Permissioned Distributed Ledger Technology in Banking Compliance: Implementation Context and Use-Case Dependencies

Zhenkun Weng[1]

Abstract

Permissioned distributed ledger technology (DLT) is increasingly being proposed for regulated banking, yet its feasibility hinges on whether distributed recordkeeping can meet compliance requirements for auditability, operational resilience, and accountability. This article evaluates permissioned distributed ledger technology (DLT) through three compliance-intensive use cases-interbank settlement, shared know your customer (KYC) utilities, and credit information sharing-and situates the discussion in the Chinese banking context using sector indicators of declining return on assets and rising non-performing loan ratios. It specifies the compliance dependencies that each workflow must satisfy, including legally meaningful settlement finality, audit-quality authorization trails, privacy-preserving identity and data governance, and supervision-compatible access and governance arrangements. This article offers a focused conceptual synthesis of peer-reviewed research across banking, audit, information systems, and financial regulation, using Chinese sector indicators as contextual motivation rather than causal evidence. The contribution is a use-case grounded translation of permissioned-DLT design choices into assessable compliance dependencies for banks, auditors, and supervisors, clarifying why blockchain adoption in banking should be treated as a redesign of evidence and governance rather than as a plug-and-play IT upgrade.

Keywords: Permissioned DLT, Banking compliance, KYC, AML, Settlement finality, Auditability

1 Introduction

Banks face an increasingly exacting compliance environment in which routine frictions have become a material source of cost, delay, and operational exposure. Customer due diligence is repeatedly performed across products, legal entities, and jurisdictions, resulting in duplicate know-your-customer (KYC) files that are expensive to maintain yet often inconsistent in quality and timeliness. At the same time, anti-money laundering (AML) obligations push banks toward documentation-heavy processes that can drift into “check-the-box” behavior, even as supervisors expect demonstrable risk sensitivity and traceable decision rationales (El Yacoubi, 2020; Masciandaro & Filotto, 2001). These pressures are not confined to onboarding. They extend across ongoing monitoring, periodic refresh, recordkeeping, and internal escalation, all of which must be auditable under examination and defensible in enforcement

[1] Master student of 学校名字 University of Macau,， Major: Data Strategy and Compliance Management; Eemail:charleszhenkun@hotmail.com

contexts (Magnusson, 2009). Empirical and doctrinal work in financial crime compliance has therefore converged on a core diagnosis: compliance failure risk is frequently less about the absence of rules than about the difficulty of producing coherent, institution-wide, regulator-legible evidence from fragmented information systems and interdependent processes (Chitimira & Munedzi, 2023; ElYacoubi, 2020; Korpela, 2025; Masciandaro & Filotto, 2001).

These frictions interact with a second set of constraints that are central to banking supervision but often treated separately in technology discussions, including auditability, operational risk, and cross-border settlement finality (Dai & Vasarhelyi, 2017; Parra Moyano & Ross, 2017). Auditability is not merely the capacity to store records; it is the ability to demonstrate, ex-post, who knew what, when they knew it, which controls fired, and which exceptions were granted, across distributed teams and outsourced functions. Operational risk, in turn, is amplified by process complexity, third-party dependencies, and IT change, making "control effectiveness" as important as control design. Cross-border payments add further layers, multiple intermediaries, reconciliation steps, and jurisdictional handoffs, increasing settlement latency and uncertainty over finality, complicating sanctions screening, transaction monitoring, and post-event reconstruction. For these reasons, the compliance promise of distributed ledger technology (DLT) is not that it is inherently transformative, but that a shared, append-only record and standardized state transitions could reduce duplicative verification, support richer audit trails, and constrain certain error paths if embedded within banking-grade controls (Kahn & Roberds, 2007; Schmitz & Leoni, 2019).

