Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

FINANCIAL TECHNOLOGY AS AN ANTI-CORRUPTION TOOL: A REVIEW OF BLOCKCHAIN, AI, AND RegTech APPLICATIONS

ANAS ALQUDAH
Banking and Finance Department, Business Faculty, Yarmouk University, Jordan.

LARA ALHADDAD
Banking and Finance Department, Business Faculty, Yarmouk University, Jordan.

DUNYA KHALED ELWAKED
School of Management, Universiti Sains Malaysia, Minden, Penang, Malaysia.

Abstract

This review examines how emerging financial technologies, particularly blockchain, artificial intelligence (AI), and regulatory technology (RegTech), can serve as tools in the global effort to combat corruption. Drawing from case studies, regulatory literature, and forensic applications, the paper critically evaluates the technological affordances and governance challenges associated with these tools. The promise of blockchain's immutability, AI's predictive capabilities, and RegTech's compliance automation are assessed within the frameworks of institutional trust, accountability, and data transparency. However, the paper cautions against techno-optimism, emphasizing that without robust institutional backing and contextual adaptability, these technologies may be co-opted or rendered ineffective. The paper proposes a taxonomy of corruption types, discusses socio-technical risks, and highlights both successful and failed FinTech applications across jurisdictions. Ultimately, the study advocates for an integrated, ethics-sensitive approach that embeds technological solutions within broader policy, regulatory, and civil society frameworks.

Keywords: Anti-Corruption Technology; Financial Technology; Blockchain Governance; Artificial Intelligence In Finance; Regtech; Transparency; Digital Compliance; Smart Contracts; Financial Crime; Ethics Of AI; AML/CFT; Forensic Finance.

JEL Codes: D73**,** G28**,** K24**,** O33

1. INTRODUCTION

Traditional anti-corruption efforts encompass regulation and punishment. Rule Tokenization seeks to expand the scope of the law by assigning specific legal meanings to objects and utilizing them as proxies for concepts, institutions, and relationships. Designated entities that employ tokens allow them to create classes applicable to a broader range of actors than legal registries. While blockchain facilitates new forms of secure record-keeping, the financial services industry and security professionals primarily perceive it as a ledger within finance. The potential for speculation and illegality associated with cryptocurrencies draws considerable attention. Moreover, the materiality of blockchain, as a distributed ledger, prompts questions about whose truth it genuinely reflects (Khasawneh, Al Qudah, et al., 2025).

The notion of trust is closely tied to this. Blockchain facilitates agreements with untrusted parties; however, this does not mean that economic actors can safely disregard other avenues of trust. In high-value business transactions, other reputational considerations

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

are also taken into account. Paradoxically, secure record-keeping permits the default to alter agreements without negotiation, allowing untrusted entities access to restricted applications. Contrastingly, entertaining the possibility of record falsification permits executives access to financial, employment, or correlational data on employees for surveillance, espionage, and competition stifling.

Applications outside finance that rely on automatic action often polarize between perceived autonomy and algorithmic capture. Detaching fields from their human registrants inadvertently augments capitalism's hold on them by automating decision-making. Corporate finance is predicated on relationship building and in-depth knowledge of the firm. Automated engagement with counterparts within the context of linked ledgers and product offerings implies a definitive break from this tradition. Human oversight is nonetheless expected at certain junctures to stimulate competition. When the precise decision-making criteria are hidden from traders, loyalists signal collective interests to humans at exchanges to coordinate joint strategies (Akartuna et al., 2022).

2. UNDERSTANDING CORRUPTION

Corruption is the abuse of power or authority for private gain. The concept of corruption can be traced back to ancient times, at least to the Roman Empire, where governors were tasked with ensuring good governance by combating corruption in their local provinces. Yet, despite such historical antecedents, combating corruption remains a formidable challenge today (Villamil et al., 2022). The reach and scope of corruption vary significantly across countries and territories, often hindering their socio-political and economic development outcomes. The social scientific study of corruption has gained traction in recent years, as demonstrated by the proliferation of corruption datasets and the collective efforts of governmental and inter-governmental organizations, non-governmental organizations, and academic researchers aimed at understanding the causes and consequences of corruption, as well as the design and effectiveness of anti-corruption policies (Al Qudah et al., 2025).

Despite the extensive efforts mentioned above, there is no panacea to eradicate corruption (Akartuna et al., 2022). Beyond the social, psychological, structural, and situational causes of corruption, there are also high costs associated with acquiring and using the "right" data to study corruption. The lack of reliable and quantifiable measures of corruption, coupled with the intangible nature of certain forms of corruption, remains a significant barrier to understanding and combating corruption (Khasawneh, Hailat, et al., 2025).

Corruption can vary across two key dimensions: a source dimension and a target dimension. In terms of the source of the corrupt act, corruption can be classified into two subtypes: private corruption and public corruption. Private corruption, also referred to as corporate or political corruption, involves the misuse of power by corporate executives or politicians for personal gain. Public corruption, also known as bureaucratic or administrative corruption, refers to an arrangement between a bureaucrat and a citizen to exchange favors, in which the bureaucrat violates the state's rules governing public

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

service. Regarding the target of the corrupt act, corruption can also be classified into two subtypes: positive corruption and negative corruption. Positive corruption involves illegal acts that reduce costs or obstacles facing the procurer of favors, allowing them to enter or continue a transaction with a target. Black or negative corruption, on the other hand, involves illegal acts that force a target to concede costs or obstacles that were justifiably imposed on the corruptor, ultimately leading to the termination of a transaction or preventing the procurer of favors from entering a desired engagement (Al Qudah, 2009).

2.1. Definitions and Types of Corruption.

Corruption can be broadly defined as the abuse of public power for private gain. One of the challenges in studying corruption is the existence of definitions that vary from relatively narrow to very broad. Such struggles have led to the emergence of several typologies of corruption. Nevertheless, corrupt behavior can be categorized into three main types: bribery and quid pro quo, nepotism and favoritism, and false accounting and financial misconduct. All these complex elements can also be aggregated at a higher level, as the wealth sought through the abuse of public power can take various forms.

Bribery, the most widely recognized form of political corruption, is defined as the offering, receiving, or soliciting of an advantage as an inducement for actions related to the performance of a public function. It can be categorized into active bribery (offering bribes) and passive bribery (receiving bribes). This practice may also occur in the private sector, where it is similarly regarded as a form of corruption. Since the advantages offered to bribed authorities typically benefit only one party in the transaction, it seems reasonable to consider bribery the most standardized and prominent form of corruption. However, one could also argue that bribery is a symptom of more generalized forms of blatant corruption (Al Qudah, 2024).

In recent decades, the concept of bribery has repeatedly expanded, encompassing a broader range of inappropriate advantages and emphasizing procedural correctness while shifting the focus away from the abusive effects on behavior. The extensive use of definitions and typologies that group various behaviors under the same umbrella term has led to the emergence of often oxymoronic terms such as white-collar bribery, bureaucratic bribery, or agricultural bribery, raising the unhelpful question of when bribery would become non-corrupt behavior. Thus, bribery as a corruption offense needs to be clearly distinguished from its precursors or variants in antisocial behavior or the wrongful pursuit of wealth.

2.2. The Impact of Corruption on Economies

Corruption is a multi-faceted and complex phenomenon that is often difficult to comprehend, both in terms of measurement and conceptualization. Numerous definitions of corruption exist, none of which are universally accepted. Corruption may be defined as “the abuse of public office for private gain” or “the misuse of public power for private benefit.” However, many forms of corruption may involve the public sector, the private sector, or both. Corruption threatens prospects for socio-economic development, as it increases the cost of doing business, hinders the competitive performance of firms, incurs

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

unkind expenditures from energy output, and diverts resources from crucial human development investments (Akartuna et al., 2022).

