Electronic Commerce Research and Applications 65 (2024) 101386

Contents lists available at ScienceDirect

Electronic Commerce Research and Applications

journal homepage: www.elsevier.com/locate/elerap

Blockchain solutions with consensus algorithms and immediate finality: Toward Panopticon-style monitoring to enhance anti-money laundering

Thomas Vinther Daugaard [a], Jakob Bisgaard Jensen [b], Robert J. Kauffman [c,d], Kwansoo Kim [c,*]

[a] Northstake A/S, Copenhagen
[b] Alipes Capital ApS, Copenhagen
[c] Copenhagen Business School
[d] Singapore Management University

ARTICLE INFO

Keywords:
Anti-money laundering (AML)
Blockchain
Compliance
Distributed ledger technology (DLT)
Exploratory research
Know-your-customer (KYC)
Transaction cost theory (TCE)
Transaction monitoring

ABSTRACT

Banks can reduce resources spent on anti-money laundering (AML) compliance with blockchain-based transaction infrastructure. We consider AML compliance as a superset of know-your-customer (KYC) and transaction monitoring capabilities. We carried out this research with Danske Bank and Concordium, using internal documents and interviews that served as empirical data. We show how storing digital representations of verified IDs with a blockchain can automate tasks and reduce redundant verification in KYC onboarding. Blockchain transparency also improves identifying counterparties, determining funds sources, and creating alerts in transaction monitoring. These reduce time and labor costs for AML compliance, which may lead to smaller banks. When more banks commit to layer-1 blockchain technology, the benefits of blockchain-based AML will increase. We carried out this theory-based qualitative research and encourage ECRA readers to recognize that the emerging technology innovations we study in this article have not yet been widely adopted and implemented by financial services firms. We also include a theoretical model with study hypotheses to make the main constructs that we investigate easily understood by non-technical ECRA readers. The findings we have developed are consistent with early-stage exploration in our research context and are intended to encourage more well-developed empirical results as the passage of time permits such work to be undertaken.

1. Introduction

During the 2008–2009 financial crisis, opportunistic behavior by bank lending officers and their borrowers, combined with lacking regulation, allowed financial institutions to exploit society's trust. Many lenders eschewed cautious credit analysis in lieu of securitizing risky mortgage loans in the national markets of the U.S. (Baily et al., 2008) and made many inappropriate complex derivatives and hedge fund trades that caused problems later. Several large American banks also failed to follow risk capital compliance standards of the era that led to illicit financial transactions, criminal payment practices, and money laundering (FATF, 2023).[1] These activities led to losses of billions of U.S. dollars (Weeks-Brown, 2018).

Through the awareness the present explorative research creates, we seek to deter money laundering. If anything, it has increased the demand for regulating financial activities more effectively and promoting regulatory technology innovations (Kurum, 2023). *Regulatory technology* (regtech) *solutions* can ease regulatory compliance, as AML processes consume ever-larger human and economic resources.

We will explore how incumbents and new entrants seek solutions to improve their AML processes. An industry initiative underway since the 2010s has been to reduce overlapping *know-your-customer* (KYC) and

* Corresponding author.
E-mail addresses: thomas@vinther.dk (T. Vinther Daugaard), jakob_bisgaard@hotmail.com (J. Bisgaard Jensen), rk.digi@cbs.dk (R.J. Kauffman), kkw.digi@cbs.dk (K. Kim).

[1] Acronyms used in this article are all listed here: *know-your-customer* (KYC); *distributed ledger technology* (DLT), *anti-money laundering* (AML); *6th Amendment of the Anti-Money Laundering Directive* (6AMLD); *peer-to-peer* (P2P); *Bank for International Settlements* (BIS), *Financial Action Task Force* (FATF), *United Nations Office on Drugs and Corruption* (UNODC), *European Commission* (EC), *World Economic Forum* (WEF), EC's *General Data Protection Regulation* (GDPR); *permissioned distributed ledger technology* (PDLT); *artificial intelligence* (AI), *generative artificial intelligence* (GAI), *large language models* (LLMs), *quantum machine learning* (QML), *decentralized finance* (DeFi); *Chainalysis* (CH); *Concordium* (CC); *Danske Bank* (DB), *Napier* (NP); *standard operating procedures* (SOPs), *customer due diligence* (CDD); *transaction cost economics* (TCE); and the *National Institute of Standards and Technologies* (NIST). If you require a definition, see the Glossary for our selected entries.

https://doi.org/10.1016/j.elerap.2024.101386
Received 27 August 2023; Received in revised form 6 February 2024; Accepted 15 March 2024
Available online 21 March 2024

AML compliance checks and lighten the information burden that financial institutions must bear (McKinsey & Co., 2019c). We focus on *distributed ledger technology* (DLT) and blockchain structure as relevant solutions (Deloitte, 2023, Thammandru and Chakka, 2020).[2]

We will argue that blockchain-based transactions operating on a *consensus algorithm* with *immediate finality* alleviate the contract costs and create a technical foundation for enhanced AML with automated KYC and transaction monitoring. Decentralized blockchains rely on consensus algorithms to determine the network's state. The Concordium blockchain network employs a *distributed proof-of-stake mechanism* for this purpose. In the absence of a central entity, validator nodes execute a common script to address the *Byzantine generals'* problem and achieve a shared consensus. Immediate finality, a crucial factor in transactional efficiency, is exemplified by the Concordium blockchain, which distinguishes it from networks with delayed finalization. The Bitcoin (BTC) blockchain generally requires 6 blocks, or 60 min, for finality. Concordium's immediate finality not only enhances transactional infrastructure but also supports traditional financial roles, such as clearinghouses and central securities depositories, thereby streamlining nonspecific transactions.

A *consensus algorithm* is: "*a procedure through which … peers of a blockchain network reach common agreement about the present state of the distributed ledger. Consensus algorithms achieve reliability in the blockchain network and establish trust between peers in a distributed computing environment*" (Patel, 2023). In contrast, *immediate finality* for blockchains is: *"… the affirmation that all well-formed blocks will not be revoked once committed to the blockchain. When users transact, they want to be confident that once their transactions go through, that the transactions cannot be arbitrarily changed or reversed"* (Gauda, 2023).

These reduce AML processing time, and the bank receives the benefits flows sooner (Bains, 2022, Bamakan et al., 2020, Bank for International Settlements, 2019). All transaction costs related to business trade relationships generate contractual incentives due to opportunistic behavior that often occurs. We examine opportunities and challenges for operational risk and offer foundations for our work based on *transaction cost economics* (TCE) (Williamson, 1991). Transaction costs in blockchain are akin to friction in physical transactions, which rise with more complexity and intermediaries. Traditional electronic payment systems involve multiple intermediaries, leading to elevated transaction costs, especially in cross-border transactions. Blockchain technology, through its capabilities and incentive structures, addresses this issue.

The consensus mechanism ensures honest behavior, authorizes transactions, and facilitates deterministic finalization within seconds. Blockchain also offers a way to conduct anonymous value exchange between counterparties. We discuss the challenging possibility of the technology effects on issues of trust, along with uncertainty in its liability, scalability, and security for the AML process. Our findings indicate that banks can reduce resources spent on AML compliance if they use blockchain-based transaction infrastructure.

Money laundering is a continuing and significant problem, with the annual amount of money laundered equivalent to 2% to 5% of global GDP each year (United Nations Office on Drugs and Crime, 2022) and banks employ 10% of their resources on AML-related activities (McKinsey & Co., 2021). The anticipated total cost of financial crime compliance exhibits varied trends across countries and continents, reflecting the dynamic nature of the regulatory landscape. In the U.S., expenditures surged from USD 35.3 bn in 2020 to USD 40.7 bn in 2022, indicating increased commitment to combating financial crime. Similarly, Canada witnessed a rise in compliance costs, escalating from USD 6.8 bn in 2020 to USD 9.2 bn in 2022. Germany, a major economic player, made a substantial financial commitment, with compliance costs reaching USD 57.2 bn in 2020 and further increasing to USD 61.6 bn in 2022. France had an uptick from USD 24.8 bn in 2020 to USD 27.3 bn in 2022, a more moderate increase. Central and Eastern Europe experienced an escalation in costs from USD 3.0 bn in 2020 to USD 3.9 bn in 2022, showcasing its commitment to enhanced financial integrity. Brazil, India, and the Middle East displayed marginal increases, with Brazil moving from USD 3.9 bn to USD4.2 bn, India going from USD 3.98 bn to USD 4.2 bn, and the Mid East rising from USD 3.4 bn to USD 4.2 bn. South Africa, in contrast, only grew from USD 3.3 bn in 2020 to USD 3.8 bn in 2022. The variations in compliance costs and diverse approaches adopted by countries are clear. (See Fig. 1.).

These problems are exacerbated by little or no cooperation or transparency between banks caused by the *coopetition paradox*. It occurs under "*conditions when cooperation would matter most, but stable agreements achieve only little*" (Finus and McGinty, 2019, p. 54). The implication is that no firm in the sector will want to take the lead on information-sharing projects that benefit AML processes industry-wide because they believe they will not be able to monetize the benefits (McKinsey & Co. 2019b).

Blockchain has applications in many industries and contexts with use cases beyond cryptocurrencies (Nofer et al., 2017), digital provenance (Mazumdar et al., 2021), and supply chain transactions (Schmidt and Wagner, 2019). Blockchain in AML-related processes is new and relevant due to creating transparency, immutability, and decentralization in information-sharing among firms. But blockchain-based solutions in AML processes in commercial banks are under-studied. Past research investigated blockchain-based KYC and identity management solutions (Kuperberg, 2020, Lootsma, 2017, Malhotra et al., 2022). And related in-depth work has focused on how *self-sovereign identity* and blockchain can be utilized to optimize KYC processes (Schlatt et al., 2021, Soltani et al., 2018). Efficiency improvement for AML processes based on blockchain has not been addressed for banks fully yet though (Merkle Science, 2023). So, researching blockchain as infrastructure for AML activities in banks is worthwhile – there are quite a few other issues too.

2. Literature and background theory

2.1. Blockchain and DLT effects

A *blockchain* is an append-only distributed ledger maintained by a *peer-to-peer* (P2P) network. The value of the blockchain is that, based on cryptographic proof instead of trust, any two parties can transact or distribute information without a trusted third party. Each network node holds a copy of the ledger, ensuring a decentralized network with no single point of failure. Thus, the technology assures integrity, immutability, transparency, and non-repudiation in decentralized computing

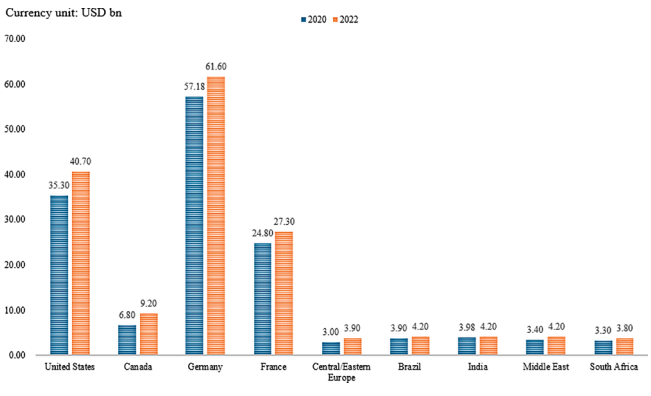

Fig. 1. The Total Cost of Financial Crime Compliance in 2020 and 2022.
Note. The anticipated aggregate cost of financial crime compliance for all financial institutions in the markets studied comprising North America, Latin America, Europe, and Asia Pacific in the 2022 investigation amounts to USD 274.1 bn (LexisNexis Risk 1 Solutions, 2022).

