller.¹²⁷ The right to data portability should not adversely affect the rights and freedoms of others.¹²⁸ If the requested data was provided by multiple data subjects, such as a joint bank account, the portability applicant needs to seek agreement from all parties involved.¹²⁹ Where the service offered by the controller to the individual involves processing personal data about others, for example, a webmail service that includes a directory of contracts, then the controller should, on request, transfer all such data included in the service to the new provider.¹³⁰

If a controller is subject to sector-specific legislation which includes portability obligations, these legal requirements should prevail over the GDPR. As the right to data portability is applied to money and payment, decentralized monetary systems, such as cryptocurrencies and CBDCs, give users more control over their

124. General Data Protection Regulation, Art. 20, Right to Data Portability, (Eur. Union).

125. *Id.*

126. *Id.* at 1(b).

127. General Data Protection Regulation, Art. 6(1)(e), Lawfulness of Processing, (Eur. Union).

128. *Right to Data Portability*, INFO. COMM'R'S OFF., <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/> (last visited Feb. 9, 2023).

129. *Id.*

130. *Id.*

data and assets. Payment service providers should observe Europe's second payment services directive (PSD2) when providing banking account history to account information service providers.¹³¹ While PSD2 encourages competition and innovation in different products and services and creates access to personal data so that third parties can enter the payments market, it should be obeyed in line with the data protection standards in the GDPR. For instance, data processing and portability are all based on users' consent. Systems providing local storage of the monetary asset, accompanied by offline peer-to-peer transfer capabilities, should give the user more freedom to hold and reuse the asset by controlling the data therein. Such data portability can occur both vertically and horizontally.¹³² That is, it can happen in the data transfer with upstream service providers, or between rival payment service providers.

C. *Technical Proposals for Interoperability, Privacy and Security*

Having the technological capacity to receive data is not the same as interoperability at the data layer.¹³³ Hence, technical design should be paid sufficient attention as it demonstrates how both law and technologies are playing constitutive roles in designing a payment system, bearing normative values and policy considerations in its operation. And there are inherent different data access profiles of different techniques.¹³⁴ This technical implementation is a holistic project, ranging from unified data formats, digital identity, consensus protocol, connected layer, communication mechanism and data access control.¹³⁵

131. Douglas W. Arner et al., *The Future of Data-Driven Finance and RegTech: Lessons from EU Big Bang II*, 25 STAN. J. OF L., BUS. & FIN. 245, 264–65 (2020).

132. Chris Riley, *Unpacking Interoperability in Competition*, 5 J. OF CYBER POL'Y 94, 95, 97 (2020).

133. Stephen O'Connor, *What is Interoperability, and Why Is It Important?*, Advanced Data Systems Corporation (May 30, 2017), <https://www.adsc.com/blog/what-is-interoperability-and-why-is-it-important>.

134. See Riley, *supra* note 133, at 102–03.

135. See generally Emma McGuigan et al., *Value Untangled*, Accenture (2020), <https://www.accenture.com/content/dam/accenture/final/capabilities/technology/software-engineering/document/Accenture-Executive-Summary-IPS-Ecosystem-ITL-12-21.pdf>.

1. Standardized Data Formats and Protocol

To facilitate data flow and usage, data formats should be standardized. Standard-setting of data formats, when mandated through the enforcement or regulatory action, will require active monitoring and enforcement,¹³⁶ clearly defined decision-making power and dispute resolution approaches, and funding decisions on the implementation of standards.¹³⁷ Data should be aggregated and reported for real-time analysis, as part of the compliance and regulation process.¹³⁸ Reporting templates should be harmonized for systemically important financial institutions for better supervision.¹³⁹

Central banks and governments should use common language and protocol to bridge different ledgers and technologies.¹⁴⁰

Linguistic diversity comes at a considerable economic cost.¹⁴¹ A common language has been found to increase dramatically bilateral trade between countries by more than 40%.¹⁴² In payment transactions, different terminologies used in systems may serve the same function.¹⁴³ Therefore, the message format and key terms used should be aligned to save transaction costs and regulatory costs. This has been experimented in

136. Jan Krämer et al., MAKING DATA PORTABILITY MORE EFFECTIVE FOR THE DIGITAL ECONOMY: ECONOMIC IMPLICATIONS AND REGULATORY CHALLENGES 79 (Centre on Regulation in Europe 2020).