A journal-relevant context for this discussion is the growing experimentation with permissioned, consortium-based DLT. In banking settings, permissioning is not a cosmetic choice; it is a compliance architecture. It determines who can write to the ledger, who can read sensitive fields, how identities are verified, how governance rights are allocated, and how exceptions and reversals are handled when legal or operational realities intrude on technical immutability (Lineros, 2021). These design choices bear directly on accountability, because "who is responsible" for a state transition may shift from a single institution to a network governed by rules, code, and joint decision rights. They also bear directly on supervision, because supervisory technology (SupTech) and regulatory technology (RegTech) increasingly rely on machine-readable reporting, continuous monitoring, and explainable evidence trails, none of which can be assumed to emerge automatically from a ledger deployment. In short, permissioned DLT sits at the intersection of information technology (IT) governance, audit and assurance practice, and supervisory design, and must be evaluated as such (McCarthy, 2022; Zeranski & Sancak, 2021).

However, the current literature does not adequately connect these elements in a way that is usable for banking compliance design. Research on blockchain in finance often emphasizes efficiency gains, transparency, or disintermediation, while leaving the control logic implicit or assuming that auditability follows from immutability. In parallel, legal scholarship on smart contracts and digital assets tends to debate enforceability and regulatory perimeter questions at a high level, without tracing how permissioned DLT alters the micro-foundations of compliance controls and supervisory access in

regulated intermediaries. Meanwhile, audit and accounting studies increasingly identify the governance and assurance implications of blockchain-based records, but rarely map ledger design properties to concrete banking compliance controls such as KYC refresh, sanctions screening evidence, exception management, and settlement finality attestations. The defensible gap, therefore, is an underdeveloped mapping from permissioned DLT technical properties to specific compliance risk controls and supervisory accountability arrangements that would meet banking-grade standards (Gomber et al., 2018; Rozario & Thomas, 2019).

This article focuses on three banking use cases-interbank settlement, shared KYC utilities, and credit information sharing-and specifies the compliance dependencies that determine whether permissioned DLT can be examined and sustained under regulation. Section 2 summarizes the permissioned-DLT model and the Chinese banking context (Figures 1 and 2). Section 3 analyzes each use case and distills implications for supervisors and consortium governance.

2 Conceptual and regulatory background

2.1 Distributed Ledger Technology in Banking: Opportunities and Constraints

Banks and regulators have turned their attention to distributed ledger technology (DLT), often epitomized by blockchain, as a potential solution for industry-wide information coordination. The conceptual appeal of blockchain in regulated banking is not about cryptocurrencies or eliminating intermediaries; rather, it lies in redesigning how data is shared and validated among trusted institutions. A permissioned DLT system can be seen as a consortium ledger or shared database that multiple banks jointly write to and read from, under agreed-upon rules. In principle, this promises a single, tamper-evident record of transactions or customer data that all relevant parties can refer to, reducing the inconsistencies and lags that plague the current siloed approach (Böhme et al., 2015; Tschorsch & Scheuermann, 2016). For compliance-heavy use cases, the permissioned, private blockchain model has emerged as the favored approach over public, permissionless networks. In a consortium or private blockchain, participants are vetted institutions, and access rights are carefully tiered. This permissioning is fundamentally a compliance-driven design choice; it enables alignment with legal accountability and data privacy requirements by controlling who can join the network, who can validate transactions, and how information is disseminated. Early pilots and studies have accordingly focused on use cases such as interbank payments and settlement, KYC data-sharing utilities, and credit information registries, where multiple institutions benefit from a shared record. In each scenario, the purported benefits include lower duplication of effort, faster processing, and enhanced transparency or traceability (Böhme et al., 2015; Catalini & Gans, 2020; Lamport et al., 1982; Tschorsch & Scheuermann, 2016).