[2] See Appendix Table A1 for a Glossary of Terms and Definitions used in this article.

networks (Belotti et al., 2019).

In this regard, the *network effect* refers to the increased value of a service as its usage expands. The demand for a specific service is closely tied to the interest it generates, influencing overall utility and success. Blockchain technology and cryptocurrencies in their early stages are influenced by the network effect, which shapes their value and potential. This phenomenon is not limited to blockchain; industries such as social media and credit cards also experience value improvement with an increase in users. We next will further consider network effects in greater detail.

Blockchain network. Blockchain ecosystems experience network effects like traditional markets. Success is not solely driven by innovation, as factors influencing longer-term success are multifaceted. Timing plays a critical role in creating network effects for a cryptocurrency project, with the success of innovations often contingent on their reception as a suitable market solution upon their introduction for whatever problem context has been targeted. Interestingly though, projects that initially are technologically inferior may still achieve success by being introduced at opportune moments to build an installed base early on, further highlighting the potentially important impact of network effects.

Social media. YouTube exemplifies the power of network effects due to its expanding ecosystem and the forces that are projected beyond it. It serves as a substantial income source for individuals and firms alike, particularly benefiting vloggers who accrue substantial earnings through entertaining content, video blogs, and other in-demand offerings. YouTube and other platforms evaluate a channel's worth based on their subscriber count, viewership, and growth rate. This has led to the YouTube platform being a dominant player in its sector, which benefits from its market power overall as an Internet video-sharing monopoly. The network effects have been amplified as more users engage with and share their own videos, creating a self-reinforcing cycle that has solidified YouTube's position as the default video search engine in many countries around the world.

Credit cards. The credit card industry, exemplified by VISA and MasterCard, demonstrates the ubiquitous reach of the network effects these services have created in the past forty years. These dominant players, along with UnionPay, processed 96.8 % of all credit card transactions worldwide in 2022 (CapitalOne Shopping, 2023), and play vital roles in payments, involving authorization, clearing, and fraud prevention through secure methods. Their primary contribution lies in establishing a global and dependable processing infrastructure, facilitating secure and efficient transactions for both account holders and merchants. The robust network effect manifests as increased merchant acceptance leading to a reciprocal rise in users for both VISA and MasterCard.

Blockchain technology remedies the digital currency issue of *double-spending* while providing substantial improvements in guaranteeing trust in P2P transactions without needing a centralized, trusted intermediary. Since human involvement in intermediation is no longer necessary, blockchain represents a shift from trusting people to trusting the mathematics of digital cryptography (Nofer et al., 2017). Others have pointed out that blockchain technology can be a viable solution in the sphere of AML, where similar risks may arise. Lootsma (2017) introduced the idea of using blockchain technology as an effective way to manage *digital identities* as KYC information, which can be stored on the same blockchain in which financial firms and authorities participate. Further, the costs of complying with AML regulation can be mitigated using blockchain technology, as "*transaction data can be stored and become better traceable*" (Lootsma 2017, p. 19). Malhotra et al. (2022) extended this view by arguing that blockchain in KYC will improve the customer experience and minimize the overhead costs, too.

The scope of the solutions offered by the literature is different from ours here. We have sought to assess blockchain's potential impact on AML compliance holistically and in managerial terms, while the solutions proposed in the literature develop specific technical solutions for handling KYC better. Thus, our scope of inquiry in this article is to explore how blockchain-based infrastructure can impact and offer the potential to remedy the current challenges of AML compliance in practice. This is what makes this work relevant as a sponsored research project, involving a large commercial bank and a blockchain technology innovation firm interested in exploring opportunities with new technology applications.

2.2. Transaction cost economics (TCE)

Transactions differ in three aspects: their *asset specificity*, *uncertainty*, and *frequency*. These dimensions determine how transactions should be governed. *High asset specificity* refers to investments specific to the transaction and has a substantially lower value in the best alternative use case. TCE describes problems of contracting and considers how comprehensively a contract should be designed and the contingencies it includes to remedy complex uncertainty (Williamson, 1991, Schmidt and Wagner, 2019, Li et al., 2023).

Contracting. While all transactions can be facilitated via contracts, it may be difficult to determine what is the best-suited contract type. *Classical contract law* strives for contracting that is comprehensively delimited and where all relevant future contingencies are described, and any attributes have related plans to address them. *Neoclassical contract law* acknowledges that agreements will be incomplete and so *relational contracting* is not necessarily based on any formal agreements but rather on "*the entire* [*relationship*] *as it has developed* [*through*] *time*" (MacNeil 1978, p. 890).

Governance. *Market governance* is defined by classical contract law as transactions that are highly standardized, and buyers and sellers have no reliance on one another. Market governance holds across non-specific transactions, no matter the uncertainty and frequency levels of their exchange.

Hybrid governance is a form of *bilateral governance*, blending private and public aspects. Frequently recurring transactions of mixed asset specificity are well-matched with a bilateral governance structure, based on relational contracting. The recurring frequency and specificity of the transaction make continuity a valuable aspect of the relationship. The last is *hierarchical governance*, a unified structure with one entity. Highly-specific transactions of occasional frequency are well paired with the hierarchy, as incentives for trading with other entities are weakened by high asset specificity.

Blockchain transaction cost mitigation. TCE posits that the expenses incurred by parties involved in a transaction can be categorized into three primary perspectives. First, due to the inherent self-opportunism of transaction participants, monitoring costs are accrued to ensure the faithful execution of the transaction. Second, coordination costs arise to address the information asymmetry between the involved parties, which is essential for establishing an actual transaction. These costs may also be a consequence of bounded rationality issues. Third, when the assets invested by the transaction parties are confined to the specific transaction at hand, resulting in high asset specificity, the transaction costs proportionally escalate. Notably, heightened asset specificity exacerbates problems associated with self-opportunistic behavior and information limitations. In such instances, internalizing transactions within a firm becomes relatively efficient, leading to the creation of a firm's structure apart from the market. Internal transactions, as noted by TCE,

pertain to the coordination and management of transactions conducted through the bureaucratic system of the firm.

Transaction coordination, control, incentives and opportunism. In contrast to market transactions, the coordination of transactions within a firm primarily relies on two methods: a hierarchical control system overseeing the conduct and performance of internal transaction parties or employees, and an incentive system designed to curb self-opportunistic behavior. Nevertheless, a critical question arises regarding the efficacy of these internal mechanisms, namely the hierarchical control system and incentive system, in effectively managing and mitigating the selfish behavior exhibited by transaction parties or employees within the firm.

In accordance with Moran and Gohshal's (1996) study, TCE contends that firms face challenges in mitigating human opportunistic behavior more effectively than markets through hierarchical control systems and incentive structures. While a firm's hierarchical control system can curtail opportunistic behavior among members, it also diminishes positive attitudes and employees' trust. Similarly, incentive systems can mitigate members' opportunism but still may give rise to issues such as the decoupling of performance and bonuses, fairness concerns for incentive application, and heightened internal competition. Consequently, the negative attitudes among members may be hard to restrain effectively.

Establishing effective punishments and rewards system may regulate employees' behavior as intended. But they are associated with negative attitudes toward the firm among employees, reflecting their assumed predisposition toward selfish behavior. By starting with the goal of establishing and overseeing a business that minimizes transaction costs, TCE offers explanations for complexity overall, but also establishes a foundation for understanding how transaction costs have arisen in the process and should be reduced. This is why strategic disintermediation has been important in digital commerce.

2.3. Technological change theory

Capitalism is known to be an evolutionary process. Continuous innovation is the fundamental impulse that keeps its engine in motion. Anderson and Tushman (1990) argued that the evolutionary process of technological change that constantly reshapes the competitive environment can be seen as a *technological cycle*. Initiated by breakthrough innovations that advance the technological state-of-the-art, technological discontinuities create new ways of doing business. In the new paradigm, the dominant technology, including landlines and mobile telephony, will shift to a new S-curve for diffusion (Foster, 1986). The theory highlights an industry or product as being dependent on new technology that evolves over time. Its performance will increase up to a limit, and then will stagnate no matter the new funds invested.

3. Research context

We now consider commercial banking and blockchain-based technology services in what follows.

3.1. Commercial banks

The financial crisis and multiple instances of money laundering have increased the demand for regulating financial activities more effectively. Further amendments to the Basel Accords have been made (Hull, 2018), while continuing high-cost money laundering scandals have necessitated a *6th Amendment of the Anti-Money Laundering Directive* (6AMLD) of the European Parliament, an elected legislative body of the European Commission (EC 2021). The consequences have been that banks must comply with extensive *customer due diligence* (CDD) and record-keeping requirements to prevent illicit transactions and money laundering.

In the past decade, the average annual cost of complying with 6AMLD has risen to USD 50 mm, with some banks now spending USD 500 mm-plus on ensuring AML compliance (Thomson Reuters, 2016). Thus, incumbents and entrants have sought solutions to improve their processes. By reducing overlapping KYC and AML compliance checks and lightening the information burden, distributed blockchain structure may be able to solve this operational puzzle and avoid the related costs.[3]

3.2. Blockchain-based services

Despite a high volume of investments and advances in the technology, blockchain continues to have a tarnished reputation. Trust in finance-related blockchain applications is inferior to trust in traditional financial institutions and their privacy solutions. This is due to frequent episodes of blockchain-based transactions used for illegal activities, such as drug payments, human trafficking, illicit real estate investments, and money laundering (U.S. Government Accountability Office, 2022). According to Chainalysis' yearly crime report, cryptocurrency-based crime hit a new high in 2021, with illicit addresses receiving USD 14 bn the year, up from USD 7.8 bn in 2020 (Grauer et al., 2022). Chainalysis also reported that the share of illicit cryptocurrency transactions only amounted to 0.15% in 2021 compared to 0.62% in 2020 and 3.37% in 2019. Thus, the share of illicit transactions appears to have progressively become smaller – but still there has been a gain.

The capabilities of blockchain ensure the potential of blockchain-based solutions and support improved compliance procedures. For example, the U.S.-based non-profit foundation, Sovrin (https://www.sovrin.org), has offered a KYC-compliant platform built on *permissioned distributed ledger technology* (PDLT).[4] Also, Selfkey (https://www.selfkey.org) has operated in the same space with a *blockchain-based self-sovereign identity solution*.[5] Other firms utilizing blockchain technology for efficient compliance and self-sovereign identity are ShoCard (https://www.shocard.com), Blockcerts (https://www.blockcerts.org), and Civic (https://www.civic.com) (Soltani et al., 2021). Common to these projects is the aim of enhancing KYC and identity-related processes.

The Danish-Swiss non-profit foundation, Concordium (https://www.concordium.com), has taken this a step further by developing its own blockchain with KYC built in at the protocol level to ease regulatory compliance. Thus, through the legal framework of institutional compliance while offering a blockchain-based transactional infrastructure, Concordium seems relevant in the perspective of combatting money laundering and ensuring transactional transparency.