137. See generally *id.* at 33, 82.

138. Douglas W. Arner et al., *The Emergence of Regtech 2.0: From Know Your Customer to Know Your Data*, 44 J. OF FIN. TRANSFORMATION 79 (2016).

139. See Basel Committee on Banking Supervision, PRINCIPLES FOR EFFECTIVE RISK DATA AGGREGATION AND RISK REPORTING (Bank for International Settlements 2013).

140. Darrell Duffie et al., CENTRAL BANK DIGITAL CURRENCY: PRINCIPLES FOR TECHNICAL IMPLEMENTATION 11 (2021).

141. ANDREW G. HALDANE, TOWARDS A COMMON FINANCIAL LANGUAGE. "Speech at the Securities Industry and Financial Markets Association (SIFMA) 'Building a Global Legal Entity Identifier Framework' Symposium." New York, 14 Mar. 2012.

142. Chang Hoon Oh et al., *International Trade, Foreign Direct Investment, and Transaction Costs in Languages*, 40 J. OF SOCIO-ECONOMICS 732, 734 (2011).

143. See generally Committee on Payment and Settlement Systems, A GLOSSARY OF TERMS USED IN PAYMENTS AND SETTLEMENT SYSTEMS (Bank for International Settlements 2003).

international funds transfer.¹⁴⁴ The SWIFT system claimed to start its migration to ISO 20022 from the MT messaging format in November 2021,¹⁴⁵ given that 52% of the volume and 25% of the value of high-value payments are formatted to be ISO 20022 compliant.¹⁴⁶ Likewise, states should adopt a harmonized version of message formats and common rules of mapping and converting data between different data formats.¹⁴⁷

2. Interoperable Digital Identity

Maintaining interoperable digital identities is a crucial foundation of the payment network. Interoperable IDs contribute to the correctness, credibility, and finality of payment in a chain of transactions.¹⁴⁸ A supernational digital ID can be used to represent an individual or entity, incorporating interpretable individual information.¹⁴⁹ These digital identities should be proved and validated at least at the initial registration and subject to potential verification and authentication in future payments. Notably, the term ‘identity’ can indicate personal attributes, claims, credentials, and attestation (third-party validation of a claim).¹⁵⁰ An applicable definition here is that the identity of a user is distributed in different partial identities which are valid only in a specific context.¹⁵¹ It is essential to

144. See generally Committee on Payment and Market Infrastructures, CORRESPONDENT BANKING (Bank for International Settlements 2016).

145. *Swift Community to Embark on Migration to ISO 20022 for Payments Traffic*, SWIFT (Sept. 25, 2018), <https://www.swift.com/news-events/news/swift-community-embark-migration-iso-20022-payments-traffic>.

146. *Swift ISO 20022 Migration Study*, SWIFT (Apr. 23, 2018).

147. See *Enhancing Cross-Border Payments: Stage 1 Report to the G20*, FIN. STABILITY BD. (Apr. 9, 2020), <https://www.fsb.org/wp-content/uploads/P090420-1.pdf>.

148. See generally *Defining and Measuring Payment Interoperability*, World Economic Forum (2022).

149. Danyaal Yasin, *The Future of Digital ID: What It Means For You*, YOTI (June 22, 2022), <https://www.yoti.com/blog/the-future-of-digital-id/>.