Corruption undermines the functioning of governance by distorting the establishment of a legal framework, hindering political representation, eroding the autonomy of agencies, and weakening the rule of law through the manipulation of judicial systems while fostering favoritism, vested interests, and electoral disputes. Prominent social, economic, and political theorists provide a comprehensive understanding of corruption to explain its impact on the collective projects of citizens. Corruption creates disparities in the shared commodity of wealth through monopolistic positions and market foreclosure, often resulting from dubious anti-competitive regulations or discretion in providing public services. It leads to unequal access to competition law enforcement, investment opportunities, and threats from unscrupulous businesses, such as money laundering and drug trafficking (Al Qudah & Hailat, 2025).

3. THE ROLE OF FINANCIAL TECHNOLOGY

Following the emergence of digital finance in the 1970s, the early 2000s witnessed a significant increase in its adoption among consumers, driven by the widespread and affordable availability of internet access. Many countries were underbanked or lacked adequate banking systems, while low-cost mobile phones and public access to computer kiosks made it easier for consumers to access and interact with digital financial tools than ever before, including micro- and mobile-financing initiatives and bookkeeping programs. However, disruptive technology has the potential to reveal previously concealed information and transactional black boxes that were controlled by banks and providers, leading to widespread consumer disempowerment. The concern is that unauthorized intermediaries will exploit new technologies in the same way they have in physical spaces. In the context of criminal activity, fintech can be defined as any new materials and services commercialized, employed, or funded to facilitate criminal acts. The extensive growth of fintech will necessitate detection and monitoring (Zouaoui et al., 2018).

As fintech has expanded, so too have the ways to exploit it. Primarily, this involves consumer fraud committed by operators of illicit or misunderstood schemes that either overpromise, underdeliver, or both. However, other dangers emerge. The global banking system is currently interlinked, with financial records accessible to authorities that reflect activities outside regulated channels. Underbanked or cash-reliant nations and consumers face an elevated risk of lesser-known methods of financial crime. The resulting concerns surrounding fintech are threefold: designing safer systems, monitoring and detecting misuse, and controlling economic disruption (AlQudah et al., 2024).

Few industries have garnered broader recognition and undergone a shift toward increased regulation than the fintech sector. Every jurisdiction has some form of regulation affecting fintech on a global scale. The urgency for immediate compliance often overlooks the technological gap between compliance and innovation. This is especially evident in cryptocurrencies, where regulations vary significantly across jurisdictions. The

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

investigation process for illicit cryptocurrencies is lengthy, costly, and ineffective. This gradual approach presents both a risk to the mainstream adoption of illicit cryptocurrencies and a decline in trust in state currencies. The broader issue encompasses the need for epistemological tools, as the systems currently in use struggle to scale effectively.

3.1. Overview of Financial Technology

Financial technology has become increasingly popular among private companies worldwide. FinTech refers to technology-enabled financial services and products (Akartuna et al., 2022). This review defines it to reflect its growing prominence among private companies globally, as well as its discussions at the UN and G20 meetings. Financial services must broadly encompass any services related to money, including transferring, storing, investing, and saving. Technology should specifically denote digital technology, primarily consisting of digital hardware on consumer devices and internet protocols that facilitate transactions. It is distinct from non-bank payment technologies, which may hold greater significance in less developed regions. Blockchain technologies are also specified to focus on the use of distributed ledgers for cryptocurrency transactions and their associated innovations.

FinTech innovations are extensively reviewed based on the types of financial services they support. As new financial services emerge, classifications at various levels are also introduced. The review initially focuses on the types of financial services provided by FinTech innovations and is then grounded in the technological subfields they utilize. These innovations are discussed in enough detail to enhance understanding and stimulate engagement in debates about their impact on corruption. The emphasis is on publicly available financing, resulting in a lesser-known approach to funding their development upfront. Although several emerging technologies exist for promoting privately held financial products, they are briefly reviewed for completeness, given their potentially significant impacts in the future. Furthermore, other technological fields relevant to anti-corruption efforts in countries and industries with low confidence in politically independent and capable regulators are discussed, albeit with less comprehensiveness.

3.2. Importance in Modern Economies

Financial technology (FinTech), which refers to applying technology to produce or support financial services and products, is becoming increasingly integrated into the modern financial landscape (Akartuna et al., 2022). FinTech utilizes applications, platforms, and software as a service to deliver functionalities typically found in traditional financial services, including online venture capital, robo-advisory services, automated wealth management, peer-to-peer lending, brokerage, crowdfunding, and payment transactions. Since the global financial crisis, public and private interest in using technology for financial regulation and compliance has surged. The discussion of innovative technologies applied to market integrity and compliance with regulations is commonly categorized under the umbrella of regulatory technology, or RegTech. However, a crucial difference between

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

RegTech and traditional financial technologies is evident in their areas of application, where RegTech is focused explicitly on regulatory compliance. In contrast, all other uses of technology remain firmly connected to the studies of FinTech.

Technologies for providing and delivering financial services significantly impact the risk landscape of modern financial institutions and pose challenges to compliance with constantly evolving regulations. In recent years, there has been an explosion of excitement, expectations, and hope regarding the promise of several innovative technologies applied to the financial sector, particularly in the delivery of financial services and products. FinTech is primarily defined as technology-enabled financial services and products, incorporating applications, platforms, and software-as-a-service (SaaS) to deliver functionalities traditionally found in financial services. The rapid pace of innovation in delivering financial services has significantly evolved and altered recognized risks, as well as the associated regulatory frameworks.

4. BLOCKCHAIN TECHNOLOGY

All records, including government documents, medical histories, and property titles, are vulnerable to forgery or fraud (Pandey & Litoriya, 2021). Blockchain technology has been proposed as a solution to combat such fraud. Blockchain is a digital, distributed ledger shared among numerous computers on a peer-to-peer network. All transactions within the network are recorded as blocks that form a chain. Each computer in the network stores the entire history of the chain as one of its roots. Whenever a new pro forma is created, it is immediately propagated throughout the network for validation. After verification, the block is added to all computers, providing proof of both past and present transactions. The activity on the blockchain is tamper-proof, irreversible, and can be instantly verified by all network participants.

According to many observers, blockchain technology is expected to pose a significant threat to the global financial system (Muntean, 2019). Once recorded in a ledger, a transaction is secured from later forensic effects. The only way a transaction could be altered is if 51% of the nodes in the entire network were to unite. In a permissionless network, such as Bitcoin or Ethereum, this is virtually impossible, as such a community exists globally across different nodes worldwide. The presence of a community across various computers enhances its security, as it requires time, financial resources, and strength to take control of most nodes. Thus, records engraved on a blockchain cannot be amended without extreme effort. The complete history of computations can be traversed at any time to obtain transparency regarding various transactions. Trustless computing is now possible; work can be done without needing to trust it. This eliminates the need for trusted intermediaries, such as banks, notaries, auditors, and other entities that charge fees to facilitate reliable transfers.

4.1. Fundamentals of Blockchain

Blockchain is a decentralized, publicly distributed ledger that ensures the security, fairness, flexibility, and transparency of transactions over the internet, eliminating the

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

need for third-party intermediation. The presented transactions are organized into a chain of blocks to eliminate the risk of fraud and data alteration. Blockchain enables transactions to reduce costs, minimize errors, and eliminate inefficiencies, while enhancing speed and transparency. It has a wide range of applications, including cryptocurrencies, supply chain finance, healthcare systems, food supply chains, and energy, which are among its most common uses. These capabilities make Blockchain essential for governments, enterprises, and individuals, serving as a powerful anti-corruption tool for decision-makers. Cryptocurrency is the most notable application of Blockchain (Dong et al., 2023).