4. Proposed theory

We define *transactions* as *non-specific* when they involve a simple transfer of value between two transacting parties. The friction of intermediaries from carrying out simple transfers like this generally

[3] A 2019 study by McKinsey & Co. (2019a) estimated the potential savings from blockchain-based solutions for customer onboarding, regulatory compliance, and fraud arise from these five activity categories: customer onboarding operating costs—USD 0.5–1.0 bn; lost and stolen card costs—USD 0.5–1.0 bn; funds counterfeiting—USD 3.0–3.5 bn; transaction fraud if card not present—USD 3.5–4.5 bn; and regulatory fines—USD 2.0–3.0 bn. The total in these categories is USD 9.5–13.0 bn.

[4] The firm has argued that the root of the continuing problem of lacking failsafe user identification related to Internet-based transactions is that the Internet was never conceptualized as requiring this missing identity layer to enable people to create, hold, present and retain self-identifying digital content to validate their identities. Its use of PDLT is intended to be a step in that direction, to enable all Internet users to have ownership over their digital identities.

[5] Selfkey's intention is much the same: to give a user control of their digital identify so they can transact in settings where blockchain technology is used, and benefit from the ownership and control of their sovereign identify, yet not create undue risks for others – both users and Internet firms – when the owner engages in transactions.

constitutes the contractual compliance costs in the transaction. Banks' legacy systems combined with the necessity of intermediaries' involvement in the multi-step processes entail that the friction and high contractual compliance costs will remain.

4.1. Hypotheses

We propose that blockchain technology can have a moderating effect in reducing these contract costs (Hypothesis 1a) (H1a). Transacting on the blockchain allows banks to utilize technology for AML (H1b), while the technology enables the creation of new tech foundations within AML compliance (H2a). The transparency and data quality (H2c), as well as crypto ID-representation on the blockchain (H2b), also enable regulatory compliance with less input compared to current AML technology (H2d). Moderated by the network effect of the technology (H3a), this can lead to improved AML processes and essentially shift (H3b) the boundaries of the firm, so control is more effective.

Blockchain capabilities and contract costs. Current digital payment systems heavily rely on payment authorization, clearing, and settlement processes, necessitating the involvement of intermediaries to establish trust and prevent opportunistic behavior among transacting parties. This reliance on intermediaries becomes more pronounced in complex digital transfers, especially across borders and jurisdictions, resulting in increased friction and higher contract costs. These costs are associated with ensuring settlement and guarding against opportunism. The nature of non-specific digital transactions compounds the need for intermediaries, heightening transaction costs – a common refrain in business.

Blockchain technology offers a promising solution to mitigate these transaction costs. By leveraging a novel consensus mechanism and achieving instant finality, blockchain protocols can autonomously handle payment authorization, settlement, and clearing without the intervention of intermediaries. The consensus mechanism also ensures automatic authorization and arrangement of transactions in blocks before distribution across the network, while deterministic finalization guarantees swift execution. Thus, this reduces contract costs, allowing peers to exchange value and conduct transfers without the friction associated with intermediaries, thereby streamlining the digital payment process.

Despite the advantages of blockchain though, certain contradictions and challenges still may arise. Immediate finality, while beneficial for efficiency, presents limitations as users are unable to cancel or withdraw transactions once executed on the blockchain. This lack of flexibility can lead to additional transaction costs, particularly when parties seek to reverse a transaction. In the absence of intermediaries to handle cancellations, enforcing the use of a third party to settle post-transaction disputes can result in contract costs surpassing those of traditional systems. Striking a balance between efficiency and flexibility remains a crucial consideration in the ongoing evolution of digital payment systems based on blockchain technology. Considering these aspects, we offer:

- **Hypothesis 1a (Blockchain capabilities and contracting cost reduction).** *Consensus mechanisms and instant finality are each separately associated with the reduction of contract costs when non-specific transactions are executed on a blockchain.*

Spillover effects of non-specific transactions. In an open transaction environment, money trails become transparent, a stark contrast to the cluttered and siloed data structure of banks. The transparency inherent in blockchain transactions enables authorities to closely monitor bank compliance with regulations, fostering better-aligned incentives. Currently, closed internal ledgers limit the authorities' ability to monitor banks effectively though, creating an agency problem wherein banks can profit from non-compliance. Shifting transactions to a blockchain platform rather than a closed banking system addresses this issue, aligning incentives between authorities and banks, thus allowing technology to be strategically employed for AML. The capabilities of blockchain technology not only facilitate more effective monitoring but also trigger positive trickle-down effects in aligning incentives.

Elaborating on the reduction of contracting costs, blockchain-based transactions offer a compelling alternative to centralized databases, overcoming the challenges posed by legacy IT systems in the digitization of financial services. Blockchain's secure, transparent, and open transaction system enhances the execution of transactions, ensuring confidentiality and reducing contract costs. Beyond transaction execution, blockchain's capabilities extend to providing verification for reported transactions in auditing, eliminating single points of failure in centralized legacy systems, and improving AML processes through an immutable and transparent decentralized ledger. However, it is crucial to acknowledge the contradiction that blockchain technology, despite its relative novelty, may introduce unforeseen issues when implemented as new transaction infrastructure in banks. The successful integration of blockchain for AML purposes necessitates new regulations, a process that must precede the formulation of effective AML procedures on the blockchain. To address these considerations, we propose:

- **Hypothesis 1b (Spillover effects of non-specific transactions).** *Executing non-specific transactions on blockchain is related to banks' technology use for improving AML.*

Blockchain and technological shifts. The evolutionary trajectory of technological change unfolds within a cycle involving a technological discontinuity, an Era of Ferment, a dominant design, and an Era of Incremental Change (Anderson and Tushman, 1990). Blockchain technology, introduced in 2008, marks a clear technological discontinuity, setting the stage for an Era of Ferment. At this time, various blockchain-based solutions will vie for dominance in all-out competition. Among the proposed applications, integrating blockchain capabilities into banks' AML processes has emerged as a promising avenue. Current AML processes, stemming from incremental changes since the 1950s, face challenges of excessive complexity and cost due to heightened regulatory requirements. Blockchain, in this context, offers an alternative infrastructure for redesigning AML processes and addressing present compliance challenges.

To enhance the potential of blockchain in AML processes, it is essential to note the difficulty in scientifically testing this proposition due to its conceptual nature. The argument gains coherence through industry insights, with stakeholders expressing the belief that blockchain introduces a novel way of transacting, fundamentally different from existing methods, but useful. The consensus mechanism and instant finality associated with blockchain technology present a marked departure from traditional transaction execution. As current AML processes approach their performance limit under increasing regulatory demands, blockchain's capacity for non-specific transactions provides an opportunity to reimagine and rebuild a more efficient AML framework.

An issue arises when considering the use of permissioned layer-1 blockchains by banks though. In such instances, AML processes may mirror the current banking system, especially in interbank transfers. The fragmentation of transactions across distinct layer-1 blockchains poses challenges in tracking and monitoring, reminiscent of the complexities in the present system. The need for large public blockchain networks or brokers to mediate transfers between different layer-1 blockchains adds layers of complexity, potentially hindering the envisioned transformation of AML processes through blockchain technology. This contradiction highlights the likely challenges associated with implementing blockchain in specific banking contexts. Within this focus, we further posit:

- **Hypothesis 2a (Blockchain and technology shifts).** *Executing non-specific transactions on a blockchain is linked to the assurance AML compliance makes possible in commercial banks.*

Blockchain-based KYC. The Financial Action Task Force (FATF) recommendations constitute a cornerstone in the regulatory framework for financial institutions, particularly emphasizing CDD principles. The guidelines prescribe the immediate identification and verification of all customers and beneficial owners when establishing business relations, thereby prohibiting the maintenance of anonymous accounts within financial institutions (FATF, 2022). A critical aspect of CDD implementation is evident in the resource-intensive KYC onboarding measures. The manual retrieval of identity information, such as passport pictures and background checks for new customers, has proven labor-intensive for individual banks, magnified by the large-scale nature of identity verification. This inefficiency extends systemically as financial institutions engage in redundant identity verification processes for customers previously vetted by other institutions, highlighting the central challenges of siloed data and ineffective exchange mechanisms.

As such, these challenges in the KYC onboarding process suggest blockchain technology's potential to offer effective solutions. Blockchain, with its attributes of public transparency and immutability, can address the inefficiencies plaguing the current system. Emerging initiatives propose blockchain-based solutions so that all account addresses cryptographically represent the true, verified identity of real-world individuals. By incorporating third-party specialists to verify entities on the blockchain, banks can streamline their KYC checks. The transparency and public nature of blockchain addresses facilitate their usage across financial institutions, reducing the duplication of identity verifications and addressing the systemic inefficiencies associated with the current KYC onboarding procedures.

The adoption of blockchain-based solutions introduces a significant contradiction though, primarily revolving around concerns related to privacy and data protection. The comprehensive and immutable nature of on-chain identities, directly linked to real-world individuals, raises concerns regarding potential threats to user privacy. The risk of exposing sensitive personal information through account addresses which reflect the cryptographic identity of an individual could be exploited by malicious actors, leading to identity theft and unauthorized access. Further, reliance on a centralized identity provider, managing government-issued ID data in an off-chain database, introduces security concerns. In the event of a security breach or unauthorized access to this external repository, a substantial volume of sensitive personal information could be compromised, thereby undermining the foundational principles of security and confidentiality that KYC processes aim to uphold. This contradiction highlights the balance required when leveraging the benefits of blockchain for streamlined KYC processes while safeguarding the privacy and security of individuals' sensitive information. In this view, we assert:

- **Hypothesis 2b (Blockchain-based KYC and compliance verification).** *Storing representations of identities on a blockchain will be associated with the time on verification for KYC compliance that the banks can reduce in the process.*

Blockchain-based monitoring and record-keeping. On the blockchain, transactions occur in an open environment, providing transparent money trails compared to closed institutional settings. This transparency enhances prediction accuracy and reduces the time spent investigating false positives by offering a comprehensive transaction overview and automatically recording transactions for compliance. Also, the linkage between transaction and identity data on the blockchain results in a more coherent data structure, addressing drawbacks in legacy systems and improving record-keeping and transaction monitoring processes. The related FATF recommendations emphasize ongoing due diligence effort made by financial institutions, including the regular updating of KYC data and risk assessments, aligning transactions with institutional knowledge of the customer. Unlike traditional infrastructures where transaction records are confined to bank silos, blockchain's visibility to all users fosters openness, aiding the establishment of a fuller understanding of a customer's activities, narrowing the scope of investigations.

Critics argue that the heightened transparency of blockchain transactions may compromise user privacy though, as sensitive financial information becomes visible to everyone on the network. Traditional financial structures, perceived to have more robust privacy measures, limit transaction accessibility to authorized parties. Further, if banks are not on the same blockchain network, leveraging the benefits of blockchain's data structure becomes challenging, requiring migration and interpretation for funds flow determination. Despite the advantages, these privacy and integration concerns highlight potential drawbacks in adopting blockchain for transactional infrastructure, illustrating the need for a nuanced approach in balancing transparency with privacy and interoperability. Considering these points, we suggest:

- **Hypothesis 2c (Transaction transparency and blockchain-based monitoring).** *Data quality and blockchain transaction transparency are related to the enhancement of record-keeping process effectiveness and reduce time benefits from false positives in monitoring.*

Blockchain-based AML and performance limits. Technological change theory posits that a new S-curve can be initiated by a technological discontinuity, signifying a shift to a technology with a greater performance limit. The transformation of current AML processes to leverage blockchain capabilities embodies such a technological shift. Blockchain-based AML processes, with their enhanced performance limits, represent a radical departure from conventional methods. However, the immediate implementation of blockchain-based AML processes may exhibit inferior performance compared to current processes, necessitating technological investments in the transition. As the adoption of blockchain technology increases, the performance of AML systems is expected to surpass that of existing processes, leading to more efficient allocation of resources for regulatory compliance.