150. See Irma Šlekytė, *What is Identity Verification? Process, Methods, and Benefits*, NordVPN (Nov. 15, 2022), [https://nordvpn.com/blog/identity-verification/#:~:text=Digital%20identity%20verification%20is%20the,%2C%20a%20password%2C%20etc.\)](https://nordvpn.com/blog/identity-verification/#:~:text=Digital%20identity%20verification%20is%20the,%2C%20a%20password%2C%20etc.)).

151. See 7 MD SADEK FERDUOUS ET AL., IN SEARCH OF SELF-SOVEREIGN IDENTITY LEVERAGING BLOCKCHAIN TECHNOLOGY 103061 (2019) (holding that the identity of an

specify the domain and context for the identity which consists of many attributes and the corresponding purpose and values.¹⁵² Such adaptive digital ID will better protect personal privacy and commercial secrets but may be abused by financial crimes.¹⁵³

3. Common Layer and Access Through APIs

Payment interoperability and data governance coordination are established through the compatibility or interlink between different ledgers.¹⁵⁴ But at which layer the ledger is connected makes a difference to the system structure and thereby data governance. Decentralized governance structures have been considered in many cross-border CBDC experiments¹⁵⁵, like Project Jura,¹⁵⁶ and the “m-CBDC Bridge.”¹⁵⁷

The distributed ledger enables nodes in a network or arrangement to securely propose, validate and record state changes and updates to a synchronized ledger that

entity is distributed into different partial identities which are only valid within different domains of different enterprises).

152. See *id.* (holding that it is essential to specify the domain when mentioning a partial identity since the partial identity is only valid within a specific domain).

153. See *Uses of digital ID for preventing financial crime*, CONSULT HYPERION, 1-2 (May 27, 2021), <https://chyp.com/2021/05/27/uses-of-digital-id-for-preventing-financial-crime/> (explaining that while there are many benefits to digital ID, such as increased security and privacy, there are also increased risks when it comes to financial crimes).

154. See *Central bank digital currencies: system design and interoperability*, BANK FOR INTERNATIONAL SETTLEMENTS, 9 (Sept. 2021), https://www.bis.org/publ/othp42_system_design.pdf (explaining how in order to achieve interoperability and data governance coordination, the central banks within the CBDC system need to be compatible with each other).

155. See RAPHAEL AUER ET AL., CBDCs BEYOND BORDERS: RESULTS FROM A SURVEY OF CENTRAL BANKS 12-13 (Bank for International Settlements 2021) (explaining how some banks are already de-centralising and collaborating with each other on projects to facilitate cross-border payments).

156. *Swiss National Bank, Banque de France and Bank for International Settlements Innovation Hub collaborate for experiment in cross-border wholesale CBDC*, SWISS NATIONAL BANK, 1 (June 10, 2021), https://www.snb.ch/en/mmr/reference/pre_20210610/source/pre_20210610.en.pdf.

157. RAPHAEL AUER ET AL., MULTI-CBDC ARRANGEMENTS AND THE FUTURE OF CROSS- BORDER PAYMENTS 8-9 (Bank for International Settlements 2021).

is distributed across the network nodes.¹⁵⁸ The ledger is operationally relied upon proof (of identity, authorship and validity), consensus (on visibility, resolution and throughput), and contracts (for validation, embedding and legal integration).¹⁵⁹ In combination with these elements, the blockchain infrastructure is constructed with several layers.¹⁶⁰ From bottom infrastructure to top applications, the system typically consists of: hardware layer, data layer, network layer, consensus layer, and application layer. Layers differ in their functions and capabilities,¹⁶¹ subject to institutional and technical design. Generally, the lower the level of common infrastructure, the higher degree of data sharing will occur among system operators. This is because lower levels of system infrastructure are more likely to have compatible systems and standardized protocols for data exchange. This makes it easier and more efficient to share data and optimize system resources by avoiding redundant data collection and storage. Sharing data is also necessary to maintain compatibility and prevent disruptions in the overall system.

