Leveraging Blockchain Technology for Enhancing Financial Monitoring: Main Challenges and Opportunities

Maryna UTKINA
School of Law, University of Warwick, United Kingdom
Academic and Research Institute of Law, Sumy State University, Ukraine
maryna.utkina@warwick.ac.uk

Abstract

This article examines the current state of financial monitoring as a tool for combating and preventing money laundering and corruption. The use of blockchain technology is becoming increasingly prevalent in the field of financial monitoring for legal compliance. It offers a range of benefits, including improved accuracy, transparency, and security in tracking financial transactions. However, its adoption also poses several challenges, such as data privacy concerns, regulatory compliance, and the need for skilled personnel to operate and maintain these systems. This article explores the opportunities and challenges of leveraging blockchain technology to enhance legal compliance and financial monitoring. It also examines its key features and potential applications in financial monitoring. With the increasing adoption of this technology, the financial monitoring landscape is set to transform in the coming years, paving the way for a more efficient and effective way to combat and prevent money laundering and corruption.

Keywords: artificial intelligence; blockchain; IT-technologies; financial monitoring; crime; money laundering; cybercrime;

JEL Classification: K20; K23; O31

DOI: https://doi.org/10.24818/ejis.2023.21

1. Introduction

Reducing financial crime is crucial, and regulatory expectations are high (Crossman-Smith, 2020). Financial monitoring plays a pivotal role and is one of the crucial strategies to combat such crime. One of such crime is money laundering, a significant problem globally, with criminals using various techniques to conceal the origins of their illicit proceeds. Albanese (2021) highlighted that money laundering is recognised as a type of "serious and organised crime", and its primary objective is always to escape detection by law authorities. It tends to involve complex financial instruments and structures that require sophisticated technology to carry out. Financial monitoring is critical in detecting and preventing money laundering by identifying and reporting suspicious transactions to authorities.

This article explores the current state of financial monitoring as a tool for combating and preventing money laundering and corruption, and the opportunities and challenges of leveraging blockchain technology to enhance legal compliance and financial monitoring. It also examines these technologies' key features and potential applications in financial monitoring.

In terms of structure, Section 2 briefly delineates the common core and historical background of money laundering, financial monitoring systems and a general understanding of blockchain

Received: 30 May 2023; Revised: 6 December 2023; Accepted: 15 December 2023

technology. This section outlines existing problems with the financial monitoring system that can make detecting and preventing money laundering and other financial crimes challenging. Section 3 illustrates opportunities for leveraging blockchain technology to enhance financial monitoring in legal compliance – (1) improved transparency and immutability; (2) ability to automate controls and implement (online monitoring); (3) improved audibility; (4) optimisation of the structure and responsibilities of control authorities (entities); (5) efficiency gains; (6) public interactive reporting; (7) reduction of dependence on the "human factor" and, therefore - reduction of corruption.

Section 4 outlines the main challenges in blockchain technology used for financial monitoring – (1) regulatory uncertainty, immature mechanism, and little experience in using blockchain; (2) restrictions on personal data and information disclosure constituting a commercial secret; and sender signatures, which means that transaction flows can be traced. User information can potentially be extracted through data mining, (3) scalability issues; (4) the existence of cyber threats; (5) interoperability problems; (6) development and implementation costs. Section 5 illustrates what measures can be implemented to overcome the challenges of leveraging blockchain technology for enhancing financial monitoring in legal compliance. Section 6 concludes.

2. Main Concepts and Historical Background

Historically, the term money laundering is believed to have first appeared in a legal context in America, originating from the link between organised crime and laundromats (Thommandru & Chakka, 2023). The modern concept of money laundering emerged in the mid-20th century as organised crime syndicates became increasingly sophisticated in concealing the origins of their illicit proceeds. In response, governments and law enforcement agencies began to develop laws and regulations to combat money laundering activities. Money laundering is usually associated with criminal activities that generate large amounts of illegal financial resources (Gaspareniene et al., 2022).