Blockchain relies on technologies such as hash encryption, digital signatures, consensus algorithms, and zero-knowledge proofs. Blockchains consist of linked data blocks. Each block in the chain contains a compiled record of transactions executed over the previous n periods. Blockchain is a series of blocks, forming a data structure that connects the most recently added block to its predecessor (Ellul & Pace, 2019). In each block, the hash is updated and attached to the header of the next block, creating a hash chain. The following description illustrates the data structure of a block: 1) Block height: The height of the block in the chain, with the genesis block assigned a height of zero. 2) Block header: The block header includes the version number, timestamp, previous hash value, and Merkle root hash value. 3) Transaction data: Transaction data includes the transaction number, the number of input and output addresses, and transaction outputs. 4) Nonce: A nonce is a 32-bit random number used in computation to ensure that the corresponding hash value of the block meets certain conditions. 5) Blockchain length: The total number of blocks in a blockchain. 6) Node count: The number of nodes in a blockchain.

4.2. Blockchain Applications in Anti-Corruption

Various anti-corruption applications of blockchain technology have been developed in response to the challenges in governance and transparency. Seven of them are explained here. Land registration involves recording ownership and claims to real estate. In many countries, this information is often inaccurate, incomplete, or falsified, leading to costly disputes, corruption, and informal occupancy patterns. Although considerable academic work has explored blockchain-based land registries, successfully deploying blockchain for land registration is a relatively new example. In Bidder, a web application allowing anonymous submissions of reports, suggestions, and citations was built. Public entities can utilize transparent public submissions for interpretation. Corruption issues stemming from a lack of competitive bidding can be addressed through public submissions with integrity related to provenance. A public blockchain enhances trust and confidence in the innovation, promoting transparency and accountability (Ellul & Pace, 2019). Blockchains have also been utilized to record government spending, ensuring that contracts and transactions conducted by public or subsidiary entities are transparent to the public.

In many countries, loopholes in technicalities buried in documents are exploited to evade scrutiny over public spending. Blockchains may help overcome the opacity associated with non-technical e-procurement systems. A simple search for contract details can reveal all organizations involved (Akartuna et al., 2022). In response to numerous notorious

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

bribery cases involving government/public contracts in various countries, blockchain-based government/public contracts have recently been introduced. Understanding corruption and collaborating with the right external actors can contribute to building a resilient system. Many public contracts are often criticized when non-expert teams win. In many Latin American cities, these contracts have remained opaque to the public, resulting in challenges and threats to the procurement rules. When applied to not only publicly but also privately and semi-publicly available specifications, hijacked contracts may provide a narrow-angle lens through which alternative futures can be visualized. Automated technical checks can serve to engage in crowdsourcing from use cases with uneven distribution. Strategic crowdsourcing allowances may address failures and inaction resulting from a lack of knowledge.

4.3. Case Studies of Blockchain in Governance

Several case studies illustrate how blockchain has been integrated into solutions that support governmental operations, especially in governance. One commonly researched area regarding global blockchain adoption is public safety. Government agencies around the world aid in solving crimes by utilizing third-party databases that are accessible through swaps. Internet data breaches present a risk of data leakage, potentially leading to various crimes. A party's inability to trust another may result in corrupt practices, such as tampering or market manipulation.

Based on blockchain features, one way to address these limitations is to establish a trustless relationship between parties. Trustless means that parties do not need to trust each other but can still work toward common goals, thereby creating records that no party can tamper with. The first step in this proposed solution is to form a consortium of the involved law enforcement agencies and third-party records providers. Popular sources include food safety databases and social network databases. A private blockchain is then implemented within the consortium. Each agency will run a full node in the private chain to store an immutable copy of the data. The second step is to embed and upload records, ensuring they are maintained in the blockchain. When initiating an investigation, the records can be accessed by sending a request to retrieve the evidence data for analysis. Trustless computation is achieved since neither the third-party source nor the agency data holders have control over the records in the blockchain (Rashideh et al., 2022).

Another critical area in governance is record implementation. A variety of operational records are maintained and exchanged across government sectors, including operational and facility records, transfer records, and financial transaction records. Improper implementation of records creates vulnerabilities to corruption and inefficiencies in the execution of government-assigned tasks. The inability to track records efficiently leads to issues such as a lack of control over aspects of involved parties in state procurement, the outbound surplus of consumer cash tickets, and ineffective annual budget management regarding procurement. Blockchain technology aims to automatically collect and share associated records of operations with embedded identity and automatic recording features. Using smart contracts, records are automatically sent to the blockchain and registered with the involved parties. For example, as an updated option, a merchant's

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

inventory schedule can be sent to the governmental blockchain, containing the list of food items being procured or processed, along with a signature to verify the supplier's identity and the transfer's legitimacy. With a contract corresponding to the code, a regulatory agency retrieves the records via the published controller code and status signature. Illegitimate records can be flagged in the blockchain by computing the conditions of the evidence database, which includes action, evidence, and stakeholders.

5. ARTIFICIAL INTELLIGENCE IN FINANCIAL SERVICES

Artificial intelligence (AI) is transforming the financial system by offering enhanced efficiency, resilience, and fairness at significantly lower costs than current arrangements. However, AI also poses risks to financial stability when its vulnerabilities interact with economic weaknesses. AI excels at identifying patterns in large, unstructured datasets for classification and prediction tasks. It can either assist human decision-makers or make decisions independently. A financial authority has two primary objectives: macroprudential regulation, which focuses on risk management, consumer protection, and fraud prevention, and financial stability regulation, which emphasizes the preservation of financial stability. Implementing macroprudential regulation is more challenging and less precise than financial stability regulation. It is useful to think of AI's application in financial policy as existing on a spectrum. The use of AI in the financial system is expanding rapidly, with applications in tasks such as risk management, credit allocation, fraud detection, and regulatory compliance.

Financial stability remains a key priority for the Bank of England. Many banks are starting to integrate FinTech into their services as customers demand greater choices, flexibility, and control over their banking experience. AI, a branch of FinTech, focuses on machine intelligence. The financial sector is an area where AI and FinTech can enhance banks' efficiency and reduce costs. More exploration of AI in the retail banking sector is necessary. The benefits and challenges of AI in retail banking have not been thoroughly investigated. In the UK, Santander Bank and HSBC have launched banking applications that utilize voice recognition. RBS is set to introduce its AI customer service assistant. Bank of America, Capital One, Société Générale, and Swedbank have been testing chatbots. Chatbots act as virtual customer assistants, guiding customers through text or online web chat interactions. AI is the technology that supports chatbots, and Swedbank's chatbot engages customers through the bank's website.

5.1. AI Technologies Overview

This section examines technologies that can enhance compliance, including Natural Language Processing, Machine Learning/Deep Learning, Neural Networks, Robotic Process Automation, and Human-in-the-Loop Approaches. It describes how these technologies can be utilized in various contexts, including Know Your Customer, Customer Due Diligence, Transaction Monitoring, EDD, Source of Funds, and Suspicious Activity Reports (SARs).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

Several technologies currently exist that have the potential to enhance compliance. Further research is expected to be published in this field shortly. This section outlines the capabilities that can be leveraged in developing compliance tools.

Natural language processing (NLP) refers to a computer program's ability to comprehend human language as it is spoken.

Machine Learning (ML) is defined as the ability of a computer program to improve its performance on specific tasks through experience and/or training. Three aspects of the definition warrant further elaboration: what is a computer program, what is a task, and what constitutes experience/training? This description outlines the expectations of machine learning.

Deep Learning (DL), a subfield of machine learning, has sparked significant interest in the development of artificial intelligence (AI) applications. Making data accessible in usable formats has become the bottleneck. Moreover, the gap between AI and non-AI experts in leveraging AI capabilities is widening. To address both challenges, an expert system that connects AI and text-based data analysis is proposed. As one of the pioneers in developing AI-enabled quantitative trading systems, the issues and their solutions at the technology stack level are discussed.