158. See David C. Mills et al., *Distributed ledger technology in payments, clearing, and settlement*, BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, at 10 (Dec. 2016), <https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf> (explaining that in a DLT arrangement, nodes are connected to each other enabling any entity to share and validate information with each other on a peer-to-peer basis).

159. See EMANUEL PALM, *THE PERFORMANCE, INTEROPERABILITY AND INTEGRATION OF DISTRIBUTED LEDGER TECHNOLOGIES* 11 (Lulea University of Technology 2019) (outlining the three elements of distributed ledgers).

160. See VIVEK ACHARYA ET AL., *ORACLE BLOCKCHAIN SERVICES QUICK START GUIDE* ch.1 ¶7 (PACKT 2019) (ebook), <https://subscription.packtpub.com/book/data/9781789804164/1/ch01lvl1sec07/layered-structure-of-the-blockchain-architecture>, (outlining the 5 layers of blockchain infrastructure).

161. See *id.* (showing the differences in the functions of each layer).

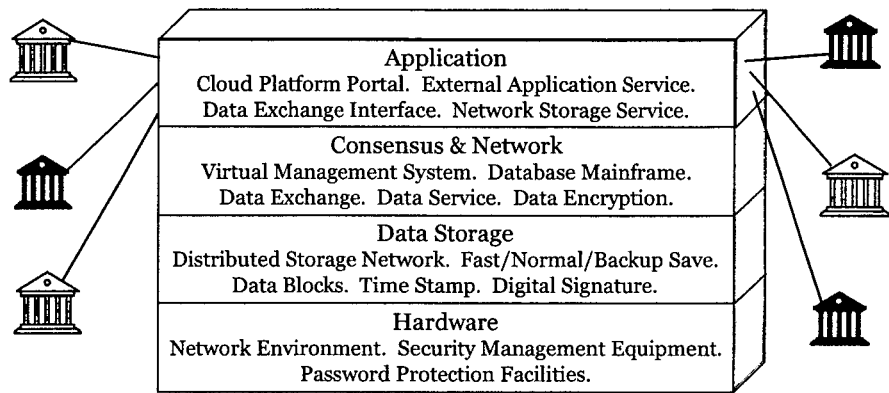


Figure 2. Payment System Layers and the Level of Connection

Domestic CBDC systems are connected to the designated layer or ledger for cross-border payments.¹⁶² Access to the common layer can be accomplished through APIs, a set of definitions and protocols for integrating application software and allowing for the data flow between the system in a controlled fashion.¹⁶³ Standardized APIs will enhance the delivery of financial services to both retail consumers and business customers, enable continuous data portability to encourage more organizations to import personal data, and encourage more users to initiate such transfers.¹⁶⁴ Open banking APIs could simplify the procedures of cross-border payments and increase financial inclusion for small and medium-sized enterprises by making

162. See generally *Central bank digital currencies: foundational principles and core features*, BANK FOR INT'L SETTLEMENTS, 12 (2020), <https://www.bis.org/publ/othp33.pdf> (explaining that in a CBDC system, payments between banks are recorded on ledgers).

163. See Laura Brodsky and Liz Oakes, *Data sharing and open banking*, MCKINSEY & COMPANY, 1 (Sept. 5 2017), <https://www.mckinsey.com/industries/financial-services/our-insights/data-sharing-and-open-banking> (explaining how an API allows for the flow of data between systems in a controlled fashion).