The process of anti-money laundering involves identifying, tracking, and analysing financial transactions to detect and disrupt criminal activity, mainly to prevent money laundering. This typically includes monitoring vital financial metrics such as revenue, expenses, profits, and cash flow and analysing financial statements and budgets. The financial monitoring process is, thus, a critical tool for law enforcement agencies and financial institutions as it enables them to identify and disrupt financial operations. At the European level, the fight against the illegal movement of cash has been enhanced through monitoring and learning from the patterns of past cases. For example, some years ago, the European Council recommended conducting a "post-mortem" analysis of money laundering cases in EU banks. It was due to understand how they came about and to help shape preventive measures (Deloitte, 2023a). The recommendation by the European Council to conduct a "post-mortem" analysis of money laundering cases in EU banks aimed to gain a deeper understanding of the root causes of such cases and to develop effective measures to prevent such incidents from happening in the future. By analysing previous money laundering cases in EU banks, authorities could identify common patterns and vulnerabilities that allowed these illegal activities to occur. The post-mortem analysis involved a thorough investigation of the processes and systems banks use to identify and prevent money laundering, as well as the actions bank employees took when such activities were detected.

This analysis also investigated the role of regulatory authorities in preventing and detecting money laundering in the banking sector.

The findings from such an analysis informed the development of more effective preventive measures, such as improved regulatory frameworks, enhanced due diligence processes, and increased training and awareness for bank employees. Ultimately, this recommendation aimed to create a safer and more secure financial system within the EU, with reduced risk of money laundering and other financial crimes. The EU process described above, focused on developing more effective preventive measures to create a safer and more secure financial system, is related to leveraging blockchain technology to enhance financial monitoring in legal compliance. This is because blockchain technology, known for its decentralised and transparent nature, has the potential to improve financial monitoring and compliance efforts significantly. Using blockchain technology, financial transactions can be recorded tamper-proof and immutable. This can help prevent money laundering and other financial crimes by providing a transparent and auditable trail of transactions. Regulators and law enforcement agencies can have greater visibility into financial activities, enabling them to detect suspicious patterns and identify potential risks more efficiently.

Reznik et al. (2023) explored the prevailing viewpoint among scientific community members regarding the factors commonly associated with money laundering. Through an analysis of diverse scientific opinions, the identified factors encompassed:

- economic factors associated with the shadow economy;
- political factors, specifically corrupt practices, which serve as a method for facilitating money laundering;
- organisational and managerial factors
- legal factors characterised by deficiencies in anti-money laundering legislation.
- socio-moral factors connected to social conflicts, primarily including the erosion of public trust in government authorities and administration (Reznik et al., 2023).

Money laundering is processing these criminal proceeds to disguise their illegal origin. This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source (Financial Act Task Force, FATF). At the same time, Schott (2006) highlighted “money laundering” as a process by which an illegal source of assets obtained or created by criminal activity is concealed to obscure the link between funds and the initial criminal activity. Understanding that was proposed in previous research was that the most appropriate to the following definition of the term “money laundering”. It was suggested to define “money laundering” as the process of transforming illegally obtained income into legal, i.e. legal income. The purpose of such a transformation is to conceal the original source of “criminal proceeds” and eliminate their traces. It was emphasised that the term “money laundering” also applied to such financial transactions that form a particular asset because of “criminal acts” (in particular, corruption) (Reznik et al., 2023).

Anti-Money Laundering (AML) activities aim to prevent various crimes such as drug-related crimes, terrorist crimes, smuggling crimes, corruption and bribery crimes, and crimes against financial management. However, how money laundering is organised is diverse, and the process is complex. The increasing internationalisation of financial flows also makes it difficult to trace the whereabouts of funds. Money laundering poses a significant threat to the safety of the international financial system once it occurs (Chang et al., 2020). The illegal incomes that flow through a country’s financial system significantly affect its economic security and can cause not only loss of financial stability of banks, insurers, etc., but also lead to an increase in crime and terrorist attacks in the state (Kuzmenko et al., 2020).