Building on this foundation, we contend that blockchain technology serves as a technological discontinuity, introducing a digital native data structure that blends identity and transaction data. This innovation renders certain aspects of KYC onboarding processes obsolete and enables real-time monitoring of fund movements across institutions and clustering risky addresses. The comparison between this technological advancement and current transactional infrastructure reveals a significant reduction in the effort required for AML processes. However, this depends on the presence of a network of multiple institutions concurrently adopting blockchain technology as the transactional infrastructure. This proposition may face challenges in practical testing against SOPs and real-world AML processes, stressing the need for added understanding of its applicability. As such, we offer:

- **Hypothesis 2d (Blockchain-based AML and compliance enablement).** *AML processes with blockchain-based KYC onboarding, transaction monitoring, and record-keeping are associated with compliance that diminishes bank effort compared to current practice.*

Network effects. Shapiro and Varian (1999) suggest that network effects are present when specific activities generate benefits for others. Blockchain technology introduces an advantage by enabling verified identities to be represented, leading to a reduction in time for KYC onboarding processes. This is attributable to the elimination of redundant identity verifications, so multiple institutions benefit from a single customer's blockchain verification. The connection lies in the causality between blockchain verification and the efficiency in KYC processes, demonstrating how network effects amplify the impacts for others in the financial ecosystem.

Network effects are evident in transaction monitoring processes supported by blockchain. Financial institutions participating in the same layer-1 blockchain (Feyen et al., 2021) contribute to an installed base of users that enhances the value of the service. Transactions in a shared blockchain network provide a holistic transactional overview, increasing the accuracy of behavioral alerts and reducing the number of false positives in identities. The cumulative effect of increased transactions in the blockchain network helps to identify patterns related to suspicious activities, too. This suggests how network effects can enhance transaction monitoring through the collaborative engagement of financial institutions.

As the number of financial institutions utilizing the same layer-1 blockchain grows, the benefits derived from KYC onboarding and transaction monitoring in the blockchain ecosystem will intensify. The network effect, grounded in the installed base of firm-level users, implies a decrease in AML processing time while maintaining a constant output of regulatory compliance. One might be concerned with the assumption of standardized regulatory requirements across jurisdictions. If financial institutions operating on the same layer-1 blockchain adhere to different regulatory environments, challenges in achieving compliance and standardization in AML processes may emerge, tempering the anticipated benefits due to network effect limitations. For blockchains, we suggest this hypothesis as a basis for examining the findings:

- **Hypothesis 3a (Network effects resulting from layer-1 blockchain adoption).** *Positive effects of blockchain on AML will be linked to the network strength when more institutions are using the same layer-1 blockchain.*

Less contracting due to blockchain-based AML effects. The integration of verified IDs on the blockchain will likely reduce the perceived need for redundant KYC onboarding tasks, and also diminish the necessity for so much contracting. Blockchain's transparent nature enhances transaction monitoring capability by providing a readily available network-wide view of transactions, reducing effort to examine customer behavior. The improved accuracy of behavioral alerts further diminishes the necessity for extensive employment contracts dedicated to investigations. As the technology streamlines AML compliance, internal contracts will likely be phased out, lowering the overall resources required.

Also, the asset specificity of transaction monitoring tasks should fall in a blockchain environment, enabling banks to outsource these processes and organize them with bilateral governance. The transparency and digital-native data structure of blockchain also should facilitate the externalization of transaction monitoring, altering the current governance mechanism. Outsourcing becomes viable as the lower asset specificity aligns with the principles proposed by Williamson (1985), who advocated market or bilateral governance in such situations. Blockchain's positive impact on AML should reduce contracting to some extent by improving processes or by allowing sensible outsourcing, guided by the lower asset specificity in transaction monitoring.

Despite the potential benefits of blockchain in AML, the situational challenges still may limit its impact on reducing the number of contracts. The upfront investment required for blockchain implementation, encompassing infrastructure, training, and system integration, may outweigh the potential labor and time savings. Integration issues pose another hurdle, as legacy systems in financial institutions were not designed with blockchain in mind, and so will lead to more complex and disruptive transitions. The time and resources needed for seamless integration may also counteract other efficiency gains.

While blockchain can automate some AML processes, human expertise remains essential for interpreting complex transactions and identifying the potential risks. Over-reliance on blockchain technology might lead to neglecting the development of skilled professionals in AML compliance, creating gaps in the detection and prevention of illicit activities. In essence, while blockchain has shown promise for AML enhancement, practical challenges and the continued need for human expertise may impede the anticipated reduction in the associated contracts. Thus, we share a final theory-based assertion:

- **Hypothesis 3b (Fewer contracts and blockchain-based AML).** *The effect of blockchain on AML performance will be related to the reduction in the number of contracts concerned with AML processes when output is held constant.*

A sketch of our theoretical model is shown next. (See Fig. 2.).

5. Data and methods

This research is based on in-depth semi-structured interviews with experts from Danske Bank (https://www.danskebank.dk), Concordium (https://www.concordium.com), Chainalysis (https://www.chainalysis.com), and Napier (https://www.napier.ai). The interviewees represent different professional functions. (See Table 1 and Appendix B on interview style, process, and content for additional background information.) We used SOPs from an excerpt of Danske Bank's AML processes as well.

All interviews were transcribed in a form suitable for coding and analysis. After transcription, each interview was coded to mark its key themes. Our transcriptions were inspired by *thematic coding strategy* (Rapley, 2011). The coding of the content formed the basis for carrying out ex post opinion-condensing interview analysis work. (See Appendix B on the coding process we used with NVivo.) Triangulation of our data points was made possible by using different data sources (e.g., interviews, documents, white papers, webinar). By comparing different forms of data, we validated the data supplied by our sources. This is an example of an *instrumental case study* (Stake, 2005, Lucas et al., 2018) involving: "[*a*] *person, specific group, occupation, department, organization*) to *provide insight into a particular issue, redraw generalizations, or build theory … in instrumental case research, the case facilitates understanding of something else*" (Mills et al., 2010, p. 473-474).

Our study also is based on *analytic generalization*, involving reasoned judgments about whether the findings from a study can be applied to other contexts. Its generalizability is built on the logic of similar transactional infrastructures from bank to bank and FATF recommendations that have been implemented in financial services sector-wide. They constitute the backbone of AML processes. But banks rely on legacy systems and may be in different stages of their digitalization journey. Further, case-based observations often have low generalizability, and yet this is an appropriate method to use in exploratory research on emerging technologies. The impact that blockchain can have on Danske Bank's AML processes ought to be like other firms that rely on core principles and technology infrastructures.

6. Mechanism analysis and results

We examine if blockchain-based transactions that operate with the consensus algorithm and immediate finality can alleviate contract costs and create a new technological foundation for enhanced AML performance, by shortening the transaction process-related time and benefits flows.

Financial infrastructures rely on *digital intermediaries* (from clearinghouses, correspondent banks, and messaging networks) for non-specific payment transactions. They typically exhibit some friction, resulting in transactions sometimes taking days to complete. This is a cost of safeguarding against opportunism and establishing trust between transacting parties. Concordium's blockchain uses a *distributed proof-of-stake* consensus mechanism and a *deterministic finality layer* to ensure trust in transactions. The consensus mechanism validates transactions while the finality layer settles them. So, a transaction on a Concordium blockchain can be completed within 12 seconds without the need for third-party involvement.

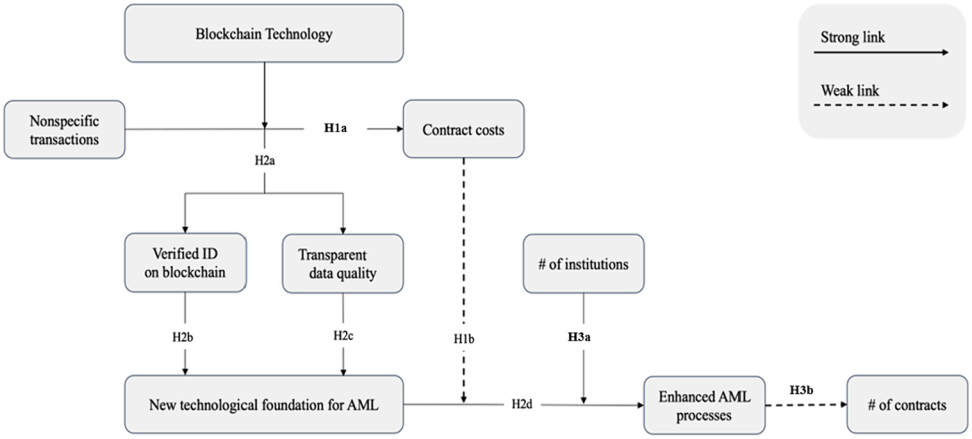

Fig. 2. Conceptual Model and Theory-based Hypotheses.
Note. This figure depicts links representing the effects based on hypotheses implied by the theory-based statement. Our evaluation was done by assessing the hypothesis in terms of whether there is qualitative evidence to suggest that the corresponding null hypothesis (for no effect) should be rejected. We thank an anonymous reviewer for providing us with input that led us to use the most basic approach to hypothesis evaluation that our data and methods allow in this research. The reader should note we include what we believe to be stronger or weaker links, in lieu of positive or negatives effects.

Table 1
Interview Participants in This Study.

Interviewee's Professional Role	Firm	Minutes
Senior Researcher	CC	37
Director (3); Senior Manager	CC	57, 60, 85; 27
Senior Manager	CC	27
Blockchain Specialist	DB	56
Executive, KYC (2)	DB	56, 57
AML Advisor, KYC (2)	DB	30, 35
AML Officer Transaction Monitoring	DB	35, 36
Director	NP	43
Compliance Manager	CH	34

Notes. Interviews: 14 total; Firms: 4, CH = Chainalysis, CC = Concordium, DB = Danske Bank, NP = Napier.

6.1. Results for the hypotheses

Hypotheses 1a and 1b. The fee for using this mechanism for a transaction is €0.01. So, the Concordium blockchain reduces contract costs related to non-specific transactions using a proof-of-stake consensus mechanism and a deterministic finality layer. In traditional financial terms, they handle authorization, clearing, and settlement without involving costly third parties. This finding supports H1a, which is backed by evidence from four Concordium employees and a quoted bank blockchain specialist: "[*Blockchain*] *would cause a much simpler process, and … we will entail that we will not need all the intermediaries that are part of the infrastructure today, that is, clearinghouses and the central securities depository.*"

H1b motivates why blockchain is relevant from an AML perspective. Transacting on an immutable, public, and transparent blockchain, not closed-ledger banking systems, aligns incentives between regulators and banks, allowing technology use for AML. H2a argues that current process technology for AML compliance is nearing its performance limit. Blockchain is an alternative infrastructure for developing novel AML processes for KYC and transaction monitoring. Using the Concordium blockchain, KYC onboarding processes can be developed with on-chain identities verified within 15 seconds by a specialized third party. H2b highlights how financial institutions like Danske Bank can use verified identities as part of their KYC onboarding process, reducing manual tasks related to ensuring ID quality and manually registering data. The transaction monitoring process relies on manual investigations of behavioral alerts, most of which are false positives.