5.2. AI Applications in Fraud Detection

Financial fraud detection is essential for the well-being of both financial institutions and individuals. Fraudulent activities result in billions of dollars in losses each year and often have severe consequences, including unemployment, delayed retirement, and wage losses. Since 2000, both asset and revenue fraud have increased. Financial fraud detection techniques can be categorized into three groups. The first group includes techniques that assess the likelihood of fraud by scoring transactions. The second group mainly analyzes records to pinpoint signs of fraud. The third group involves monitoring transactions and records to look for evidence of financial fraud. The financial industry has broadly adopted the first group. Several scoring methods have been implemented, resulting in the development of statistical classifiers and probability scoring methods. Statistical classifiers such as Kendall’s tau, Picard, Gini index, cut-off mark, and Fischer discriminant are commonly used. To identify fraud indicators, financial institutions aiming to control fraud examination costs often use clustering and group modeling methods. Traditional string matching and searching methods are reliant on clear patterns of fraud established beforehand. Numerous financial records have been examined to detect financial fraud activity by verifying anomalies (West et al., 2014).

An efficient method for generating language from descriptions supports the optimal use of fraud detection systems. Operational details of the mapping from the DSL are provided to clarify the effectiveness of this approach. Misuse of financial systems can lead to financial loss not only for institutions but also for individuals if fraudulent activities go undetected. Many distinguished information and knowledge systems have been developed to support effective auditing and evidence collection for the detection and prevention of fraud. Existing systems primarily focus on detection. Since fraud detection,

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

prevention, and active deterrence are all vital, a more effective approach would be to address fraud as soon as and as comprehensively as possible. A high-level fraud symbol can represent a pattern or grammar encompassing fraudulent institutions, the activities they involve, the resources concerned, money flows, and associated regulations. It should operationally define a fed language. A fed grammar, coupled with an automaton, hypergraph, or state-automaton writing system, is proposed. Fraud experts communicate in the fed grammar, which translates into a detection grammar realization through analysis, automatically halting the signal transfer. Prototypical automated systems have been created for the semantic web and multimedia applications. The proposed fed language generates high-quality input and anticipates practical use of language generation software (Calafato et al., 2014).

5.3. Ethical Considerations of AI in Finance

Regulators and compliance functions increasingly rely on AI systems to address compliance issues identified during audit processes, determine which breaches to pursue, and decide how to allocate resources. They enter the realm of complex systems, where experts have little hope of understanding or predicting the systems' behavior or the consequences of their actions. The unintended consequences of machine learning algorithms that identify stocks for purchase or sale, as well as nearly all other processes defined in the system, are almost impossible to anticipate. Understanding these unintended consequences and the operations of self-evolving systems is concerning (Lui & Lamb, 2018). AI is complex, its repercussions are unintelligible, and thus, there is little hope of ever grasping its workings at a deep level. We humans can often override our decisions only after time-consuming deliberation and sometimes at significant cost.

To maintain trust and confidence in the newly augmented organizations, we must avoid uncontrolled black-box systems and complex systems that are unintelligible to end-user experts. Currently, the first-order effects of machine learning algorithms, including common errors such as skill mismatches or delays in acting until sufficient evidence convinces one of the model’s validity, are at least somewhat visible (Xu, 2024). However, the potential for unforeseen consequences that may inhibit correct human or system reactions and responses is concerning. Someone may be harmed by assuming that pattern recognition systems equate a loud explosion with an inflating balloon. Few realize the latent power of model choices; therefore, they often compete ineffectively against the incommensurable co-evolution of instrument designers and machines’ learning or evolution processes.

To restore trust and confidence in functions augmented with AI, they must maintain mathematical formalism and an explanatory model that clearly outlines expectations for inputs and outputs, which can feed back into the model. Its approximation capability must be analyzable, and it must generate confidence bounds on proposed outcomes. Customers of augmented organizations must also have a clear understanding of how AI arrived at its conclusions from first principles and preconceived data. Ensuring these representations are digitized, recorded, and stored will be paramount to ensure that when systems take control of decision-making and alertness increases, there is a degree of

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

clarity. Managers and risk officers will want to know what caused a market escalation or escalation of corporate problems; they will no longer accept that it merely happened because AI deemed so, and capital and strategy must follow accordingly.

6. REGULATORY TECHNOLOGY (REGTECH)

Regulatory Technology, also known as 'RegTech', has emerged as a potential lifeline for firms to ease the burden of regulatory changes. Barberis & Ross P. Buckley Douglas W. Arner (2017) argue that the transformative nature of this technology will be captured by a new approach at the intersection of data, digital identity, and regulation. This involves reconceptualizing financial regulations by integrating information technology (IT) and digital technologies, such as artificial intelligence, cloud computing, and big data analytics, to deliver effective solutions for regulatory procedures, including regulatory monitoring, compliance, and reporting. The feasibility of deploying RegTech arises from the simultaneous progress in financial expertise, technological advancements, and the growing volume of regulations. RegTech is often associated with financial technology (FinTech). Some contend that RegTech is a subsegment of FinTech that focuses on regulations, while others believe it should be viewed as an independent sector, as it provides services to various groups beyond just the financial sector. RegTech has the capacity to standardize, automate, and streamline manual activities, making the regulatory process more robust and efficient. RegTech solutions offer enhanced agility, as interconnected data sets can be organized through intelligent technologies. RegTech represents an exciting new development that promises to simplify compliance with evolving regulations while reducing manual processes (von Solms, 2021).

RegTech, which focuses on regulatory obligations and compliance, is recognized as a distinct segment of the FinTech industry. The term RegTech refers primarily to technologies that assist regulated firms in complying with regulations more efficiently. There are two categories of RegTech: RegTech providers and embedded RegTech, which is integrated into the existing systems of regulated firms. This report emphasizes RegTech products and advocates that RegTech is an innovation utilizing technology to reduce compliance costs and enhance regulatory transparency. RegTech has arisen in response to the surge in new regulations following the Global Financial Crisis of 2008. Since that time, regulatory and compliance costs have risen significantly. RegTech vendors aim to reduce these costs associated with regulatory obligations by offering compliance services that leverage technologies such as cloud computing and big data analytics. RegTech products are primarily cloud-based and delivered under a SaaS model.

6.1. Introduction to RegTech

Regulatory Technology, or 'RegTech', is defined as a technology that focuses on regulations, assisting agencies, enterprises, and institutions in complying with existing rules and legislation. RegTech companies aim to provide solutions that navigate the complex regulatory landscape of rapidly evolving regulations, enhancing information sharing between businesses and institutions to identify suspicious business activities

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

more effectively. FinTech is a subsegment of RegTech that focuses on regulatory compliance. However, some authors argue that RegTech should be considered an independent sector offering services to a diverse range of suppliers, aggregators, and clients (Von Solms, 2021).

The argument for separation rests on the view that the emergence of FinTechs is transforming the financial industry by introducing innovations that undermine the fundamentals of the banking business. In parallel, RegTech has developed as a tool or application to assist all financial institutions in managing their regulatory obligations; hence, both the Conduction Institute and the Ministry of Finance are clients of RegTech. The significant development of RegTech is attributed to the simultaneous emergence of several factors. The first factor is the marked increase in financial and prudential expertise in the financial services sector following the Great Financial Crisis. The second factor is the advancement of technologies that facilitate the standardization, automation, and acceleration of manual activities, making the regulatory process more robust and less costly (Arner et al., 2016). The third factor is the concurrent introduction of an unprecedented volume of regulations. As a rule, business institutions require a considerable amount of time to adapt to the concept of a payment service they need to offer, comply with newly issued regulations, and verify their alignment with the required objectives.