Several existing problems with the financial monitoring system can make it challenging to detect and prevent money laundering and other financial crimes effectively. Some of these problems include:

- *Complexity*. It is generally outlined in the popular press that complexity is linked to a lack of understandability (Freedman, 2014). So, the financial system is highly complex, with multiple layers and entities involved in transactions. This complexity can make it difficult to trace the source and movement of funds, which can be exploited by criminals to hide illegal activities;
- *Lack of transparency in financial transactions*. This is especially true in jurisdictions with weak regulatory frameworks or lax enforcement. Wanjau et al. (2018) noted that financial transparency entails fully disclosing financial information to reduce information asymmetry between companies. The lack of transparency increases the risks of financial crises, whereas improved transparency contributes to economic development;
- *Inadequate regulatory frameworks*. Generally, the framework should provide a clear and trusted long-term foundation for effective regulation (Financial Services Future Regulatory Framework Review, 2019). Some countries may have weaker or inconsistent regulations, making it easier for criminals to exploit loopholes;
- *Insufficient resources*. Thus, financial monitoring agencies may lack sufficient resources, both in terms of personnel and technology, to effectively monitor and analyse large volumes of financial data. Thus, Yehuda Shaffer (cited by Vedrenne, 2021) outlined that "the number of employees is a key indicator" for the financial intelligence units' activity. As an example, the Financial Action Task Force (FATF) found that the Financial intelligence unit of the UK suffers from a lack of available resources (both human and IT) and analytical capability, which is a serious concern (Vedrenne, 2021);
- *Lack of international coordination* between regulatory agencies and law enforcement authorities, making it challenging to track and prevent financial crimes across borders. The International Monetary Fund has become aware that problems in cooperation and information exchange continue to constrain cross-border supervision (IMF, 2007). Thus, as was mentioned at National Money Laundering Risk Assessment (US Department of the Treasury, 2022), cross-body collaboration is crucial because uneven and often inadequate regulation and supervision, coupled with a lack of compliance enforcement for digital asset trading platforms and other service providers, allow criminals to expose international financial system to risk from jurisdictions where regulatory standards and enforcement are less robust;
- *Emerging technologies*. New technologies, such as cryptocurrencies, can make it more challenging to trace financial transactions, potentially allowing criminals to hide their activities more effectively. Criminals adapt their strategies according to emerging economic trends to turn a profit and avoid detection by law enforcement (Drescher, 2018). According to Gensier (2021), law enforcement agencies fear the industry will serve to enable criminal activity, and financial regulators are concerned about the crypto economy, which poses growing financial systemic risk as crypto assets, and derivative products become embedded and disbursed through mainstream finance.

The list above outlines existing problems of the financial monitoring system, which should lead to its restructuring to secure increasing efficiency and transparency and to the revision of the conditions and procedures for its implementation.

I explore that the modern IT sphere's developments[1] must be implemented to avoid falsifications, losses, corruption risks and money laundering as best as possible. Humanity is on the threshold of the Industry 4.0 revolution, where advanced technologies such as artificial intelligence, robotics, data analytics, or the Internet of Things can create breakthrough applications (Siderska et al., 2023). Anti-money laundering (AML) laws and other data protection laws that keep getting stricter have forced many financial institutions to implement long, expensive processes to stay compliant. To bridge the gap in the existing financial monitoring system that can make it challenging to detect and prevent money laundering and other financial crimes effectively, emerging technology can help mitigate money laundering and other financial crimes. Thommandru & Chakka (2023) highlight blockchain as one of the world's best-known examples of Distributed Ledger Technology (it represents an innovative and rapidly advancing method of recording and exchanging data across multiple data stores or ledgers. This technology enables the recording, sharing, and synchronising of transactions and data among various participants on a distributed network (Krause et al., 2017), which can become the key to future success in the financial sector. They also noted that blockchain technology could be used in many ways and change processes. So, blockchain can be understood as a distributed ledger in which a copy of the ledger is kept on each connected computer (Javaid et al., 2022). Chang et al. (2020) outlined that blockchain originally meant blocks of cryptocurrencies linked by chains. I am sure that implementing blockchain technology can become the technological factor that will transform the financial monitoring system into a new dimension of automatic monitoring, end-to-end search, and the accumulation of information.

Blockchain and distributed ledger technologies are now being used in various ways, with some publications proposing a blockchain-based identity and authentication architecture (World Bank, 2018). Nevertheless, the core ideas behind it emerged in the late 1980s and early 1990s (Yaga et al., 2018).