2.2 Implementation Context in Key Use Cases

Chinese commercial banks' average return on assets (ROA) declined markedly in the mid-2010s, reflecting a narrowing of interest margins and increased competition. This profitability squeeze has put

pressure on banks to streamline operations and cut costs, lending urgency to efficiency-improving innovations in areas like payments and settlement. Interbank payments and clearing, in particular, involve costly frictions under conventional systems, multiple ledgers, duplicative reconciliations, and delayed finality, which a shared ledger approach aims to reduce. In this context, lower margins (as illustrated in Figure 1) amplify the incentive to adopt technologies that can save time and resources in transaction processing. A permissioned DLT platform for interbank settlement could, for example, eliminate certain manual reconciliation steps and provide near-instant finality, thereby improving operational efficiency under high profit pressures. At the same time, such a platform would need to ensure that faster settlement does not compromise control objectives – faster processing must be accompanied by equally rigorous real-time risk screening and exception handling to maintain compliance standards (Allen & Santomero, 2001; Kahn & Roberds, 2007; Tan, 2016).

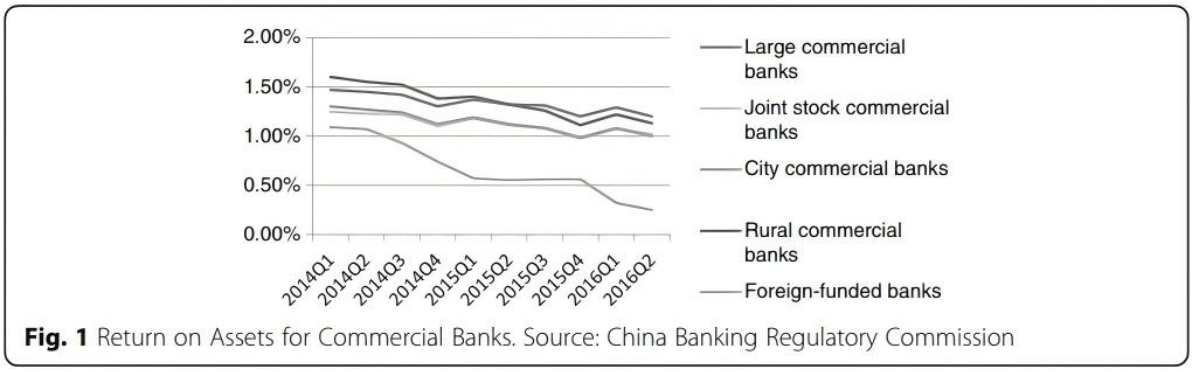

Fig. 1 Return on assets for commercial banks

Non-performing loan (NPL) ratios in China's banking sector rose during the same mid-2010s period, signaling deteriorating credit quality and heightened risk in banks' loan portfolios. This trend (shown in Figure 2) underscores the need for better credit risk data and inter-bank cooperation in monitoring exposures. Fragmented credit information systems have historically hampered banks' ability to assess borrower risk; one bank might not promptly know whether a borrower has defaulted at another bank, or might lack access to a borrower's holistic debt profile. Distributed ledger technology has been proposed as a solution to improve credit data sharing and accuracy. A permissioned blockchain could host a tamper-evident registry of credit histories and loan collateral that all lending institutions update and consult in real time. If designed with appropriate privacy and governance controls, such a system could help identify emerging credit risks earlier and reduce information asymmetry among lenders (Cong & He, 2019; García-Herrero et al., 2009). The increase in NPLs shown in Figure 2 illustrates why improving the timeliness and completeness of credit information is critical. A DLT-based credit information network might, for instance, log each loan origination and delinquency event with digital signatures from the responsible institution, creating an industry-wide view of borrower indebtedness and repayment behavior. Regulators could also gain a more aggregated and up-to-date perspective on systemic credit risk through direct access to this shared ledger, enhancing macro-prudential supervision. However, as with other use cases, the efficacy of a blockchain solution for credit data depends on data quality, data format standardization, and clear legal agreements on data usage and liability (Djankov et

al., 2007; Pagano & Jappelli, 1993). Without high-quality data and robust error-correction mechanisms (to handle mistaken or fraudulent entries on the ledger), merely "blockchaining" credit information would not automatically improve credit outcomes. Thus, rising NPLs provide a strong motivation for DLT-based innovation in credit reporting, while also highlighting the importance of complementary data governance reforms to ensure that any new system truly bolsters credit risk management (Jappelli & Pagano, 2002).