Hypotheses 2a, 2b, 2c and 2d. With blockchain for transactions, the monitoring process can be redesigned with address clustering and accurate alerts. This can reduce resources spent on investigating false positives in H2c. Transparency allows for reworking monitoring processes for efficiency without compromising effectiveness. Blockchain provides a digital native data structure that can benefit transaction monitoring and record-keeping. Combining these findings, we concluded that blockchain can enable a new process technology for AML compliance, which has a higher performance limit than the current process technology as stated in H2d. Our empirical data suggest full support for H2a, H2b, and H2d. This support is based on interviews with blockchain experts from Concordium, AML employees at Danske Bank, and SOPs for AML compliance. We found less than full support for part of H2c. But there is only mixed evidence that blockchain's data quality enhances record-keeping processes.

Hypotheses 3a and 3b. Blockchain-based AML processes cause manual tasks related to KYC onboarding to become redundant and so time spent investigating false positives in transaction monitoring can be reduced. Blockchain-based AML processes can reduce the number of contracts employed with AML compliance without compromising effectiveness. Another way to reduce time and costs related to AML processes is, as suggested in H3b, by using a bilateral governance mechanism. This is enabled by blockchain network transparency, which lowers the specificity of transaction monitoring activities. Controlling transaction monitoring by bilateral governance rather than in a hierarchy reduces transaction monitoring costs, as a bilateral governance structure accommodates the lowered specificity better than a hierarchy does.

Blockchain's effect on reducing time and compensation for AML processes is moderated by the number of institutions using the same blockchain. H3a hypothesizes how on-chain verified identities are a positive externality as institutions can benefit from synchronization of IDs provided by the Concordium blockchain. Blockchain-based transaction monitoring processes benefit from network effects as the performance of those processes increases proportionally as the number of network participants increases. Several Danske Bank employees interviewed for this research supported H3a, exemplified by a blockchain specialist's comment: "*It would certainly change completely if we all shared a common system where the transaction history was stored forever, could not be changed, and could be broken down into even the smallest bits and pieces.*"

We found support that a blockchain-based transactional infrastructure can reduce time and labor costs in AML processes, leading to less contracting. However, with the practical difficulty of testing this hypothesis, the empirical data collected for this research suggested less than full support.

Table 2 summarizes the levels of support we found for our hypotheses (full or mixed). Not all hypotheses could be assessed as having received full support though. We now turn to a broader discussion of what we have learned through this research.

7. Discussion: A panopticon effect of self-monitoring

We next will discuss a number of issues which arose in our research process that merit comment.

7.1. Transparency, monitoring and the blockchain panopticon

Overall, our findings suggest blockchain's transparency can cause transaction monitoring to be less time-consuming for banks. This finding has wider implications since transparency can affect the basic incentives to launder money through financial institutions. Blockchain infrastructure is an open and public system in which anybody with Internet access may trace the history of transactions. As such, this openness makes it difficult to conceal illicit financial activity. Transactions in a blockchain network can be always observed; so, money launderers using the network never know if they are being watched.

Thus, transparency creates a *panopticon*, in philosophy of science language (Foucault, 1995). *Panoptic surveillance* leads to regulatory acceptance and compliance, like a guard's observation tower in a prison. The effect of a blockchain panopticon is that money launderers must expect to be observed, as all of their activities can be traced and documented, and they can be held accountable for inappropriate action. As a result, the incentive for them to use a blockchain network to launder money is mitigated or even removed in the presence of panoptic monitoring due to force of the related penalties. This effect can have collateral ramifications for AML and transaction monitoring. When the incentive to launder money through institutions is reduced, banks can deploy less transaction monitoring. As such, the costs for commercial banks might be even lower.

The task of transaction monitoring can be outsourced to third parties though. Their expertise is built on knowledge of blockchains' inner workings, how to analyze transaction flows, and financial regulations. As such, analytics firms like Chainalysis benefit from knowledge about the technology's capabilities being concentrated with only a few industry specialists. This concentration of knowledge is a potential barrier to the panopticon effect. So, widespread awareness of blockchain's transparency and the 2008 financial crisis, with the pervasive opportunistic behavior combined with a shortage of regulation, allowed financial institutions to exploit society's trust. Some banks facilitated illicit transactions and money laundering, too. We have sought to understand and interpret the impacts of the financial crisis and the more recent instances of money laundering. They have increased demand for regulating financial activities with greater technological strength, as suggested by the regulatory technology subsector, *regtech*, of the Fintech Revolution. Accordingly, technology-based solutions aimed at easing compliance have risen in popularity, such that AML processes continue to consume exorbitant amounts of human and economic resources in the discovery and innovation work that has ensued.

Table 2
Hypotheses, Support Levels and Comments.

H's	Support Level	Strength of Results: Comments
1a	Full	Concordium's business model and four interview responses supported H1a.
1b	Mixed	Practice literature supported it; but interviews didn't cover all related topics.
2a	Full	Interviews, practice, research, and white papers supported H2a.
2b	Full	Interviews, Danske Bank SOPs, and consulting white papers supported H2b
2c	Mixed	Less than full support as interviews didn't fully cover the topic.
2d	Full	Evidence from our fieldwork and secondary published sources was positive.
3a	Full	Responses were positive, especially Danske Bank's on shared systems.
3b	Mixed	Interviews were positive but had weaker support compared to secondary data and other published materials.

Notes. When we indicate that there was support, it is because the information that we uncovered was consistent with the hypothesis we present in the theory section of this article. All results are based on the extensive interviews reported in Table 1, along with selective use of practice (1a, 1b, 2a, 2d, 3a) and university (1a, 3b) research. Chainalysis' webinars (2a, 2c, 3a), consulting white papers (1a, 2b), and Danske Bank's SOPs (2b) were also used.

7.2. Overlapping compliance checks, process information, and transaction cost reduction

We addressed incumbents and new entrants in financial services (e.g., fintech start-ups and challenger banks) that have sought novel solutions to improve their current processes. By reducing overlapping KYC and AML compliance checks and lightening the information burden, the distributed blockchain structure may be able to resolve some of the hassles that innovative firms have been experiencing. We also hypothesized that blockchain-based transactions that use a consensus algorithm and immediate finality alleviate contract costs and create a new tech foundation for AML performance – via automated KYC and transaction monitoring – shortening AML transaction processing-related time in the process. In theory terms, all transaction costs related to business trade relationships generate contractual incentives according to opportunistic behavior that occur frequently between partners. We examined the opportunities and challenges for operations risk managers to address that directly.

Blockchain is widely recognized in the past fifteen years as influential and revolutionary as a new digital method for exchanging value. We considered blockchain technology related to issues of trust, along with uncertainty in its related scalability, and security for AML in transaction processes. Our empirical findings indicate that commercial banks can indeed reduce resources spent on AML compliance with a blockchain-based transaction infrastructure. The effectiveness of such technology implementations are yet to be studied and measured, though this will surely be undertaken in the coming years as the diffusion of this technology advances.

8. Conclusion

We conclude with our contributions to theoretical and practical knowledge, how the technology applies in the case settings we discussed. We also will share our coauthors' practice-related assessments on the importance of studying other emerging technologies that are appropriate for future research study in this domain.

8.1. New knowledge contributions from this research

An exploratory process model for blockchain impacts. We offer an exploratory process-focused assessment of blockchain technology's impact on AML compliance. Our first contribution is focused on modeling blockchain's impact on AML processes and assessing what it means for commercial banks and other financial institutions. By focusing on blockchain's practical impact on AML processes, including transaction monitoring and KYC, we noted that it can enable banks to develop new AML compliance processes requiring fewer manual resources. Our theoretical model contributes exploratory knowledge about how this may reduce a bank's compliance costs, particularly when many other banks participate in the same blockchain network. This provides a foundation for research to estimate bank savings of compliance costs made possible by blockchain-based AML, though it may be too soon to launch a full-blown empirical study that would target these issues. Additional industry adoption and implementation work needs to be

carried out, so it is possible to capture empirical data rather than observe what is likely to happen based on the applicable theory and managerial logic. This prompted our exploratory qualitative empirical approach.

A GDPR-compliant KYC model. Our second contribution is how a novel blockchain with built-in transaction participant identification can affect the practical procedures involved in KYC processes. The literature on blockchain and compliance that we discussed offered suggestions for how blockchain can optimize KYC and eliminate unnecessary overlapping verification. Many proposed solutions have run into European GDPR issues though, as data on a blockchain cannot be deleted and may be difficult to truly anonymize (iCommunity Labs, 2023). We have not identified any research that examines blockchain with embedded IDs that seeks to link real-world identities with transactions – without breaching GDPR compliance. Taking this into account, we studied the Concordium blockchain as an element that contributes to the business and economics literature with insights on the practical use cases of a solution not encountered before. This work also contributes to the fintech research literature, through its use cases for AML solutions, which have not been described before. Also, by relating the Concordium blockchain to leading commercial banks' KYC processes, we provided knowledge on how blockchains with integrated ID functions can reduce manual work in KYC processes – another attractive topic for future in-depth research.

Blockchain's impact on transaction monitoring. Our third contribution is related to blockchain's likely impact on transaction monitoring. We levered our exploratory instrumental case study approach to banks' AML processes by considering transaction monitoring. This is comparable in importance to KYC processes in terms of the operating expenses they consume. More specifically, we investigated transaction monitoring processes to discover areas where the blockchain-based AML approach can potentially improve the processes. This fills a gap in the literature regarding blockchain-based AML solutions. Moreover, it encourages further research into how transaction monitoring can be redesigned for a blockchain solution, and what implications it has for the industry's capabilities going forward and returns of new technology investments in this area.

8.2. Observations related to other emerging technologies for AML practice

The contributions of this research have practical implications in other ways, too. We discovered the capabilities of layer-1 blockchain and why they apply directly to processes in an established financial institution. We considered knowledge about how and what areas the technology may be utilized in established businesses, with relevance for emerging blockchain firms and new fintech firms. They all need to be aware of areas where blockchain technology can beneficially impact their operations. Our findings allow them to develop more accurate business cases for the new technology based on the settings we were able to explore.

Other important opportunities are available for different emerging technologies. In the dynamic landscape of AML practices, integrating generative AI presents a significant opportunity for enhancement. With advanced data processing and pattern recognition capabilities, GAI can identify complex, non-linear transaction patterns, and transaction amounts and unexpected counterparty identity anomalies indicative of money laundering activities. Efficiently analyzing vast datasets, including transaction histories and customer profiles, GAI approaches are likely to excel in generating predictive models and risk assessments with greater accuracy at a faster speed than traditional methods can (Goldbarsht, 2023). Further, GAI tools are likely to facilitate continuous updating and refinement of AML models, to adapt them for emerging laundering techniques. When combined with blockchain's transparency and immutable record-keeping, GAI offers a new proactive approach to AML compliance, enabling real-time detection and responses to suspicious activities. This synergy enhances the efficiency of AML processes and supports a more robust financial system against the evolving tactics of financial crime (Chen et al., 2021, Kalia, 2023). Despite its immense potential, collaborative efforts are needed to address challenges like data privacy and ethical concerns for effective integration.