As to the definition of the given notion of "blockchain", there is no unified one, leading to many conflicting definitions. "Blockchain" is an append-only ledger, a sequential database maintained by a decentralised network of users responsible for agreeing upon additions to the chain and secured through cryptography (COSO, 2023). Also, it is understandable as a distributed ledger technology that refers to a system where transactions recorded within a specific database are shared, synchronised, and approved across a network. A blockchain is a shared ledger of transactions between parties in a network, not controlled by a single central authority (OECD, 2018). Consensus using cryptographic algorithms verifies the authenticity and accuracy of transactions (Deloitte, 2023b). As Ozili (2019) mentioned, nowadays, the most common use of blockchain is for trading in cryptocurrency, that is, buying and selling cryptocurrency such as bitcoins. Blockchain technology offers "a secure, transparent, fast, and affordable digital solution to many government problems" (Rooney et al., 2017).

The decentralised form of the blockchain reduces the volume of control procedures in confirming the authenticity of the information because system participants have equal rights and conditions of access to information. Success requires close interaction with other emerging technologies, regulators, officials, and stakeholders.

[1] E.g. Artificial Intelligence, Internet of Things, Blockchain, Cloud Computing, Quantum Computing and others

Blockchain, combined with other IT technologies, has significant transformative potential despite its shortcomings (Smith, 2020; Hashem et al., 2023).[2] [3] First, external threats are caused by the lack of a legal basis for decentralised register technology. However, the ability to meet global transparency trends, improve the image and ensure public support and trust in regulatory authorities requires searching for the most appropriate configuration of blockchain implementation in the state's financial monitoring system. Thus, the success factors and results of financial monitoring, transparency and openness can be significantly increased thanks to the introduction of blockchain.

As for money laundering, several technologies have been developed in combination with various methods to detect counterfeit currency, money laundering and credit card evasion. According to the money laundering process, bankers, lawyers, accountants, and other professionals participate in a three-step process, which often takes advantage of the laws of the "spouse" countries. Law enforcement agencies' investigation of virtual assets, such as cryptocurrencies, is complex due to differences in regulatory requirements between states regarding the cross-border search for digital information (Thommandru & Chakka, 2023).

Lewis et al. (2017) noted that blockchain technology is increasingly being applied to meet Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements in financial applications. This is because the information is open and pseudonymous to all public blockchain systems, while private systems have limitations on who can participate. However, it is essential to note that every technology can be used for good or evil, and the ethical use of blockchain technology ultimately depends on the intentions and actions of its users.

The global financial system provides services to billions of people daily while managing trillions of cash (Javaid et al., 2022). The finance sector has been grappling with several challenges for a considerable period in its pursuit of achieving these ambitious goals (Tian et al., 2020). These issues include the expenditure of numerous stakeholders, delays, extra paperwork, and data breaches, resulting in enormous losses the business endures yearly. The problems facing the global financial system may be resolved by blockchain technology (QingQiu et al., 2021).

The use of blockchain technology has made significant progress in the fight against Anti-Money Laundering by enabling the effective identification of suspicious transactions. This is achieved by tracking customer transactions and activities in real time, providing financial institutions with a more accurate and up-to-date understanding of their customer's financial behaviour. As Javaid et al. (2022) highlighted, blockchain is one of the best technologies for any sector that benefits from the speedy movement of verifiable, fraud-free information and transactions due to its peer-to-peer network and anti-tampering features With this enhanced visibility, financial institutions can more quickly and accurately identify suspicious transactions and take appropriate action to prevent money laundering (Lai, 2018).

[2] E.g. double-spending; 51% attack; large amount of energy and because of it – blockchain can be costly; high developments costs.
[3] E.g. unauthorised access and threats to confidentiality

3. Opportunities of Leveraging Blockchain Technology for Enhancing Financial Monitoring in Legal Compliance

Friedman & Ormiston (2022) highlighted that blockchain's four main attributes can be viewed as security, transparency, efficiency and decentralisation. One area where blockchain technology can significantly impact is in enhancing financial monitoring and legal compliance. Legal compliance refers to ensuring financial institutions comply with regulatory frameworks, such as anti-money laundering (AML) and know-your-customer (KYC) regulations. Blockchain technology can improve financial monitoring and legal compliance by providing a secure and transparent record of financial transactions that authorised parties can access. By using blockchain technology, financial institutions can improve their ability to detect and prevent financial crimes, reduce the risk of fraud, and ensure regulatory compliance.