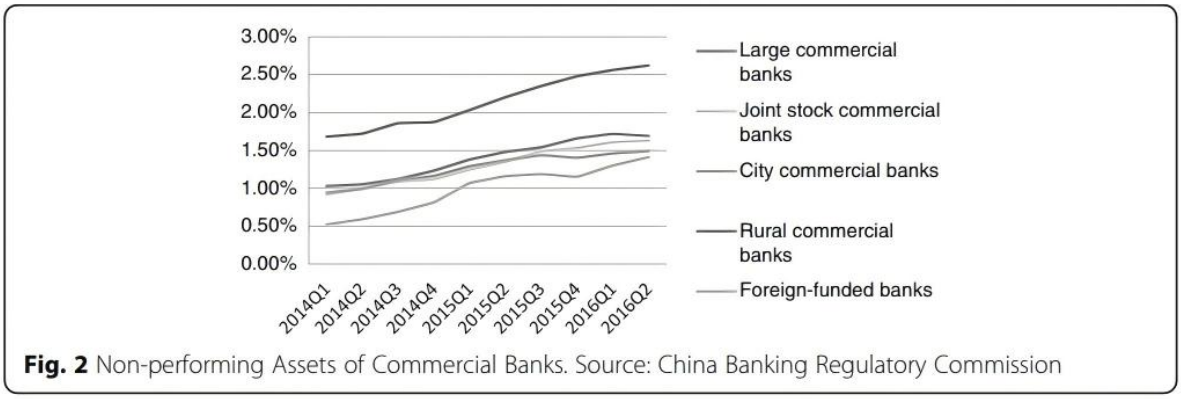

Fig. 2 Non-performing assets of commercial banks

3 Banking blockchain use cases and compliance dependencies

In regulated banking, the practical significance of blockchain is best evaluated through specific use cases, because the relevant unit of analysis is the control environment that surrounds a business process. Banking infrastructure is not merely a transaction pipe; it is a compliance system that must generate defensible evidence for audits and supervisors while sustaining operational resilience and clear accountability. A use-case lens, therefore, foregrounds the key question for permissioned DLT: which compliance dependencies must be satisfied for a given workflow to be examinable, contestable, and legally sustainable once recordkeeping and execution become distributed (Gomber et al., 2018; Yermack, 2017).

3.1 Interbank payments, clearing, and settlement

Interbank payments, clearing, and settlement illustrate why technical architecture cannot be separated from compliance and legal finality. Conventional settlement chains involve multiple institutions and ledgers, producing reconciliation tasks and time lags that are not only costly but also compliance-relevant, because sanctions screening, fraud detection, and ex post investigation depend on coherent, time-ordered evidence across intermediaries. Permissioned DLT is often proposed as a shared state machine for interbank obligations, potentially reducing duplicated recordkeeping and providing a single reference record for confirmation and settlement. However, the compliance dependencies are stringent; the system must support legally meaningful settlement finality, preserve audit-quality evidence of state transitions and authorizations, remain resilient under operational disruption, and specify accountability for validation and exception handling in a multi-institution setting. These requirements link the economics of settlement and finality to organizational risk control and governance design

(Chitimira & Munedzi, 2023; Dai & Vasarhelyi, 2017; Kahn & Roberds, 2007).

A central compliance dependency in this use case is the relationship between faster settlement and control timing. When settlement windows compress, ex ante controls such as sanctions screening and transaction monitoring must either be automated reliably or complemented by robust exception management, because post-settlement remediation can be legally and operationally constrained (ElYacoubi, 2020; Rozario & Thomas, 2019). At the same time, regulators and internal audit functions require evidence that controls operated as intended, including logs of approvals, overrides, and reconciliation actions. Permissioned DLT can strengthen evidentiary integrity by making process events more consistently recorded, but only if identity binding, authorization rules, and data visibility are designed so that "who did what, when, and under which authority" is reconstructable without exposing confidential business data. In this sense, interbank DLT is simultaneously a payments innovation and an audit redesign problem, aligning technical immutability with accountability and assurance practices (Kahn & Roberds, 2007; Rozario & Thomas, 2019; Schmitz & Leoni, 2019).