164. See *id.* (explaining how APIs have enhanced the delivery of financial services); See Jan Krämer et al., *Making Data Portability More Effective For The Economy*, CTR. ON REGUL. IN EUR. 11 (June 2020), https://cerre.eu/wp-content/uploads/2020/07/cerre_making_data_portability_more_effective_for_the_digital_economy_june2020.pdf (explaining the benefits of standardized APIs).

lending processes faster and more reliable.¹⁶⁵ Through a ledger interoperability protocol, contract language, and synchronization protocol can guarantee that data is reliably shared with entitled parties in a way that is correct and reliable, even in the presence of malicious actors.¹⁶⁶

As to the right to data portability, an open-source, service-to-service data portability platform can be created so that all individuals across the web can easily move their data between online service providers.¹⁶⁷ The platform may use the services' existing APIs and authorization mechanisms to access data.¹⁶⁸ "It then uses service-specific adapters to transfer that data into a common format, and then back into the new service's API."¹⁶⁹ Besides, users can share their data in the network without losing control and ownership of it. Through a blockchain repository, they "can track who shared what, with whom, when, by what means and for what purposes" in a verifiable fashion.¹⁷⁰

4. Privacy and Security

To protect data security, the data exporter may split the data before transmission, "in a way that no individual processor receives suffices to reconstruct the personal data in whole or in

165. See *The Next Phase of the Banking Open API Journey*, Hong Kong Monetary Authority, 39 (2021), https://www.hkma.gov.hk/media/eng/doc/key-functions/ifc/fintech/The_Next_Phase_of_the_Banking_Open_API_Journey.pdf (explaining how open banking APIs could increase financial inclusion by making lending processes faster and more reliable).

166. See *Canton*, DIGITAL ASSET, <https://www.canton.io> (last visited Feb. 9, 2023) (showing an example of a ledger interoperability protocol called Canton, and the advantages that come with using it).

167. See generally DATA TRANSFER PROJECT, <https://datatransferproject.dev/> (last visited Feb. 9, 2023) (showing an example of an open-source, service-to-service data portability platform called the Data Transfer Project, which allows individuals to move their data between online services as they wish).

168. See *id.* (explaining how Data Transfer Project uses existing APIs and authorization mechanisms to access data).

169. DATA TRANSFER PROJECT, <https://datatransferproject.dev/> (last visited Dec. 13, 2021).

170. Ajay Kumar Shrestha et al., *A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives*, FRONTIERS IN BLOCKCHAIN, Oct. 22, 2020, at 1.

part.”¹⁷¹ “The data exporter receives the result of the processing from each of the processors independently, and merges the pieces received to arrive at the final result which will constitute personal or aggregated data.”¹⁷² During the transmission, the system may hire a third-party notary for the authentication of information across ledgers.¹⁷³ Without these third-party transmitters, system participants may use an inter-ledger protocol to enable communication between different ledger payment systems, hash-locking for direct communication between ledgers, sidechains, or relays that validate data from other blockchains, and application layer adaptors for communication between multiple software applications.¹⁷⁴

In this communication process, privacy should be embedded in the digital infrastructure and building blocks.¹⁷⁵ The tighter encryption imposed on the data subject identity, data communication, storage, and transfer, the larger scope of data sharing can be allowed in the system.¹⁷⁶ Personal information and important data can be anonymized before and during transmission.¹⁷⁷

Anonymization can make the data unrelated to an identified or identifiable person so as not to constitute “personal data.”¹⁷⁸ The effect of anonymization is that the individual cannot be singled out from the data, the records of an individual are

171. Privacy Maverick, *Diagramming Data Transfers*, PRIVACY MAVERICK (Dec. 7, 2021), <https://privacymaverick.com/diagramming-data-transfers/>.

172. *Id.*

173. Dr. Ahmed Mansour et al., *Strategies for Adopting DLT/Blockchain Technologies in Arab Countries*, 1-68, 26 (Arab Monetary Fund, Working Paper No. 167, 2021).

174. *Id.* at 27–29.

175. *New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations*, at 40, COM (2017) 134 final (Mar. 23, 2017).

176. *Encryption*, EDUCAUSE, <https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/encryption> (last visited Feb. 13, 2022).

177. *Guidelines for Data De-Identification or Anonymization*, EDUCAUSE (July 2015), <https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/guidelines-for-data-deidentification-or-anonymization>.