Current trends in digital development, big-data implementation, blockchain technologies, the introduction of innovative technologies require improvement of existing methods to assess the money laundering risk of financial institutions and to develop fundamentally new approaches (Lyeonov et al., 2020).

According to those mentioned above, I propose to outline the following opportunities for using blockchain technology to enhance financial monitoring:

(1) *Improved transparency and immutability*. Without blockchain, each organisation has to keep a separate database (IBM, n.d.). By its definition, blockchain is unable to forget since tampering with transactional data stored in it has been identified as nearly impossible (Finck, 2018). Blockchain technology provides a transparent and immutable record of transactions. This transparency and immutability make it difficult for bad actors (Cambridge Dictionary)[4] to manipulate transactions, making it easier for financial institutions to comply with legal regulations. Members can view the entire transaction history when all transactions are immutably recorded and are time- and date-stamped. It virtually eliminates any opportunity for fraud (IBM, n.d.).

Blockchains, by definition, are unable to be forgotten since tampering with transactional data stored in blockchains has been identified as nearly impossible.

As to the immutability, once data is recorded on the blockchain, it becomes nearly impossible to alter or manipulate. According to those mentioned earlier, it ensures the integrity of data, ensuring it remains unchanged and tamper-proof (Artasanchez, 2023).

(2) *Ability to automate controls and implement online monitoring*. Blockchain technology enables the development of smart contracts, self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Smart contracts can automate the execution of business processes and reduce the need for manual intervention, increasing efficiency and reducing the risk of human error.

By leveraging smart contracts and blockchain technology, financial institutions can automate controls and implement online monitoring, reducing the need for manual monitoring and intervention. This can lead to significant cost savings and improve the accuracy and timeliness of financial monitoring. Automation substitutes technology for manual labour while enabling real-time or near real-time reporting via dashboards (Deloitte, 2022). Although automation can dramatically reduce costs, not every control should be automated. For example, a smart

[4] A person or organisation responsible for actions that are harmful, illegal, or morally wrong.

contract could be developed to automatically monitor transactions for suspicious activity and alert financial institutions of potential money laundering or fraud. The smart contract could also automatically freeze assets or block transactions in the event of suspicious activity, reducing the risk of financial crimes and increasing the speed and efficiency of response. Furthermore, blockchain technology enables real-time monitoring of transactions, allowing financial institutions to detect and respond to suspicious activity in real-time. This can significantly reduce the risk of financial crimes and improve the accuracy and timeliness of financial monitoring.

(3) *Improved auditability*. In general, auditability is the ability of an auditor to achieve accurate results in the examination of a company's reporting (Liberto, 2021). The transparent and immutable nature of blockchain technology makes it easier to audit transactions. Auditing is an essential aspect of legal compliance, and blockchain technology can help financial institutions improve their audit capabilities. This is because one of the three layers of blockchain is the storing of permanent, auditable and unchangeable digital records which provides data security (Friedman & Ormiston, 2022).

(4) *Optimisation of the structure and responsibilities of control authorities (entities)*. With blockchain technology, the distribution of transaction records across a decentralised network makes it easier for regulators and auditors to monitor financial transactions and identify potential financial crimes. Thus, blockchain technology enables real-time data sharing while reducing points of weakness (Pratt, 2021). The use of blockchain technology can enable the creation of a more effective and efficient regulatory framework by improving the transparency and traceability of financial transactions.

By implementing blockchain technology, regulators and auditors can access a single, secure, and tamper-proof source of information that can be used to monitor financial transactions and detect potential money laundering or fraud. Blockchain technology can automate regulatory processes, reducing the need for manual intervention, and thus increasing efficiency. This can lead to a more streamlined regulatory framework, which helps reduce compliance costs for financial institutions while maintaining the integrity of the financial system. Additionally, blockchain technology can create decentralised regulatory bodies that can operate independently without a centralised authority. This can reduce the risk of corruption and improve the effectiveness of regulatory bodies.