RegTech provides a playbook and solutions for addressing mismanagement, enabling business institutions to enhance warning and other systems across their products and services. Typical solutions provided by RegTech companies include investigations into the customer base and statistics related to it, the use of AI and other data-gathering and processing technologies to standardize payments and transactions, as well as consideration of aspects beyond the regulated banking industry. Almost all consumer-facing financial firms are required to comply with Know Your Customer (KYC) standards. Although the BG term is a misnomer and should be defined as OYC, not all suppliers would be subject to regulations. In contrast, suppliers and businesses delivering services to clients for various purposes and objectives throughout the service lifecycle could be viewed as corresponding (KYC) back-office companies.

6.2. RegTech Solutions for Compliance

Regulatory technology (RegTech) encompasses the use of technology to enhance regulatory processes, focusing on the production and delivery of regulatory information and compliance (Arner et al., 2016). RegTech can cover any area of compliance, including reporting, auditing, agents, supervision, and analysis. Firms can ensure compliance more efficiently and effectively. RegTech can learn to maintain regulatory compliance in a changing and dynamic environment through iterative modeling of compliance systems and iterative testing of that model against large amounts of real-world data. Expected outcomes and perceived risks can be inferred from past performance. RegTech can assist in the initial identification of noncompliance and the drafting of a report. Over time, RegTech could assess compliance performance across different market segments and help fine-tune the regulation itself. Firms and management

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

banks internationally must adjust both compliance and product offerings to meet an increasing number of new and changing regulatory requirements (Alqalawi et al., 2023).

The probabilistic model checks a compliance process against a regulatory rule. If compliance fails, the point of failure is identified, and the model analyzes the necessary changes to the process to restore compliance. Lastly, the outcomes and risks of regulatory rules are learned from regulatory, compliance, and outcome data, which can be used to refine regulations, make them more precise by quantifying terms, or identify implementation problems within RegTech models (Ryan et al., 2020). Through this technology, regulators learn to understand innovative products, complex transactions, and designed behaviors that could potentially harm the market and individuals. It can clarify the assumptions underlying product design, allowing unintended uses to be identified and addressed. RegTech may learn and model internal fraud patterns and their outcomes, infer possible collusions in transaction patterns, and identify the interests of non-transacted clients facing service change risks.

6.3. Impact on Transparency and Accountability

Discussions about accountability often consider the roles of institutions and civil society in exercising it. These attribution issues highlight structural problems related to accountability. A distributive, attentive, and responsive agency emphasizes the role of civil society in ensuring accountability. Accurately interpreting problems and relying on civil agents to uphold accountability raises broader social questions. Similar manuals for holder and seeker accountability would shift the focus from political and institutional failures to the social, cultural, and cognitive infrastructures that support and constrain agency. There are normative reasons to be concerned about the weakening linkages between civil society, public administration, and politics.

The advent of new technologies holds the potential to transform systems of accountability fundamentally. Until now, human agency has been necessary to aggregate and connect information on public behavior with formal interpretations of misbehavior and the anticipated effects of sanctions, considering both past and future contexts. The issue of outsourcing accountability may shift from one of manipulation and incomplete or false aggregation and interpretation to one of surveillance and click-feeding.

Many accountability frameworks related to public sector corruption aim for greater transparency regarding the resources, processes, and outcomes that the public mandates and funds. Anti-corruption measures must safeguard accountability, ensuring that diagnoses of poor performance in complex economic, social, and political systems are maintained and acted upon, rather than concealed in black boxes. Economic and social accountability in a world of competitive regulation presents a broader issue than how states exercise accountability over private regulatory systems aimed at anti-corruption. Additionally, public authorities may violate their accountability obligation if they either overreact or underreact to black boxes in ways that do not improve accountability.

STM has been regarded as the intelligence backbone of the digital economy due to its power for automation and strength in data handling. AI refers to a system or computational

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

device that can solve a problem in a manner deemed intelligent by a human being. The potential across multiple domains has generated vast interest and investment from both the public and private sectors. Rapid innovations in algorithms and methods have now made it possible for real applications to emerge. There is a need for policy and research to understand better how AI can be effectively implemented in various contexts, particularly with a focus on new opportunities in the public sector to facilitate innovative research.

7. INTEGRATION OF TECHNOLOGIES

The independent or combined use of technologies can help create a more transparent, fair, and equitable world. AI can deliver a network monitor and create a level playing field for deals and contracts, while blockchain can provide immutable records. AI, blockchain, and interpretable AI are needed in close combination to find the proverbial needle in a haystack (Arner et al., 2016). The potential use of these technologies, both combined and separately, is outlined for various entities, including banks, central banks, investigative bodies, regulators, and civil society. The challenges of implementation, financial inclusion concerns, and a way forward to achieve consensus and avoid fragmentation are also discussed.

The integration of technologies can leverage the complementary strengths of various technologies being researched and developed (Akartuna et al., 2022). For example, AI and big data combined can identify anomalies in large data streams. The absence of interpretable AI can hinder the understanding of risks associated with AI system findings. There is an opportunity to use blockchain in conjunction with AI to provide interpretable AI. Blockchain can track the parameters of the AI training data and model responsible for specific decisions, as well as the random seed of an algorithm. The models can be retrained using the recorded parameters, resulting in a version that is back-engineered with fewer resources. This approach would clarify the rationale behind AI decisions.

A deeper understanding of financial institutions' exposures could be achieved by integrating and processing vast amounts of data in ways previously inconceivable. Systematically classifying institutional exposures to risks such as financial crime, climate change, and COVID-19 would enable meaningful scenario and stress testing. This approach could help establish improved rules and limits governing these risks, viewing prudential, conduct, and safety as fronts in a common battle. The sharing of data among regulators would be encouraged by a technological means that allows for this exchange without exposing sensitive, firm-specific data, and a governance structure that ensures prohibitions against such sharing are respected.

7.1. Synergies Between Blockchain, AI, and RegTech

The triple synergy of blockchain, RegTech, and AI in anti-corruption measures ensures that the decentralized public ledger (blockchain) makes accurate data tampering impossible. Consequently, information stored on a blockchain provides unparalleled provenance to data across the financial ecosystem. Smart contracts enable contracts to

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

be enforced without third-party involvement. As a result, processes such as trade clearing can become partially automated, enhancing reliability, fault coverage, and system throughput. AI systems, which may be classified as supervised or unsupervised learning, rules-based systems, or hybrid systems, can detect data anomalies significantly faster than manual methods. They can sift through potential transaction datasets and initiate actions for human investigation in a considerably shorter timeframe than is typically required for such inquiries. Outcomes from machine learning, particularly supervised learning, can be consistently expressed as rules that can be coded into RegTech solutions for immediate automated enforcement and correction measures (Von Solms, 2021).

Machine learning may discover new behavior patterns that are not explicitly codified in contemporary knowledge bases. Solutions like peer-to-peer networks, privately vested miners, and public consensus algorithms can be deployed in RegTech applications. AI RegTech solutions provide rule-breaking measures that firms can immediately enforce using their regulatory technology. In collaboration with blockchain, enforcement measures will become significantly more powerful. Information loss and lack of control over event context are two significant challenges faced by AI RegTech solutions. These problems can be alleviated by integrating the solutions as data providers into a blockchain, which enables operational auditability and comprehensive monitoring of the knowledge lifecycle.

In addition to RPC-based communication, message queues, edge-based processing, and in-stream transformation/persistence may be utilized by any analytic RegTech solutions. Events generated by machines and conveying messages about changes in a compatible manner can be described in a blockchain, which will provide all users with event data provenance and trust. Like large, customizable glass walls that provide firms with real-time monitoring capabilities, streaming business dashboards are powerful enough to define corrective actions before measurable consequences occur.