178. *Id.*

unlinked, and other information about the individual cannot be inferred from the data.¹⁷⁹ Pseudonymization aims at the function that the data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the assistance of additional information.¹⁸⁰

Using encryption techniques, access to information can be conditional and selective, only by authorized and verified entities, limited to the information necessary for a specific task.¹⁸¹ The strength of the encryption could consider the specific period during which the confidentiality of the encrypted personal data must be preserved, and implemented by properly maintained software in conformity with the specific task of the algorithm.¹⁸² Data can be dynamically masked to eliminate time-consuming manual processing.¹⁸³ Dynamic data masking shields confidential information in production data in real-time, without making physical changes to the data set, and prevents data requesters from accessing sensitive information.¹⁸⁴

Multi-party computation¹⁸⁵ and zero-knowledge proof¹⁸⁶ can be used to share data at an only necessary level without sharing sensitive information.¹⁸⁷ For example, threshold cryptography

179. Council Regulation 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, and Repealing Directive 95/46/EC, art. 26, 2016 O.J. (L 119) 1 (EU).

180. *Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, at 31 (June 18, 2021), https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf.

181. Olivia Gonzalez, *Cracks in the Armor: Legal Approaches to Encryption*, 2019 ILL. J. L., TECH. & POL'Y 1, 8–9 (2019).

182. European Data Protection Board, *supra* note 60, at 30.

183. IMMUTA, <https://www.immuta.com/product/secure/orchestration-dynamic-data-masking/> (last visited Dec. 13, 2021).

184. *Id.*

185. ASSAF BEN-DAVID ET AL., FAIRPLAYMP – A SYSTEM FOR SECURE MULTI-PARTY COMPUTATION 257 (2008), <https://dl.acm.org/doi/10.1145/1455770.1455804>.

186. *Id.* at 258.

187. Victor Shilo, *Zero-Knowledge Proof: Protecting Your Personal Information Without Sacrificing Open Data*, FORBES (Feb. 3, 2022), <https://www.forbes.com/sites/forbestechcouncil/2022/02/03/zero-knowledge-proofprotecting-your-personal-information-without-sacrificing-open-data/?sh=263586ef6eb5>.

can be used to allow for access to data only after parties more than the threshold number cooperate in the decryption or signature protocol.¹⁸⁸ The private key is distributed among several decryption servers so that at least some servers are needed for decryption.¹⁸⁹ The keys should be reliably managed, including its generation, administration, storage, link to the identity of the intended recipient, and revocation, by the exporter or an entity trusted by the exporter under a jurisdiction offering an essentially equivalent level of protection.¹⁹⁰ Data in the interoperable ledger system can be processed jointly by many independent processors in different jurisdictions without disclosing the content of the data.¹⁹¹

For congregate protection, the regulator may set up a firewall for digital money-related information and strictly implement privacy protocols, without interfering with the central bank's access and control of the data.¹⁹² As to the most sensitive data, automated erasure will guarantee that only data necessary for instant payment is transferred without leaving long-lasting records and thus information about the financial situation of the payee.¹⁹³

188. *Threshold Cryptosystem*, WIKIPEDIA, https://en.wikipedia.org/wiki/Threshold_cryptosystem (last visited Feb. 27, 2022).

189. Dan Boneh, et al., *Chosen Ciphertext Secure Public Key Threshold Encryption Without Random Oracles*, SPRINGER TOPICS IN CRYPTOLOGY – CT RSA 1, 1 (2006).

190. *Recommendations on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data*, EUR. DATA PROT. BD. (Jun. 18, 2021), https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo20_supplementarymeasurestransferstools_en.pdf.

191. *Inclusive Deployment of Blockchain for Supply Chains: Part 6 – A Framework for Blockchain Interoperability*, WORLD ECON. F. (Apr. 2020), https://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf.