Quantum computing, alongside GAI, has potential to further revolutionize AML assessment by employing advanced anomaly detection and process monitoring at lightning speeds. Rapid processing of very large-scale datasets will enable the identification of hidden patterns in financial transactions, crucial for spotting money laundering activities (Herrmann and Masawi, 2022). This technology enhances cryptographic security too, ensuring safe handling of sensitive data in AML operations, while real-time transaction monitoring allows for immediate detection and response to suspicious activities. Quantum computing optimizes AML workflows and strategies, elevating the precision of financial crime detection and improving overall computational speed. Quantum communication security, also leveraging quantum mechanics, is an emerging transformative capability for ensuring the security of sensitive financial data, offering unprecedented certainty against eavesdropping or tampering (Egger et al., 2020). For this, *quantum machine learning* (QML) combines quantum computing and ML techniques, showcasing the potential for anomaly detection, model training, and enhancement of ML models, with applications in AML practice and real-time fraud detection in financial services (Grossi et al., 2022).

8.3. Innovative reshaping blockchain-based AML for regtech use

The ongoing wave of innovations we have discussed are poised to reshape the financial sector, with profound implications for AML, KYC, and associated regulatory frameworks. Quantum computing, with its groundbreaking capability to process enormous datasets at unprecedented speed, is introducing a new era of hyper-personalization in banking services that will come to fruition prior to 2030. This disruptive and transformational technology necessitates a reevaluation of AML and KYC protocols, as the advent of hyper-personalized banking experiences demands an agile regulatory response to effectively address the emerging risks (Orus et al., 2019). The continued effectiveness of regulatory measures hinges on the adaptation to the intricacies introduced by quantum computing, ensuring a harmonious integration of innovative technologies into the regulatory environment.

Simultaneously, the integration of AI into banking operations stands as a pivotal factor in automating and securing financial processes. AI systems play a crucial role in enhancing fraud detection, risk management, and compliance with AML and KYC regulations. Regulatory bodies must evolve to effectively accommodate these technological advancements, acknowledging the impact of AI on reshaping the banking landscape. The rise of *decentralized finance* (DeFi) and cryptocurrencies adds a layer of complexity to the regulatory environment, challenging traditional notions of money movement. The influence on existing blockchain-based AML mechanisms becomes pronounced as such technology becomes integral to ensuring financial transparency and security. The immutable nature of blockchain records offers potential advantages in AML by providing a secure and transparent ledger for tracking financial transactions. However, the evolving landscape demands continuous refinement of blockchain-based AML approaches to address emerging challenges and ensure their efficacy in modern banking.

8.4. Limitations

Next, we will highlight the scientific limitations that influenced our research and its findings. The research design we chose for an exploratory instrumental case study, our care with the methods for data collection, and quality assurance were appropriate, but several aspects are essential to look at more closely when assessing the reliability of this work.

For example, our analysis is based on fourteen interviews, which is close to the ideal number of interviews for this kind of study (Kvale, 1996). But, though our interviews for this research closely followed the

recommendations we identified from other authors, the success of this research inquiry still depended on our specific context. Our assessment of current AML processes and the outlook for ensuring more efficient compliance within this regime would have benefitted from additional interviews with executives at more Danish and other European banks. Interviews with more employees in KYC onboarding processes also could have strengthened our triangulation related to our data, in combination with the SOPs we applied. This was not possible in the timeframe we had for the present research though, which was limited by both our time-constrained organizational access, as well as the university's schedule for industry-sponsored graduate thesis research.

Another methods issue regarding the data is that all interviews were conducted online via the Microsoft Teams app – a Covid pandemic accommodation, and so not ideal. Still, online interviewing created a comfortable atmosphere since most respondents were interviewed in their homes. But it did not allow the same degree of intimacy and relationship building as physical, face-to-face interviews could have permitted: this created some distance between the authors and the respondents in our interview situation. Further, online interviews made it difficult to read the respondents' expressions and body language, and may have caused delayed responses, which also hindered our content collection.

The last limitation is about how we established response concordance in the interviewing process. Our practice was aimed to encourage the different respondents to share the same concepts to create commonality in understanding, as well as our own analysis and interpretation. It was hard to comply with this in practice when interviewing some of the respondents though. Blockchain is a novel topic, and some interviewees had different perceptions and ideas related to the use and adoption of blockchain. The Covid pandemic lockdown and our inability to form tighter bonds with our interviewees were also salient factors in our process. Nevertheless, each interview expanded our knowledge base, forcing us to reiterate and update some questions for the subsequent respondents. Motivated by a desire to explore the relevant concepts, we sacrificed the reliability that fully concordant interviews could have yielded, while opting for greater learning-as-we-went flexibility for new knowledge discovery. In the end, this proved to be a workable approach for our research team.

Investigating a general phenomenon by examining a specific case also has its limitations, as experienced qualitative methods field study researchers know well. We focused on just two firms: Danske Bank and Concordium. This small sample may have hindered our ability to provide reliable information about other relevant firms, but our work was intended to be exploratory, and carried out prior to seeking larger-scale funding and participation. Relying on interview data also made it so our empirical foundations were derived from individual perceptions of the issues and technologies under study, not what might be the more general perception had we conducted a sector survey or been able to obtain data from many firms. This is typical in exploratory research we pursued and was still an effective starting point.

As a final caveat to others, we should note that the same research carried out in other contexts and time periods may have yielded different findings, but we stand by our findings as the product of purpose-designed, early-stage exploratory empirical research. This does not undercut the importance of the present investigation though. *Context-dependent research* has allowed us to discover the richness of our fintech and commercial banking settings through reiteration, and then by distilling an aggregated picture of the related potential fintech innovation impacts – rather than following purely rule-governed, context-independent theory (Flyvbjerg, 2006). Indeed, there was so much to be learned from the interviewees. So, in this instance at least, the rich path for case study-based knowledge discovery proved to be the right one.

CRediT authorship contribution statement

Thomas Vinther Daugaard: Conceptualization, Investigation, Writing – original draft, Writing – review & editing. **Jakob Bisgaard Jensen:** Conceptualization, Investigation, Writing – original draft, Writing – review & editing. **Robert J. Kauffman:** Conceptualization, Methodology, Writing – original draft, Writing – review & editing. **Kwansoo Kim:** Methodology, Supervision, Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

Acknowledgement

Thomas Vinther Daugaard and Jakob Bisgaard Jensen appreciated assistance from the Master's Thesis Administration at Copenhagen Business School. Kwansoo Kim recognizes the Endowed Chair in Digitalization at Copenhagen Business School (CBS) for financial support. Rob Kauffman also is grateful to CBS for supporting his research under the Endowed Chair in Digitalization, with assistance from Gustav Eller Andersen and staff at external sponsor, Danske Bank in Denmark, as well as staff at Concordium. All errors and omissions are the sole responsibility of the authors.

Appendix

Appendix A, Table A1. Glossary of terms

Term	Definition	Source
Anti-money laundering	Disguising proceeds of crime and moving value via trade transactions to legitimize illicit origins. This can be achieved by misrepresenting price, quantity or quality of imports or exports.	Financial Action Task Force (FATF). (2006)
Asset specificity	Degree that an asset can be redeployed for alternative users without sacrifice of productive value.	Williamson (1991)
Bilateral governance	Agreements between parties in which each agrees to fulfill their role. Bilateral contracts involve an equal obligation or consideration from the parties, although this need not always be the case.	Hayes (2021)
Blockchain-based KYC	Knowing with whom they are trading is important. Banks use KYC processes for security through authenticating the counterparty. Process begins when customer agrees on relationship terms. Of. They send required dox (ID, credit card information, bills, etc.) for the bank to conduct KYC verification. Bank analyses them and certifies if customer is validated or rejected. Making this process blockchain-based ensures data capture, transparency, immutability, cost control, and info security.	Techskill Brew (2020)
Clearing	Process of updating the payee's and payee's accounts and arranging for the transfer of value.	Chen (2023)
Consensus algorithm	Process to achieve agreement on value of data among multiple nodes in distributed systems.	Bamakan et al. (2020)

(*continued on next page*)

(*continued*)

Term	Definition	Source
Contextual knowledge	Covers knowledge that experts develop by working in varied case settings; enables them to create new and often generalizable, cross-context knowledge.	Flyvbjerg (2006)
Context-independent & dependent study	Context-independent knowledge is basic textbook content. Social Science has not been effective in producing context-independent knowledge and theory though. Context-dependent knowledge discovery builds from verified observances toward more generalized knowledge with more data.	Flyvbjerg (2006)
Coopetition paradox	Simultaneous pursuit of cooperation and competition (coopetition) between firms, and the tensions that develop at individual, firm, and interfirm levels as a result.	Bengtsson et al. (2016)
Decoherence	Loss of a quantum state in a qubit. Environmental factors can cause the quantum state of qubits to collapse. A challenge in constructing a quantum computer is designing features that delay *state decoherence*, such as building specialty structures that shield the qubits from external fields.	Amazon Web Services (AWS) (2024)
Deterministic consensus finality	Algorithm with rules to reach agreement finality faster than probabilistic consensus does. Latter applies probabilistic mechanisms but process does not always result in consensus finality.	Vincent (2022)
Digital identity	A robust digital ID allows individuals without traditional identification to have a robust identification to access financial services and improve financial inclusion.	Financial Action Task Force (FATF). (2020)
Digital intermediation	The use of digital technology and platform capabilities to transform the creation, production, sale, distribution, and after-market follow-up and exchange beyond the simple methods of the 1990s.	Chircu et al. (2000)
Digital proof-of-stake	A consensus protocol in blockchains; offers a way to decide which user(s) validated new blocks of transactions and earn(s) a reward for doing so correctly.	McKinsey & Co. (2023)
Distributed proof-of-stake	Make blockchain networks more efficient by eliminating the energy-intensive computational mining process in proof-of-work protocols. PoS algorithms incentivize users to confirm network data and ensure security through a process of collateral staking.	Gemini. (2023)
Dominant design	The emergence of a single architecture that establishes dominance in a product class and indicates the maturation of an industry or a product's development.	Anderson & Tushman (1990)
Double-spending	Transacting with same set of digital assets more than once. This problem has plagued many digital money systems and is what most blockchain networks are designed to prevent.	Yaga et al. (2018)
Economics of governance	Processes to support economic activity and transactions by protecting property rights, enforcing contracts, and taking collective action for physical and firm infrastructure.	Dixit (2008)
Entanglement	When two systems link closely, knowledge about one gives you immediate knowledge about the other, no matter how far apart they are. Quantum processors can draw conclusions about a particle by measuring another. *Quantum entanglement* allows solving complex problems faster.	Amazon Web Services (AWS) (2024)
GDPR	European regulatory law that established obligations of data controllers and processors handling personal data on their behalf, with obligation to implement appropriate security measures, according to the risk involved in the data processing operations they perform.	European Commission (2024)
GAI	GAI focuses on generating new data or content that resembles a training dataset used to create it. Its error rate is more related to the quality and fidelity of generated outputs. Generative models strive to produce outputs that resemble the patterns and characteristics of the training data.	Kalia (2023)
Immediate payment finality	The moment at which funds, recently transferred from one account to another, officially become the legal property of the receiving party. Such payments thus become irrevocably settled.	Fernando (2023)
Instrumental case study	An instrumental case study aims to provides insight into an issue or refine a theory in which the case itself here is secondary and might be atypical of other cases.	Lucas et al. (2018)
KYC onboarding	Digital IDs used for identification & verification at customer's first opening of a new account.	Financial Action Task Force (FATF). (2020)
Large language models	Machine learning and neural network models that can comprehend and generate human language text. They work by analyzing massive data sets of language and are applicable in many settings.	Cloudflare (2024)
Layer-1 blockchain	A base blockchain on which secondary blockchain networks and applications are sometimes built. Bitcoin and Ethereum are the two biggest Layer-1 (L1) blockchains in the world. They provide basic infrastructure and security that Layer-2 (L2) blockchains need to function.	Lepcha (2023)
Null & alternative hypotheses	Null: a theoretical statement to disprove in empirical research of no effect of a variable on an outcome, with the alternative hypothesis, for which we attempt to give evidence of its truth..	
Quantum computing	A multidisciplinary field comprising aspects of Computer Science, Physics, and Math that utilizes quantum mechanics to solve complex problems faster than a classical computer can solve them.	Amazon Web Services (AWS) (2024)
QML	*Quantum machine learning* blends the capabilities of ML with quantum approaches to computation based on the use of algorithms that support qubit-based approaches to data analytics.	
Panoptic surveillance	The idea of panoptic surveillance was developed by French philosopher, Michel Foucault, in 1975 by viewing the *panoptic as* the disciplinary society of surveillance, which can be understood as a state of constant monitoring. The one that is observing is centralized and those who are being observed are never directly communicated with, like in department stores and MRT platforms.	Sociology Group (2019)
Quantum mechanics	Quantum computers solve some problem types faster than classical computers by leveraging *quantum mechanical effects* (e.g., *superposition, entanglement*, and *decoherence*). Some applications provide speed boosts, (e.g., for ML, optimization, and simulation of physical systems).	Amazon Web Services (AWS) (2024)
Regulatory technology	*Regtech* involves the application of various new technological solutions that assist highly-regulated industry stakeholders, in setting, effectuating and meeting regulatory governance, reporting, compliance, and risk management obligations.	World Economic Forum (WEF) (2022)
Relational contract	A contract that is primarily enforced by the moral suasion that two non- contracting parties have with one another, as opposed to a formal written or legally-recognized contract.	Li et al. (2023)
Self-sovereign identity (SSI)	An identity mgmt model that creates fraud-proof credentials to instantly verify their authenticity. Individuals have ownership and control of their digital identities without a central authority.	Dock (2024)
Settlement	Exchange of funds between a payer and payee in a transaction, so that the payer can use them.	Chen (2023)
Spillover effect	The impact that seemingly unrelated events can have on other settings. Though there are positive spillover effects, the term is commonly applied to negative impacts, like social sentiment has on the stock market due to inflation, firm-related news, and other unexpected events.	Kenton (2020)
Superposition	Like waves in physics, you can add quantum states to create another valid quantum state. You can represent every quantum state as a sum of other distinct states. This *superposition* gives quantum computers their parallelism, allowing them to process millions of operations simultaneously.	Amazon Web Services (AWS) (2024)