7.2. Challenges in Integration

The effectiveness of financial technology as an anti-corruption tool hinges critically on its integration with existing institutions. Blockchain technology and other fintech applications cannot be viewed as “silver bullets” to eliminate corruption entirely on their own. Transparency and accountability must be fostered by the institutions using these technologies; otherwise, their anti-corruption potential is hamstrung. While blockchain’s anti-corruption potential is evident in the most developed use cases, a general lack of understanding of blockchain systems means this potential will be largely squandered (Chang et al., 2020).

In less developed nations, the general lack of robust institutions will hinder efforts to promote transparency and accountability, such as using blockchain. Transparency initiatives, such as public procurement contracts, will be ineffective in combating corruption if there are no regulatory enforcement authorities empowered to investigate these contracts. Still, developing countries also have potential opportunities to support

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

blockchain-based public decision-making. Lower levels of digital legacy would facilitate a more centralized design of blockchain-based applications and potentially guide institutions that view anti-corruption as a negative phenomenon. To mitigate the challenges posed by limited statehood and address legitimacy issues from social communities, these projects will need to connect with traditional political and administrative decision-making processes regarding law, court, and pathway knowledge. Based on these lessons learned, this paper concludes with avenues for future research to further advance the understanding of the potential for fintech-based anti-corruption initiatives.

In addition to the trust provision mechanisms of transparency and accountability, incorporating oversight mechanisms would be valuable in fostering trust when robust institutions are lacking. This is especially relevant for corruption cases with lower risk. In such instances, overstepping transparency and accountability mechanisms may exacerbate the problem. Accordingly, significant research is still necessary to investigate the socio-technical perception of trust, to elaborate on use cases based on risk, and to shed light on the counterintuitive pathways for designing blockchain systems (Akartuna et al., 2022).

8. CASE STUDIES

This research examines the application of a machine learning tool for identifying illicit Bitcoin transactions and its associated forensic requirements. First, the methodological framework is discussed in detail, demonstrating how to approach anomalous transaction detection with Graph Attention Networks, which show better performance than traditional networks. Next, decisions regarding the dataset and assessment strategy are explored. Novelty detection is presented. Results highlight similarities between observations using GAT and GCN, with the latter being preferred as a solution for AML/CFT due to its more straightforward implementation and stronger mathematical description (Al Qudah et al., 2019; Pocher et al., 2023).

Money laundering (ML) and terrorist financing (TF) pose significant threats to national and economic security by generating anonymous resources. To address this challenge, countries implement regulations on financial institutions. ML jeopardizes marketplaces as illicit actors aim to exploit regulated entities for profit. Cryptocurrencies have experienced a dramatic price surge, captured the attention of both the technology and investment communities, while simultaneously served as a primary vehicle for illicit activity due to ineffective regulation. Bitcoin transactions are irreversible. This paper examines the operational and technological challenges in monitoring, with a particular emphasis on forensic capabilities. The first advantage of DAGA approaches identified is the potential for emerging detection options. A related research avenue involves the jailbreaking of readily available blockchain cleaning toolkits. The second advantage is that it offers practitioners a roadmap for implementation. Regulation, illicit finance typologies, and model risk should be considered concurrently. Treating these three axes as separate objectives would result in underperforming solutions (Akartuna et al., 2022).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

Overall, expectations should be calibrated based on an understanding of the model and the regulatory environment. Datasets should remain widely shared yet somewhat proprietary. New sources are unlikely to be sufficient for producing better performance estimates, considering the potential devaluation of data pipelines that are not continuously updated by law enforcement. Research into the latest DeFi use cases involving bad actors would best guide banks in targeting the most probable funding cases. However, the pursuit of the highest and riskiest profits could entice illicit actors to conceal their actions further. Research could unveil novel countermeasures; however, information asymmetries are widespread. Efforts should focus on identifying and sharing improved de-anonymization tactics to integrate risk-evaluation models and ghillie classification.

8.1. Successful Implementations in Various Countries

In Mexico, in an unprecedented move to decentralize control of its debt auction process and reduce lag time from posting to settlement, the central bank (Banco de México) has made all state debt auction data available on the federal government's open data portal and is pre-aggregating it (Akartuna et al., 2022). This is complemented by real-time monitoring of participation by various public sector entities, along with a well-publicized letter of expectations from the central bank governor to the minister of finance. It is also noteworthy that, despite the sale of p-products, liquidity has dramatically improved in the secondary market, limiting profit margins and reducing transaction costs. Moreover, all issues, buying and selling activities, and interest payments of state debt securities can now be tracked through a free investor assistance system that allows access to test scores from exercising arbitrary fields in the public tender and secondary trading records.

8.2. Lessons Learned from Failures

Despite the great potential of FinTech to promote anti-corruption efforts worldwide, it is essential to highlight the lessons learned from past failures. These lessons stem from a review of the literature, which highlights the negative aspects of technology and FinTech applications that may have facilitated corrupt activities.

In hindsight, the tunable centrality measures of the empirical network may have influenced the averages of the asymmetry, clustering coefficient, and path length of the generated graphs. Testing against growth factors of networks and transactional filters is worthwhile. Complex networks, such as those in Bitcoin, where link dynamics depend on node characteristics, have been shown to evolve in a self-organizing manner. In this respect, it would be interesting to examine the evolution of the network with a time-consistent index, such as the average degree or the total number of edges (Pocher et al., 2023).

As previously stated, this was the first application of so-called FinTech (implicit) technology for AML/CFT purposes, providing an experimental model. Meanwhile, the first machine learning approach for Bitcoin was introduced with promising results. However, other forensic methods exist, and some are tailored to detect Bitcoin-only criminal activities that fall outside the classification trained for this experiment (Akartuna et al., 2022). Different approaches, such as clustering, guessing, and probability calculations,

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

also demonstrate superior performance compared to the regression approach. Among the machine learning models, Support Vector Machines appear to offer a better-balanced trade-off between resource demand and performance. Nonetheless, the goal was to establish the best baseline for future research, and at the time, this was the optimal combination of speed and performance. As more research emerges and applicable models are shared, the regression-based approach may be reconsidered. Simultaneously, the optimal combination of classifiers and hyperparameters discussed in other studies outside of the AML/CFT domain may be tested.

9. FUTURE TRENDS

The rapid development of financial technology (FinTech) presents an excellent opportunity for the future of anti-corruption (AC). Distributed data storage, artificial intelligence (AI), and other tech-driven solutions will significantly enhance transaction clarity as well as pattern identification. Together, these advancements enable the forensic analysis of corruption networks without relying on vulnerable or unreliable human testimony. Interoperable and immutable reporting standards will ensure that all transaction types and data points are delivered accurately, transparently, and in a timely manner to regulatory authorities. Furthermore, these technologies enable a “light-touch” regulatory approach, allowing smaller players to easily enter the regulatory system, yet pose a danger once they are inside. Rules can be automated and enforced immediately. Crazy ideas turn into products. Models improve as data flows freely around the world, enabling instantaneous forecasting. Great power amid significant risk.

Conversely, the emergence of advanced technological capabilities will not eliminate corruption but merely make it easier and more profitable. Even as corrupt firms strive to adopt these tools, existing loopholes in the regulatory framework will also take on a digital form, as many companies can still operate unchecked and unenforced. Properly regulated fiscal and business institutions must be established to foster the growth of healthy FinTech. Truly groundbreaking innovations have always relied on accessible business models and regulatory frameworks within which they can be applied. That said, as this type of business development matured and prior rapid growth led to systemic failures, disruptions began to occur. Loopholes were patched, and reigning in became a priority. The same prospect is anticipated: regulators must stay ahead of seized opportunities or risk being blindsided and overwhelmed by chaos (Al Qudah, 2024).