3.2 Shared KYC and identity utilities

Shared KYC and identity utilities represent a second high-value use case because they directly address one of banking's most enduring compliance frictions: repetitive customer due diligence and fragmented identity records across institutions. Academic work on AML compliance has long noted that compliance costs and procedural burdens can be substantial, and that institutions often duplicate verification and monitoring efforts because legal responsibility remains institution-specific even when customers are shared across markets (De Filippi & Wright, 2018; Masciandaro & Filotto, 2001). A permissioned DLT-based KYC utility aims to reduce duplication by enabling authorized institutions to reference, attest to, and update validated identity attributes and due diligence artifacts within a shared governance framework. The compliance dependencies, however, are as important as the efficiency logic; the utility must preserve traceability of who contributed which verification, support controlled updates and periodic refresh, and maintain record retention and audit trails that remain legible to internal audit and supervisors. The operational promise is therefore conditional on governance arrangements that allocate liability and on technical architectures that separate shared attestations from sensitive underlying documents (Arner et al., 2017; Magnusson, 2009; Parra Moyano & Ross, 2017).

Data protection and confidentiality constraints sharpen these dependencies. KYC involves highly sensitive personal and sometimes corporate information, which must be protected against unauthorized disclosure while remaining accessible for legitimate compliance and supervisory purposes. Permissioned DLT designs can support confidentiality through access control, data partitioning, and cryptographic techniques that enable verification without full disclosure, but these capabilities introduce governance burdens, including key management, permission administration, and accountable disclosure mechanisms (Werbach, 2018; Zyskind et al., 2015). The compliance challenge is therefore not simply privacy versus transparency; it is the construction of a defensible information governance regime in which data minimization, purpose limitation, and retention rules can be operationalized and audited across

institutions. In this setting, the design choice of putting raw data on-chain versus storing proofs or references off-chain becomes a compliance control decision with implications for audit evidence, dispute resolution, and liability allocation (Dai & Vasarhelyi, 2017; De Filippi & Wright, 2018; Werbach, 2018).

3.3 Credit information systems and data-sharing architectures

Credit information systems and data-sharing architectures provide a third use case in which DLT is frequently invoked to address fragmented data, low-quality records, and limited interoperability among institutions. A substantial literature in banking and financial economics shows that credit information sharing can improve screening and reduce default by reducing information asymmetries, yet it also raises governance concerns about data accuracy, strategic withholding, privacy, and the distribution of benefits among participants (Djankov et al., 2007; Padilla & Pagano, 2000). Permissioned DLT can, in principle, provide a shared infrastructure for logging consented queries, recording updates, and producing tamper-evident histories of who accessed which data and when. The compliance dependencies mirror those in KYC but are distinct in emphasis, accuracy and contestability of records become central, as does the ability to correct errors while preserving an auditable history, and the need to ensure that access and use of credit data remain aligned with lawful purposes and accountable decision-making. The value proposition depends less on “decentralization” than on enforceable governance for data quality and rights management in a multi-party environment (Brown & Petersen, 2009; Djankov et al., 2007; Jappelli & Pagano, 2002; Padilla & Pagano, 2000; Pagano & Jappelli, 1993).

Across these use cases, a consistent pattern emerges, permissioned DLT can reduce reconciliation and evidence fragmentation only when its technical properties are deliberately translated into compliance-relevant controls. Settlement applications require an explicit alignment of state transitions with legal finality and operational resilience; KYC utilities require a joint design of identity assurance, retention, and privacy-preserving auditability; and credit data sharing requires mechanisms for accuracy, correction, and accountable access (Arner et al., 2017; Dai & Vasarhelyi, 2017). These dependencies anticipate the paper’s risk taxonomy by revealing how finality, identity, and governance choices become compliance risk mechanisms. In other words, the most consequential design decisions in banking DLT are those that determine how evidence is produced, how responsibility is allocated, and how supervisors can verify compliance without undermining legitimate confidentiality (Arner et al., 2017; Dai & Vasarhelyi, 2017; Werbach, 2018; Yermack, 2017).