(*continued on next page*)

(*continued*)

Term	Definition	Source
Technological discontinuities	These are caused by technological innovations that depart dramatically from the norm of continuous incremental innovation that characterizes product classes; they may either affect underlying processes or the products themselves.	Anderson & Tushman (1990)
Transaction cost theory (TCE)	TCE levers Economics, Law, and Org Theory to understand economic organization. It does so in terms of firms, markets, and mixed modes, and views the allocation of economic activity as a decision variable. Firms act as governance structures, with consequences for how production occurs, and organizational design and strategy are implemented, and covers the contracting process.	Williamson (1984, 2010)

Appendix B. Interview Style, Process, Content, and NVivo Analysis

Style. In this study, we sought to foster openness and genuine dialogue in our interviews while maintaining focus on the research theme. The interviews allowed us to adapt to the interviewees' statements and make progress in areas related to our RQs. Each interview commenced with a briefing on the research purpose for the content, followed.by questions to elicit rich and spontaneous responses on different research aspects of blockchain-based AML. Our post-interview debriefing aimed to highlight valuable points that the interviewees shared.

Semi-structured interviews supported openness and a genuine dialogue, while keeping the focus on the research theme in exploratory empirical research. Their purpose was to allow the interviewer to adapt their dialogue to interviewees' statements and identify areas where relevant knowledge for the RQs could emerge. We very often use this approach when we do exploratory research involving content experts and management staff and business and technology leaders. We typically use questionnaires when there are tens or hundreds of consumers targeted. So, we ask the reader to appreciate the contrasting purposes of the more intimate data collection methods.

Before recording started, interviews were initiated with a briefing on the purpose for context and comfort, while allowing direct factual questions to be asked quickly. Two interviews had introductory warm-up questions that yielded rich and spontaneous descriptions and got the interview flowing. We similarly debriefed the interviewees by stating some of the most valuable points they provided to relieve post-interview tension. Interviews were conducted in an AML or blockchain-related mixed business-technical way, to uncover processes and concepts.

Process and content. This study emphasizes thematic questions aligned with a proposed theoretical framework for blockchain-based AML in banking organizations. The interviewing process leverages the professional insights of the interviewees, specifically probing their perceptions of the advantages associated with blockchain-based payments. The interview guide questions have been intricately linked to our RQs and overarching research themes, maintaining alignment with the theoretical underpinnings of the study. These inquiries deviate from conventional academic discourse and are designed to delve into the practical nuances of AML processes and blockchain technology, with a particular emphasis on business and technical dimensions. An example for a Concordium employee was: "*What are the benefits of conducting payments on a blockchain compared to in the current system?*" This relates to contracts and transaction cost theory. Similarly, a Danske Bank executive was asked "*If the burden of KYC increases, is the solution then to employ more people or to redesign the process?*" Our research view was to acquire input on how technology change theory might play a role. The interview questions thus were developed to encourage the interviewee to talk about their professional expertise to facilitate useful information exchange.

The interviewees are from different functions in Concordium and Danske Bank, as well as experts from Chainalysis and Napier. The objective of the Danske Bank interviews was to explore and assess current AML processes and identify shortcomings and why they appear. Eight employees were interviewed: five from the operational level, two from the executive level, and one blockchain specialist. This distribution was chosen as the operational employees are the ones involved in the processes of AML, our subject of analysis. The execs offered insights on the strategic challenges of AML compliance, while the blockchain specialist discussed how blockchain can be levered as an emerging technology for the established financial industry.

On the Concordium side, the objective was to understand how employees envisaged the technology's impact on the future economy and what processes Concordium's blockchain solution can mend. Five employees were interviewed, one with extensive experience in Danske Bank and another with broad experience in the financial industry. Two other interviews with industry experts enriched the research design with perspectives on the industry from outside of the two case firms. The first was with a Compliance Manager from Chainalysis, a company specialized in transaction monitoring on the blockchain. This interview provided insight into how AML functions for blockchain-based transactions. The second was with a former AML employee in Danske Bank and now a director at Napier, an AI-powered AML platform. This amounted to 14 interviews as the foundation of the analysis. In addition to the in-depth interviews, *standard operating procedures* (SOPs) of an excerpt of the AML processes within Danske Bank were used to provide additional qualitative data.

NVivo analysis and coding. We employed a careful coding process for the transcribed interview material to ensure a thorough understanding of the data. This process entailed the *identification and linking of keywords and themes directly to the content of the data material.* By doing so, we were able to categorize, collect, and connect substantial amounts of data efficiently. Our coding approach was largely deductive, influenced by our field study understanding of the investigated phenomenon and the coding process. This method aligned well with *thematic coding strategy*, where themes were not just identified but were also linked back to the broader context of the research. Such a strategy allowed us to maintain a balance between detailed familiarity with the content and an overarching view of the key themes emerging from each interview. This approach was instrumental in uncovering nuanced insights and ensuring that our analysis was rooted in the empirical data while being guided by our initial theoretical framework.

Through the coding process, we developed a total of 15 codes, which were integral to our analysis. Notable examples of these codes include "bank-based KYC," "bank-based transaction monitoring," and "friction." To ensure consistency and accuracy in our analysis, each interview was coded individually and then compared collectively. We utilized NVivo's software for coding, thereby enhancing the efficiency and effectiveness of the process. This coding process laid the groundwork for a condensed opinion analysis of the interview transcripts. By identifying natural meaning units and extracting and interpreting their main themes, we were able to analyze the extensive interview texts comprehensively.

In the process of this research, we collected new insights regarding the practical applications and challenges of blockchain technology in the context of AML compliance. The coding of interviews revealed useful perspectives on how blockchain technology, particularly in KYC and transaction monitoring, can substantially streamline compliance processes. One novel insight was the identification of specific frictions and inefficiencies in current banking practices that blockchain can potentially mitigate. Additionally, our study sheds light on the readiness and adaptability of financial institutions toward embracing blockchain solutions for their key application areas. These findings highlight the evolving landscape of AML practices,

including the opportunities and the hurdles in integrating advanced technologies like blockchain in the banking sector.

References

Amazon Web Services (AWS), 2024. What is quantum computing? Seattle, WA. Retrieved January 29, 2024, from https://rb.gy/dcj3gc.

Anderson, P., Tushman, M.L., 1990. Technological discontinuities and dominant designs: a cyclical model of technological change. Administrative Science Quarterly 35 (4), 604–633.

Baily, M.N., Litan, R.E. Johnson, M.S., 2008. The origins of the financial crisis. Brookings Institution, Washington, DC, November 24. Retrieved January 29, 2024, from https://bitly.ws/3abkm.

Bains, P. 2022. Blockchain consensus mechanisms: A primer for supervisors. Fintech Note 2022-003, Washington, DC, January 26. Retrieved January 29, 2024, from https://bitly.ws/3abjZ.

Bamakan, S. H.B., Motavali, A., Bondarti, A.B., 2020. A survey of blockchain consensus algorithms performance evaluation criteria. Expert Systems with Applications 154 (15), 113385.

Bank for International Settlements (BIS), 2019. Distributed ledger technology in payment, clearing and settlement: An analytical framework. CPMI No. 127, Basel, Switzerland, February 27. Retrieved January 29, 2024, from https://bitly.ws/3abjQ.

Belotti, M., Božić, N., Pujolle, G., Secci, S., 2019. A vademecum on blockchain technologies: when, which, and how. IEEE Communications Surveys & Tutorials 21 (4), 3796–3838.

Bengtsson, M., Raza-Ullah, T., Vanyushyn, V., 2016. The coopetition paradox and tension: the moderating role of coopetition capability. Industrial Marketing Management 53, 19–30.

Capital One Shopping, 2023. Credit card market share statistics. McLean, VA, December 28. Retrieved January 29, 2024, from https://bitly.ws/3ajXp.

Chen, J., 2023. What is clearing? Definition, how it works, and example. Investopedia, July 22. Retrieved January 29, 2024, from https://rb.gy/x8mvn4.

Chen, Z., Soliman, W.M., Nazir, A., Shorfuzzaman, M., 2021. Variational autoencoders and wasserstein generative adversarial networks for improving the anti-money laundering process. IEEE Access 9, 83762–83785.

Chircu, A.M., Kauffman, R.J., Wang, B., 2000. Beyond the 'eBay of blank': next stage digital intermediation in electronic commerce. In: Barnes, S.J. (Ed.), E-Commerce and V-Business, 1st ed. Butterworth-Heinemann, London, UK, pp. 43–78.

Cloudflare. 2024. What is a large language model (LLM)? Retrieved January 29, 2024, from https://www.cloudflare.com/learning/ai/what-is-large-language-model/.