9.1. Emerging Technologies in Finance

Disruptive technologies, defined as those that introduce a product or service or transform the current market about existing procedures, applications, and markets, pose a risk of becoming tools for money laundering or terrorist financing (ML/TF) as market valuations soar and public interest increases. The most disruptive financial means widely regarded in the coming years are expected to be digital currencies that utilize distributed ledger technology for their settlement. High volumes of transactions, fast payouts, and the absence of intermediaries through fintech solutions raise concerns about the most effective ways to guard against illicit financial flows. The willingness to pay in cash to

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

prevent cash transactions from being detected not only enhances the economic efficiency of virtual assets in ML/TF methods and mechanisms, but the fully digital transaction model also hinders investigators' substantive involvement or their ability to gather evidence (Akartuna et al., 2022).

Removing anonymity is crucial for preventing money laundering and terrorist financing. For instance, since zero-knowledge is vital in creating mechanisms for proof-of-purchase of both Monero and Zcash, regulatory agencies have resisted the notion of either or both currencies becoming legal tender. However, the underlying technology stacks could significantly influence ML/TF activities, leading to the expectation that any technology that obscures the underlying participants of a transaction could be associated with Chokepoint 2.0 and have broader applicability than virtual assets alone. The development of zero-knowledge proofs could assist ML/TF activities beyond the cryptocurrency domain: evidence of a transaction amount could facilitate after-the-fact transfers of cash without requiring verification of the source of that cash, whether illicit or from legitimate ventures. ML/TF actors might gain greater credibility from these systems, and their usage could expand to other sectors. Zero knowledge could offer benefits as a service or through an extortion model.

While regulatory agencies assert that ML/TF funds should be placed into a financial institution, analysis of the methods and mechanisms suggests a more substantial reliance on decentralized or unregulated financial means. The situation is more complex in practice, as the same ecosystem fuels some forms of crypto asset use while hindering others. As funds within the ecosystem increase, more tools will become available to convert ill-gotten wealth into real-world assets, as exchanges target more jurisdictions and chains become custodial wallets.

9.2. Predictions for Anti-Corruption Efforts

Consistent with prior qualitative studies in this domain, experts believe that the bulk of this technology will be more widely adopted and enter the mainstream within the next 5–10 years (Akartuna et al., 2022). Respondents are somewhat optimistic that global anti-corruption efforts, particularly about new anti-corruption technologies, are poised to grow and prosper (or at least not decline) over the next 5–10 years. They expressed some concern that low-latitude countries, with their weak institutions, might fall behind again in adopting new technologies. This could further exacerbate existing inequalities, with a risk that corruption will infiltrate the borderless architecture provided by digital technologies and the internet. Additionally, the pace of technological innovations in the anti-corruption arena, including compliance tools, might even outstrip the pace of governance responses within institutions operating under arguably outdated models. In that light, it might not be out of the question to expect an ‘AI’ of sorts where corrupt agents leverage text, image, and video generating tools similarly to predictions made about lab-created viruses and AI-generated malware.

Experts reiterated several caveats raised in Phase 1: the diabolical nature of snake-oil technologists; governments' tendencies to misuse technology to exert power over the

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

populace; the bifurcation of the ecosystem, where unsafe countries might outlaw or legally control the upstream designs of safe technologies; and concerns that the code of anti-corruption technologies might become too complex for anyone to find exploitable design or programming errors reasonably.

10. POLICY IMPLICATIONS

The premises of this review suggest that large-scale financial technology mechanisms within the field of information technology exist to help mitigate corruption. Subsequently, the large-scale applications of big data, artificial intelligence, machine learning, blockchain, and regulatory technology are examined in relation to their impact on corruption. These broad categories of technology provide mechanisms that furnish tools for those seeking to prevent corruption, conduct analyses that can better reveal corruption if it exists, and offer resources for those who wish to combat corruption after it occurs. Some of the available applications in each category are presented, along with strategies for considering their use in combating corrupt acts within a financial context.

As a field of policy scholarship, corruption is defined as “dishonest or illegal behavior, especially by powerful people” in general, and “an act of corruption” specifically. There are, of course, numerous elaborations of that set of definitions, but collectively, they reflect behavior that “includes, in some sense, a departure from the canonical definition of a principal-agent relationship,” which helps frame ethical considerations, particularly regarding financial technology applications in contexts that transcend national borders. Financial corruption is primarily understood as the act of “influencing someone not to carry out their official duties fully and faithfully,” while also considering whether there are financial technology streams that assist in complying with statutes designed to combat foreign corruption.

Several conclusions can be drawn from this review. First, there are financial technology solutions currently available that fit within the discussed categories and assist in combating corruption. While these solutions may not be specifically designed for that purpose, they provide crucial building blocks for those who wish to engage in such efforts. They also reflect enthusiasm in the technical community for this task. Second, while the identified technologies are on-the-shelf solutions for their proposed applications, they are not typically off-the-shelf innovations. Their practical implementation would require substantial investments and, at times, sophisticated maintenance. As a result, only organizations with significant resources are likely to be able to utilize them effectively. Finally, some areas appear technologically ready for innovative development related to financial corruption, such as the detection and prevention of corruption through agent kickbacks, collaborative pilots involving various agents, ensuring the integrity of source documents, and mitigating information integrity issues in behind-the-scenes payments.

New payment methods represent modern ways to complete financial transactions and have long been viewed as risks, especially in developing countries that lack extensive financial services or regulatory compliance. These new payment methods include mobile money transfers and prepaid cards. Currently, financial services are the primary focus of

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

regulations that require financial institutions to conduct customer due diligence to identify suspicious transactions. However, innovation is rapidly digitizing traditional services, facilitating remote and anonymous access to online banking and fundraising. There has been a 'significant growth' in suspicious activity reports filed by these services. Authorities have struggled to keep pace with the advancements of modern criminals, who have created innovative methods to evade regulations.

10.1. Recommendations for Policymakers

The results of this review provide policymakers with multiple recommendations. First, donor organizations and TI agencies should identify, and support models based on successful pilots for regulated stablecoins and Decentralized Finance (DeFi) instruments that incorporate strong anti-corruption features, as part of providing otherwise non-existent financial infrastructure for contextually appropriate billion-plus unbanked populations. Second, there is a need for impact evaluations of existing FinTech deployments in LDCs to identify effective models, including back testing the past decade of blockchain-based eCash initiatives in the context of AML/CFT (Akartuna et al., 2022), and AI options that offer possibilities for holistic controls complementing existing state measures in jurisdictions where political integrity is too compromised for honest tax collection. Third, development efforts should be made to enhance existing architectures for transparency (regulated DeFi). Such efforts would require ongoing support for multi-stakeholder architecture design, development, and management, involving the private sector, as well as TI organizations and LDOs.

Fourth, policies governing the selection of AI development, deployment, and adoption partners and projects should be established based on research that identifies potential new forms of impermissible discrimination and the necessity for compliance risk assessments throughout the ML pipeline. A global database and governance structure, based on NGOs, should be considered to register AI tools and provide impact assessments from various perspectives, supporting the decision-making processes of civil society, governmental AI partners, funders, and adopters. Fifth, trusted frameworks should be explored to crowdsource and cost-effectively test the integrity of GANs for different classes of FinTechs or tax policymakers' use of social media bots. These frameworks could rank financial services based on their potential involvement in corrupt schemes, enabling policymakers to assess the robustness of brand deployments.

Sixth, principled alert frameworks connected to existing anti-corruption compliance infrastructures and assessments should be developed to guide reporting on compliance-quality concerns, unsolicited communications, corruption risks, or assessment impediments that contribute to non-compliance. The hope is that proactive measures to prioritize FinTech as a development focus within the G20 will be embraced and therefore globally financed and disseminated during the current golden window of opportunity, rather than waiting for a data breach that would incur greater long-term negative costs.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

10.2. Role of International Organizations

Financial Technology (FinTech) innovations have been increasingly adopted in both the public and private sectors to mitigate corruption risks. By streamlining the flow of information, encouraging proactive advocacy, and collecting vast amounts of real-time data, they can potentially support anti-corruption efforts. However, it is essential to recognize that FinTech is a mixed blessing, as it is also used by corrupt actors to bypass control measures. In this context, international organizations play a crucial role in helping countries realize the anti-corruption benefits of FinTech applications.