192. *Firewall (computing)*, WIKIPEDIA, [https://en.wikipedia.org/wiki/Firewall_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing)) (last visited Feb. 27, 2022).

193. See Shuja Kahn, *Automate and Schedule Data Erasure Tasks to Maintain Privacy*, BITRASER BLOG (Mar. 28, 2022), <https://www.bitraser.com/blog/automate-and-schedule-data-erasure-tasks-to-maintain-privacy/> (Automated eraser helps maintain data privacy by regularly wiping data files).

V. CONCLUSION

A cross-border CBDC system is an integrated organism constituted by legal rules and digital programming, which are inextricably linked. The various elements comprising the payment system, such as security measures, privacy protection, centralized or decentralized organization structure, interact and couple with each other to make the system secure, stable, and efficient. Design features of digital money affect the functionality of cross-border payments in crucial aspects to achieve broader public interest and sustainable development goals.¹⁹⁴ Most of the current cross-border payment models are established upon application connections that are executed through several parts, including direct application program interface connections, a central switch, and a third-party aggregator or moderator.¹⁹⁵ Newly emerged technologies, by contrast, allow for system interoperability in new forms. For instance, blockchain allows for the access to and sharing of data in more transparent and accountable ways. Users and payment institutions can access data and services through the internet. Authorized institutions can save files to a remote database and retrieve them on demand.

Since digital money and data are indivisible in a digital payment system, data governance arrangements are essential for more efficient and accessible cross-border payments. Digital money interoperability offers a prototype of data involving public interest that should be dealt with. The principle of transnational data governance is that data should be properly used for market integrity, fair competition, beneficial innovation, and consumer welfare.¹⁹⁶ Data sharing is not a binary choice of data blockage or unconditional sharing. Regulators have a range of choices around the type of data to keep confidential, who to keep it secret from,

194. See Tao Zhang, *New Forms of Digital Money: Implications for Monetary and Financial Stability*, INT'L MONETARY FUND (Oct. 30, 2020), <https://www.imf.org/en/News/Articles/2020/10/30/sp103020-new-forms-of-digital-money>.

195. See *Exploring Multilateral Platforms for Cross-Border Payments*, BANK FOR INT'L SETTLEMENTS (Jan. 2023), <https://www.bis.org/cpmi/publ/d213.pdf>.

196. See *Recommendation of the Council on Enhancing Access to and Sharing of Data*, OECD LEGAL INSTRUMENTS (May 10, 2021), <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463>.

in what situations, and for what purposes. It is useful to recognize the heterogeneity of data categories and understand their importance, and the identify the scope of data sharing in different contexts.

As to specific data sharing arrangements, regulators should apply different technologies to fulfill these data protection rules regarding different types of data. Here the constitutive role of technology is often underplayed; technology is not merely a passive implement of the above legal rules, but an active infrastructure that makes the whole set of activities and legal design possible. By the time the public infrastructure is being designed, data layer and the ability of interconnected systems should consider the scope of data sharing. Encryption, decentralized transmission networks, and open APIs make possible the separation between general ownership and the right to use, manage, and transfer.¹⁹⁷ In other words, the storage and control of data can be secured while allowing the value of data to be exploited. Encryption techniques have also made data sharing and the realization of socio-economic functions no longer an either-or situation where the information is either fully known by one party or not. Restricted disclosure and knowledge-delivery allow for appropriate scopes of data sharing in line with specific payment tasks.

197. See Adam Hayes, *Blockchain Facts: What Is It, How It Works, and How It Can Be Used*, INVESTOPEDIA (Sep. 27, 2022), <https://www.investopedia.com/terms/b/blockchain.asp>; See *Interlinking Payment Systems and the Role of Application Programming Interfaces: A Framework for Cross-Border Payments*, BANK FOR INT'L SETTLEMENTS (Jul. 2022), <https://www.bis.org/cpmi/publ/d205.htm>.