4 Conclusion

Permissioned DLT is most plausibly understood as a governance and evidence architecture for multi-party banking processes, not as a generic efficiency technology. The Chinese sector indicators in Section 2 illustrate why banks seek shared ledgers to reduce reconciliation and improve information sharing while supervisors remain attentive to credit and operational risks. Across interbank settlement, shared KYC utilities, and credit information sharing, the analysis identifies compliance dependencies that determine whether a workflow is examinable and legally sustainable. Settlement applications

require explicit alignment between state transitions and legally meaningful finality, together with audit-quality evidence of authorization and disciplined exception handling. Shared KYC utilities require privacy-preserving data governance, provenance of attestations, and liability allocation for stale or erroneous due diligence evidence. Credit information sharing requires mechanisms for accuracy, correction, and accountable access so that tamper-evidence does not substitute for data quality or lawful purpose limitation. For policy, permissioned-DLT pilots should be conditioned on consortium governance charters and evidence standards that support supervisory review, including authorization logs, access-control audit trails, and predefined exception pathways. Where direct supervisory access is contemplated, it should be engineered as a bounded capability compatible with confidentiality constraints and due process.

References

Allen, F., & Santomero, A. M. (2001). What do financial intermediaries do? *Journal of Banking & Finance*, *25*(2), 271-294. https://doi.org/https://doi.org/10.1016/S0378-4266(99)00129-6

Arner, D. W., Barberis, J., & Buckley, R. P. (2017). *FinTech and RegTech in a Nutshell, and the Future in a Sandbox*. CFA Institute Research Foundation.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, Technology, and Governance. *Journal of Economic Perspectives*, *29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213

Brown, J. R., & Petersen, B. C. (2009). Why has the investment-cash flow sensitivity declined so sharply? Rising R&D and equity market developments. *Journal of Banking & Finance*, *33*(5), 971–984. https://doi.org/https://doi.org/10.1016/j.jbankfin.2008.10.009

Catalini, C., & Gans, J. S. (2020). Some simple economics of the blockchain. *Commun. ACM*, *63*(7), 80–90. https://doi.org/10.1145/3359552

Chitimira, H., & Munedzi, S. (2023). An evaluation of customer due diligence and related anti-money laundering measures in the United Kingdom. *Journal of Money Laundering Control*, *26*(7), 127-137. https://doi.org/10.1108/JMLC-01-2023-0004

Cong, L. W., & He, Z. (2019). Blockchain Disruption and Smart Contracts. *The Review of Financial Studies*, *32*(5), 1754-1797. https://doi.org/10.1093/rfs/hhz007

Dai, J., & Vasarhelyi, M. A. (2017). Toward Blockchain-Based Accounting and Assurance. *Journal of Information Systems*, *31*(3), 5-21. https://doi.org/10.2308/isys-51804

De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.

Djankov, S., McLiesh, C., & Shleifer, A. (2007). Private credit in 129 countries. *Journal of Financial Economics*, *84*(2), 299-329. https://doi.org/https://doi.org/10.1016/j.jfineco.2006.03.004

ElYacoubi, D. (2020). Challenges in customer due diligence for banks in the UAE. *Journal of Money Laundering Control*, *23*(2), 527-539. https://doi.org/10.1108/JMLC-08-2019-0065

García-Herrero, A., Gavilá, S., & Santabárbara, D. (2009). What explains the low profitability of Chinese banks? *Journal of Banking & Finance*, *33*(11), 2080-2092. https://doi.org/https://doi.org/10.1016/j.jbankfin.2009.05.005

Gomber, P., Kauffman, R. J., Parker, C., & Weber, B. W. (2018). On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services. *Journal of Management Information Systems*, *35*(1), 220-265. https://doi.org/10.1080/07421222.2018.1440766

Jappelli, T., & Pagano, M. (2002). Information sharing, lending and defaults: Cross-country evidence. *Journal of Banking & Finance*, *26*(10), 2017-2045. https://doi.org/https://doi.org/10.1016/S0378-4266(01)00185-6