Over the years, member states have adopted a variety of resolutions and conventions targeting different aspects of corruption, including its definition, prevention, and punishment. However, the approach heavily relies on countries taking ownership and fulfilling their responsibility to develop and implement comprehensive and effective measures. The organization lacks the authority to impose corrective actions on countries. Consequently, political realities often hinder the successful implementation of the anti-corruption agenda. It is noteworthy that the organization incorporates FinTech into its capacity development efforts in a limited number of countries. In addition to milestone briefings, there is a need for efforts to deepen knowledge of FinTech applications and their relevance to anti-corruption initiatives, as well as to provide guidance on pitfalls and countermeasures against misuse and abuse.

The organization also plays a crucial role in implementing anti-corruption and integrity efforts through its organizational mandates and expertise. Several counter-corruption actions could be considered, such as analyzing current national systems against global best practices from a FinTech perspective; assessing risks, mitigation measures, and expected cost-benefit ratios of FinTech applications; and supporting investigations into illicit financial flows while assisting with relevant forensic inquiries in the Global South.

11. CONCLUSION

The contribution of financial technology to the anti-corruption field is explored through a scoping review of the literature in the humanities. Corruption conditions are examined and categorized into a taxonomy of 14 elements, organized by types, levels, and whether they are need- or capability-focused. Exploratory case studies of anti-corruption tools based on blockchain, artificial intelligence, and regulatory technology are assessed according to that taxonomy. The findings indicate that, while innovative uses of technology exist at both the international and national levels in terms of data connectivity and public awareness, anti-corruption tools based on these technologies may only address a limited set of capability-focused corruption conditions. Recommendations for future research agendas and the advancement of anti-corruption technology tools are offered.

Building on that empirical foundation, the second part of the article addresses the overarching research question, “To what extent and under what conditions can financial technologies serve as anti-corruption tools?” The literature is reviewed for insights into

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

five major technologies: big data analytics, the Internet of Things, blockchain, artificial intelligence, and regulatory technology. Emphasis is placed on blockchain, AI, and RegTech, as they are considered the most prominent and relevant technologies available to combat corruption and are the most frequently cited in the media and literature. The theoretical contribution of each technology to anti-corruption tools is assessed by evaluating its potential to disrupt and prevent corruption, including how it would be specifically deployed to achieve this.

The analysis of individual technologies is supplemented by countervailing forces, vulnerabilities, and antagonistic interests that may hinder the technology from serving anti-corruption goals. These forces also extend from the theoretical to the practical and reflect an “anti-technology” stance. The article concludes with a brief discussion of limitations, methodological notes on evaluation techniques, and suggestions for further case studies. As the struggle against corruption continues vigorously into the 2020s, positions for or against technologies can suggest how these technologies contribute to identifying specific priorities.

References

1) Akartuna, E. A., Johnson, S. D., & Thornton, A. E. (2022). The money laundering and terrorist financing risks of new and disruptive technologies: a futures-oriented scoping review. Security Journal, 1.

2) Al Qudah, A. (2024). Unveiling the shadow economy: A comprehensive review of corruption dynamics and countermeasures. Kurdish Studies, 12(2), 4768-4784.

3) Al Qudah, A., Bani-Mustafa, A., & Yamen, A. (2019). The mechanism of control of corruption and the rule of law: Mediating the effect of culture on terrorism financing. Journal of Money Laundering Control, 22(3), 498-514.

4) Al Qudah, A., & Hailat, M. A. (2025). Deciphering the links: evaluating central bank transparency impact on corruption perception index in G20 countries. Journal of Money Laundering Control, 28(1), 1-14.

5) Al Qudah, A. M., Al-haddad, L., & Aljabali, A. (2025). Combatting medical corruption: A global review of root causes, consequences, and evidence-based interventions. International Journal of Innovative Research and Scientific Studies, 8(2), 968-985.

6) Al Qudah, A. M. H. (2009). The Impact of Corruption on Economic Development-the Case of Jordan. University of Newcastle.

7) Alqalawi, U., Alwaked, A., & Al Qudah, A. (2023). Assessing tax collection efficiency of G20 countries: an analysis of tax potential, tax evasion and anti-corruption efforts. Journal of Money Laundering Control, 27(3), 489-504.

8) AlQudah, A., Al Zoubi, N. M., & Al Haddad, L. (2024). Mitigating Financial Crimes: How Anti-Money Laundering Mechanisms Shape Bank Outcomes. Advances in Decision Sciences, 28(3), 79-105.

9) Arner, D. W., Barberis, J., & Buckey, R. P. (2016). FinTech, RegTech, and the reconceptualization of financial regulation. Nw. J. Int'l L. & Bus., 37, 371.

10) Calafato, A., Colombo, C., & Pace, G. J. (2014). A domain specific property language for fraud detection to support agile specification development.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 06:2025
DOI: 10.5281/zenodo.15621371

11) Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees. Technological forecasting and social change, 158, 120166.

12) Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: an overview. PeerJ Computer Science, 9, e1705.

13) Ellul, J., & Pace, G. (2019). Blockchain and the common good reimagined. arXiv preprint arXiv:1910.14415.

14) Khasawneh, R., Al Qudah, A., & Hailat, M. (2025). The role of government effectiveness in suppressing corruption: Insights from the BRICS emerging economies.

15) Khasawneh, R., Hailat, M., AlQudah, A., & Mohammad, A. H. (2025). The dual impact of tax evasion, does tax evasion incentivize or dampen FDI, perspectives from the emerging economies of BRICS and CIVETS blocs? International Journal of Innovative Research and Scientific Studies, 8(1), 2796-2803.

16) Lui, A., & Lamb, G. W. (2018). Artificial intelligence and augmented intelligence collaboration: regaining trust and confidence in the financial sector. Information & Communications Technology Law, 27(3), 267-283.

17) Muntean, G. (2019). Blockchain potential and disruptors for South Africa towards 2030.

18) Pandey, P., & Litoriya, R. (2021). Promoting trustless computation through blockchain technology. National Academy Science Letters, 44, 225-231.

19) Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2023). Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. Electronic Markets, 33(1), 37.

20) Rashideh, W., Alajmi, M., Alshammari, A., Alqudah, A., Obidallah, W. J., & Alkhathami, M. (2022). Investigating the challenges and value creation of open government data initiatives. IJCSNS, 585.

21) Ryan, P., Crane, M., & Brennan, R. (2020). Design challenges for GDPR RegTech. arXiv preprint arXiv:2005.12138.

22) Villamil, I., Kertész, J., & Wachs, J. (2022). Computational approaches to the study of corruption. arXiv preprint arXiv:2201.11880.

23) Von Solms, J. (2021). Integrating Regulatory Technology (RegTech) into the digital transformation of a bank Treasury. Journal of Banking Regulation, 22(2), 152-168.

24) West, J., Bhattacharya, M., & Islam, R. (2014). Intelligent financial fraud detection practices: an investigation. International Conference on Security and Privacy in Communication Systems,

25) Xu, J. (2024). AI in ESG for financial institutions: an industrial survey. arXiv preprint arXiv:2403.05541.

26) Zouaoui, A., AlQudah, A., Elaoun, C., Arab, M. B., & Eleuch, H. (2018). Impact of corruption in economic development: case of Tunisia. Applied Mathematics & Information Sciences, 12(2), 461-468.