(5) *Efficiency gains*. Blockchain technology can automate compliance processes, reducing the need for manual intervention. Automation in regulation and compliance can lead to significant efficiency gains, reducing the time and cost associated (Open Access Government, 2018). Blockchain technology also vastly improves the speed and quality of the regulatory review process since there would no longer be a need for reconciliation (Akmeemana, 2017).

(6) *Public interactive reporting*. With blockchain technology, financial institutions can provide real-time, transparent, and secure access to financial information, including transactions and balances, to regulators, auditors, and the public. Blockchain technology enables the creation of a decentralised, transparent, and immutable ledger that anyone with the necessary permissions can access. This can lead to greater transparency in financial reporting and help to build trust between financial institutions and their stakeholders.

By leveraging blockchain technology, financial institutions can provide interactive reporting capabilities that allow stakeholders to drill down into financial data and perform data analytics in real-time. This can enable stakeholders to identify potential financial crimes, such as money laundering or fraud, more quickly and promptly.

Furthermore, blockchain technology can enable financial institutions to provide secure and tamper-proof reporting, reducing the risk of data breaches and cyberattacks. This can lead to greater confidence in the accuracy and integrity of financial reporting. In addition, interactive public reporting can help increase the effectiveness of financial monitoring by providing greater detail and transparency than traditional reporting methods. This can lead to improved regulatory compliance and greater accountability for financial institutions.

(7) *Reduction of dependence on the "human factor" and, therefore - reduction of corruption*. Traditional financial systems rely highly on human judgement and decision-making, which can increase the risk of corruption and fraud. However, with blockchain technology, financial transactions are recorded and verified automatically by the network, eliminating the need for human intervention. This can help reduce the risk of errors and fraud and increase the efficiency and speed of financial transactions.

Furthermore, blockchain technology can enable the creation of smart contracts, self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Smart contracts can help reduce the need for intermediaries, such as lawyers and notaries, reducing the risk of corruption and fraud.

Moreover, blockchain technology can provide a more transparent and auditable system for financial transactions, reducing the opportunities for corrupt practices. The decentralised nature of the blockchain means that transactions are recorded on multiple nodes and are available for public verification, making it difficult for anyone to manipulate the system without being detected.

Most compelling is blockchain's potential for transformative analytic capabilities. One of the beneficial outcomes of blockchain is easy access to structured data, which can then be used to generate advanced analytics and accelerate machine learning. This will enable tools to get smarter and drive us further and faster toward more continuous auditing and assurance (Deloitte, 2023b).

Integrating IT development with the legal and organisational principles, basic principles and procedures for financial monitoring, and its entities' powers allows to decentralise of the financial monitoring system. It increases its transparency, safety, and efficiency. The symbiosis of cryptography and computerisation, the use of mathematical calculation algorithms, and the exclusion of humans and the human factor in decision-making by the system provide considerable advantages to blockchain technology.

4. Main Challenges of Leveraging Blockchain Technology for Enhancing Financial Monitoring in Legal Compliance

Blockchain technology has the potential to transform the financial industry by enhancing transparency, security, and efficiency. The decentralised, immutable ledger that underpins blockchain technology can provide a tamper-proof record of financial transactions, making it ideal for use cases such as supply chain management, trade finance, and digital identity verification. Blockchain technology can improve financial monitoring and legal compliance by providing a secure and transparent record of financial transactions that can be accessed by authorised parties. By using blockchain technology, financial institutions can improve their ability to detect and prevent financial crimes, reduce the risk of fraud, and ensure regulatory compliance. At the same time, blockchain technology has not yet attained the highest level of

interoperability in the financial sector owing to energy consumption, privacy ethics, user trust, laws and regulations, compliance rules/protocols, supervision, and network integration (Weerawarna et al., 2023).

While blockchain technology has the potential to enhance financial monitoring and legal compliance, several *challenges* need to be addressed.

(1) Regulatory uncertainty, immature mechanism, and little experience in using blockchain. It is relatively new, and regulatory bodies are still grappling with how to regulate it. And at the same time, the lack of adequate regulation creates a risky environment (Singh, 2020). Regulatory uncertainty is "*an individual's perceived inability to predict the future state of the regulatory environment*" (Hoffmann et al., 2009).