Deloitte, 2023. Can blockchain turn the tide on financial crime? New York. Retrieved January 29, 2024, from https://bitly.ws/3abjt.

Dixit, A.K., 2008. Economic governance. In: Durlauf, S.N., Blume, L.E. (Eds.), The New Palgrave Dictionary of Economics, 2nd ed. Palgrave McMillan, London, UK.

Dock, 2024. The ultimate guide to self-sovereign identity. San Francisco, CA, January 11. Retrieved January 29, 2024, from https://bitly.ws/3aky2.

Egger, D.J., Gambella, C., Marecek, J., McFaddin, S., Mevissen, M., Raymond, R., Simonetto, A., Woerner, Yndurain, E., 2020. Quantum computing for finance: state of the art and future prospects. IEEE Transactions on Quantum Engineering 1, 1–24. https://doi.org/10.1109/TQE.2020.3030314.

European Commission, 2024. The general data protection regulation. Brussels, Belgium. Retrieved January 29, 2024, from https://bitly.ws/3anA4.

Fernando, J., 2021. Finality of payment. December 23. Retrieved January 29, 2024, from https://bitly.ws/3abhS.

Feyen, E., Frost. J., Gambacorta, L., Natarajan, H., Saal, M., 2021. Fintech and the digital transformation of financial services: Implications for market structure and public policy. Paper No. 117, Bank for International Settlements, Basel, Switzerland, July. Retrieved January 29, 2024, from https://bitly.ws/UUL8.

Financial Action Task Force (FATF), 2006. Trade-based money laundering. Paris, France. Retrieved January 29, 2024, from https://rb.gy/cd7zfi.

Financial Action Task Force (FATF), 2020. Guidance on digital identity. Paris, France, March 6. Retrieved January 29, 2024, from https://rb.gy/x9fdhi.

Financial Action Task Force (FATF), 2023. The FATF recommendations. Paris, France. Retrieved January 29, 2024, from https://rb.gy/r1teki.

Finus, M., McGinty, M., 2019. The anti-paradox of cooperation: diversity may pay! Journal of Economic Behavior and Organization 157, 541–559.

Flyvbjerg, B., 2006. Five misunderstandings about case-study research. Qualitative Inquiry 12 (2), 219–245.

Foster, R.N., 1986. Why leaders become losers. Chapter 2 in Innovation: The Attacker's Advantage. Summit Books, Singapore, pp. 26–43.

Foucault, M., 1995. Discipline and punish. Random House, New York.

Gauda, A., 2023. Finality in blockchain consensus. Medium, August 30. Retrieved January 29, 2024, from https://bitly.ws/3abeG.

Gemini, 2023. Proof of stake (PoS) vs. delegated proof of stake (DPoS). Cryptopedia staff, Liverpool, UK, October 23. Retrieved January 29, 2024, from https://bitly.ws/3anuR.

Goldbarsht, D., 2023. Leveraging AI to mitigate money laundering risks in the banking system. Chapter 3 in Money, Power, and AI. Cambridge University Press, Cambridge.

Grauer, K., Kueshner, W., Updegrave, H., 2022. 2022 crypto crime report. Chainalysis, New York. Retrieved January 29, 2024, from https://rb.gy/7qupvr.

Grossi, M., Ibrahim, N., Radescu, V., Loredo, R., Voigt, K., Altrock, C.V., Rudnik, A., 2022. Mixed quantum–classical method for fraud detection with quantum feature selection. IEEE Transactions on Quantum Engineering 3, 1–12.

Hayes, A., 2021. Bilateral contract: Definition, how it works, and example. Investopedia, May 2. Retrieved January 29, 2024, from https://bitly.ws/3abeq.

Herrmann, H., Masawi, B., 2022. Three and a half decades of artificial intelligence in banking, financial services, and insurance: a systematic evolutionary review. Strategic Change 31 (6), 549–569.

Hull, J.C., 2018. Risk Management and financial institutions. John Wiley, New York.

iCommunity Labs, 2023. Blockchain and GDPR. Retrieved January 29, 2024, from https://rb.gy/za1vup.

Kalia, S., 2023. Potential impact of generative artificial intelligence (AI) on the financial industry. International Journal on Cybernetics & Informatics 12 (6).

Kenton, W., 2020. Spillover effect. Investopedia, September 29. Retrieved January 29, 2024, from https://bitly.ws/3abdL.

Kuperberg, M., 2020. Blockchain-based identity management: a survey from the enterprise and ecosystem perspective. IEEE Transactions on Engineering Management 67 (4), 1008–1027.

Kurum, E., 2020. Regtech solutions and AML compliance: what future for financial crime? Journal of Financial Crime 30 (3), 776–794.

Kvale, S., 1996. InterViews. Sage, Thousand Oaks, CA.

Lepcha, M., 2023. Layer 1 (Blockchain). Techopedia, July 8 Retrieved January 29, 2024, from https://bitly.ws/3abdy.

LexisNexis Risk Solutions, 2022. True cost of financial crime compliance study. New York, Retrieved January 29, 2024, from https://risk.lexisnexis.com.

Li, X., Kauffman, R.J., Kim, K., 2023. Within and beyond firm boundaries: Can strategic digitalization & cross-firm information integration lessen complex uncertainty? In Proceedings of the 2023 Hawaii International Conference on Systems Science, Maui, HI.

Lootsma, B., 2017. Blockchain as newest regtech application: opportunity to reduce the burden of KYC for financial institutions. Banking & Financial Services Policy Report 36 (8), 16–21.

Lucas, P., Fleming, J., Bhosale, J., 2018. The utility of case study as a methodology for work-integrated learning research. international journal of work-integrated. Learning 19 (3). Special Issue, 215–222.

MacNeil, I.R., 1978. Contracts: adjustment of long-term economic relations under classical, neoclassical, and relational contract law. Northwestern University Law Review 72 (6), 854–906.

Malhotra, D., Saini, P., Singh, A.K., 2022. How blockchain can automate KYC: systematic review. Wireless Personal Communications 122 (2), 1987–2021.

Mazumdar, S., Jensen, T., Mukkamala, R.R., Kauffman, R.J., Damsgaard, J., 2021. Do blockchain and IoT architecture create informedness to support provenance tracking in the product lifecycle? In Proceedings of the 2021 Hawaii International Conference on Systems Science, Big Island, HI.

McKinsey & Co., 2019a. Blockchain in retail banking: Making the connection. New York, January 7. Retrieved January 29, 2024, from https://bitly.ws/3ajN9.

McKinsey & Co., 2019b. Blockchain's Occam problem. New York, January 4. Retrieved January 29, 2024, from https://bitly.ws/3ajMZ.

McKinsey & Co., 2019c. Transforming approaches to AML and financial crime. New York, September. Retrieved January 29, 2024, from https://bitly.ws/3abdZ.

McKinsey & Co., 2021. Solving the know-your-customer puzzle with straight-through processing. McKinsey on Risk 11, 38–44.

McKinsey & Co., 2023. What is proof of stake. New York, January 3. Retrieved January 29, 2024, from https://bitly.ws/3ajNm.

Merkle Science, 2023. Three reasons why the future of anti-money laundering rests on blockchain. Begaluru, India, undated. Retrieved January 29, 2024, from https://bitly.ws/3akza.

Mills, A.J., Durepro, G., Weibe, E., 2010. Instrumental case study. In Encyclopedia of Case Study Research, Sage, Thousand Oaks, CA.

Moran, S., Ghoshal, M., 1996. Bad for practice: A critique of transaction cost theory. Academy of Management Proceedings 21, 1. https://doi.org/10.5465/amr.1996.9602161563.

Nofer, M., Gomber, P., Hinz, O., Schiereck, D., 2017. Blockchain. business information and systems. Engineering 59 (3), 183–187.

Orus, R., Mugel, S., Lizaso, E., 2019. Quantum computing for finance: Overview and prospects. Reviews in Physics 4, 100028.

Patel, M., 2023. Consensus algorithms in blockchain. December 22. Retrieved January 29, 2024, from https://bitly.ws/3abmh.

Rapley, T., 2011. Some pragmatics of qualitative data analysis. In: Qualitative Research. Sage, Thousand Oaks, pp. 273–290.

Schlatt, V., Sedlmeir, J., Feulner, S., Urbach, N., 2021. Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity. Information & Management 59 (7), 103553.

Schmidt, C., Wagner, M., 2019. Blockchain and supply chain relations: a transaction cost theory perspective. Journal of Purchasing and Supply Management 25 (4), 100522.

Shapiro, C., Varian, H.R., 1999. Information rules: a strategic guide to the network economy. HBS Press, Boston, MA.

Sociology Group, 2019. What is panoptic surveillance? Michel Foucault and Jeremy Bentham. Blogpost, June 22. Retrieved January 29, 2024, from https://bitly.ws/3abmN.

Soltani, R., Nguyen, U.T., An, A., 2018. A new approach to client onboarding using self-sovereign identity and distributed ledger. In: In Proceedings of the 2018 IEEE International Conference on IoT, pp. 1129–1136.

Soltani, R., Nguyen, U.T., An, A., 2021. Survey of self-sovereign identity ecosystem. Security and Communication Networks 1–26.

Stake, R.E., 2005. Qualitative case studies. In: Handbook of Qualitative Research. Sage, Thousand Oaks, CA, pp. 443–466.
Techskill Brew, 2020. Blockchain verification & anti-money laundering. Medium, August 29. Retrieved January 29, 2024, from https://bitly.ws/3abnd.
Thammandru, A., Chakka, B., 2020. Recalibrating the banking sector with blockchain technology for effective anti-money laundering compliance. Sustainable Futures 5, 100107.
Thomson Reuters, 2016. KYC surveys reveal escalating costs and complexity, may 9. Retrieved January 29, 2024, from. https://bitly.ws/3abnn.
United Nations Office on Drugs and Crime (UNODC), 2022. Money laundering. Vienna, Austria. Retrieved January 29, 2024, from https://bitly.ws/3abns.
U.S. Government Accountability Office, 2022. As virtual currency use in human and drug trafficking increases, so do the challenges for federal law enforcement. Retrieved January 29, 2024, from https://bitly.ws/3akvY.
Vincent, T., 2022. Deterministic consensus in distributed system networks. Medium, June 22. Retrieved January 29, 2024, from https://bitly.ws/3abnp.
Weeks-Brown, R., 2018. Straight talk: Cleaning up. Finance and Development, International Monetary Fund, Washington, DC, December. Retrieved January 29, 2024, from https://bitly.ws/3a9H2.
Williamson, O.E., 1984. The economics of governance: framework and implications. Journal of Institutional and Theoretical Economics 140 (1), 195–223.
Williamson, O.E., 1991. Comparative economic organization: the analysis of discrete structural alternatives. Administrative Science Quarterly 36 (2), 269–296.
Williamson, O.E., 2010. Transaction cost economics: The natural progression. American Economic Review, 100(3), 673-690 (Nobel Prize in Economics Lecture, Stockholm, Sweden, December 8, 2009).
World Economic Forum (WEF), 2022. Regulatory technology for the 21st century. White paper, Davos, Switzerland, April 13. Retrieved January 29, 2024, from https://bitly.ws/3a9HV.
Yaga, D., Mell, P., Roby, N., Scarfone, K., 2018. Blockchain technology overview. National Institute of Standards and Technology, Gaithersburg, MD, October. Retrieved January 29, 2024, from https://bitly.ws/3a9Hr.