Kahn, C. M., & Roberds, W. (2007). Transferability, finality, and debt settlement. *Journal of Monetary Economics*, *54*(4), 955-978. https://doi.org/https://doi.org/10.1016/j.jmoneco.2006.06.005

Korpela, S. J. (2025). Between a rock and a hard place: managing the conflict between anti-money laundering and financial inclusion. *Journal of Money Laundering Control*, *28*(7), 65-80. https://doi.org/10.1108/JMLC-04-2025-0049

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Trans. Program. Lang. Syst.*, *4*(3), 382–401. https://doi.org/10.1145/357172.357176

Lineros, J. V. (2021). IT Governance Considerations for Permissioned Blockchains. *Journal of Emerging Technologies in Accounting*, *18*(1), 45-59. https://doi.org/10.2308/JETA-19-12-01-49

Magnusson, D. (2009). The costs of implementing the anti‐money laundering regulations in Sweden. *Journal of Money Laundering Control*, *12*(2), 101-112. https://doi.org/10.1108/13685200910951884

Masciandaro, D., & Filotto, U. (2001). Money Laundering Regulation and Bank Compliance Costs: What Do Your Customers Know? Economics and the Italian Experience. *Journal of Money Laundering Control*, *5*(2), 133-145. https://doi.org/10.1108/eb027299

McCarthy, J. (2022). The regulation of RegTech and SupTech in finance: ensuring consistency in principle and in practice. *Journal of Financial Regulation and Compliance*, *31*(2), 186-199. https://doi.org/10.1108/JFRC-01-2022-0004

Padilla, A. J., & Pagano, M. (2000). Sharing default information as a borrower discipline device. *European Economic Review*, *44*(10), 1951-1980. https://doi.org/https://doi.org/10.1016/S0014-2921(00)00055-6

Pagano, M., & Jappelli, T. (1993). Information Sharing in Credit Markets. *The Journal of Finance*, *48*(5), 1693-1718. https://doi.org/https://doi.org/10.1111/j.1540-6261.1993.tb05125.x

Parra Moyano, J., & Ross, O. (2017). KYC Optimization Using Distributed Ledger Technology. *Business & Information Systems Engineering*, *59*(6), 411-423. https://doi.org/10.1007/s12599-017-0504-2

Rozario, A. M., & Thomas, C. (2019). Reengineering the Audit with Blockchain and Smart Contracts. *Journal of Emerging Technologies in Accounting*, *16*(1), 21-35. https://doi.org/10.2308/jeta-52432

Schmitz, J., & Leoni, G. (2019). Accounting and Auditing at the Time of Blockchain Technology: A Research Agenda. *Australian Accounting Review*, *29*(2), 331-342. https://doi.org/https://doi.org/10.1111/auar.12286

Tan, Y. (2016). The impacts of risk and competition on bank profitability in China. *Journal of International Financial Markets, Institutions and Money*, *40*, 85-110. https://doi.org/https://doi.org/10.1016/j.intfin.2015.09.003

Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Communications Surveys & Tutorials*, *18*(3), 2084-2123. https://doi.org/10.1109/COMST.2016.2535718

Werbach, K. (2018). Trust, but Verify

Why the Blockchain Needs the Law. *Berkeley Technology Law Journal*, *33*(2), 487-550. https://www.jstor.org/stable/26533144

Yermack, D. (2017). Corporate Governance and Blockchains*. *Review of Finance*, *21*(1), 7-31. https://doi.org/10.1093/rof/rfw074

Zeranski, S., & Sancak, I. E. (2021). Prudential supervisory disclosure (PSD) with supervisory technology (SupTech): lessons from a FinTech crisis. *International Journal of Disclosure and Governance*, *18*(4), 315-335. https://doi.org/10.1057/s41310-021-00111-7

Zyskind, G., Nathan, O., & Pentland, A. (2015, 21-22 May 2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. 2015 IEEE Security and Privacy Workshops,