Countries have different approaches to regulating blockchain, with some countries banning cryptocurrencies altogether. Yeoh (2017) stated that the lack of rules and regulations for compliance and the absence of strategic governance enforcement are the reasons for losing trust in blockchain technology. This regulatory uncertainty makes it difficult for financial institutions to leverage blockchain technology to enhance financial monitoring in legal compliance.

(2) Restrictions on personal data and information disclosure constituting a commercial secret. Blockchain technology relies on the transparency and immutability of its ledger, which means that all transactions are recorded and shared across the network. To prevent double-spending and establish ownership, transparency is necessary.

However, users also require privacy (Drescher, 2018). Though, financial institutions and other businesses have legal and ethical obligations to protect the privacy and confidentiality of their customer's personal data. Feng et al. (2019) outlined that blockchain transactions typically include participants' addresses, transaction values, timestamps, and sender signatures, which means that transaction flows can be traced. User information can potentially be extracted through data mining.

In many jurisdictions, some strict laws and regulations govern personal data collection, use, and disclosure, such as the General Data Protection Regulation (2018) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) (2004) in the United States. These laws require businesses to obtain the consent of individuals before collecting and using their data, and to implement appropriate security measures to protect against unauthorised access, use, and disclosure of personal data.

Similarly, businesses may have information that constitutes a commercial secret, such as trade secrets, business processes, and confidential financial information. These types of information are critical to businesses' success and competitive advantage and must be protected against unauthorised disclosure. Therefore, the challenge in leveraging blockchain technology for enhancing financial monitoring is to find ways to balance the transparency and immutability of the blockchain ledger with the need to protect the privacy and confidentiality of personal data and commercial secrets. One possible solution is to use cryptographic techniques to encrypt personal data and commercial secrets before storing them on the blockchain, ensuring that only authorised parties with the decryption keys can access the information.

(3) Scalability issues. Blockchain technology, particularly public blockchains, faces scalability issues. The blockchain becomes voluminous with the increasing number of transactions (Zheng et al., 2018). Blockchain scalability is the ability for participants in a blockchain network to process and store a large number of transactions. The speed of transaction throughput is often

measured in transactions per second (TPS) and the size of a blockchain is measured in bytes of storage required (Golden, n.d.).

Public blockchains, such as Bitcoin, have limited transaction throughput. This makes it difficult for financial institutions to scale their blockchain solutions to meet transaction volume requirements. Despite all its success and strength, scalability is the major challenge that hinders the full adoption of blockchain in some areas (Singh et al., 2020).

(4) The existence of cyber threats. Blockchain technology is designed to be secure and tamper-proof but is not immune to cyber threats. Cybercriminals can exploit vulnerabilities in the blockchain network and smart contracts to steal funds, launch denial-of-service attacks, or corrupt the blockchain ledger. One of the most significant cyber threats to blockchain technology is the 51% attack (Aponte-Novoa et al., 2021), where an attacker gains control of more than half of the computing power in a blockchain network, allowing them to modify transaction records and potentially steal funds. Other cyber threats include phishing attacks (Banu & Banu, 2013[5]; Zafar, 2020) malware attacks, and social engineering attacks that exploit the human element of blockchain transactions.

(5) Interoperability problems. Different blockchains are built using various technologies and protocols, making it difficult for them to communicate with each other. This interoperability problem limits financial institutions' ability to leverage blockchain technology fully.

Therefore, the challenge in leveraging blockchain technology for enhancing financial monitoring is to develop robust security measures to protect against cyber threats. These security measures include implementing multi-factor authentication, regularly auditing the blockchain network for vulnerabilities, and developing contingency plans for responding to cyber-attacks. Another potential solution is to use blockchain technology to enhance existing cybersecurity measures, such as by providing a decentralised, tamper-proof record of cybersecurity events and threat intelligence sharing between financial institutions.

(6) Development and implementation costs. Blockchain technology requires significant resources, including specialised skills, hardware, and software. Moreover, the costs associated with developing and implementing blockchain technology are often higher than those of traditional IT solutions. Therefore, the challenge in leveraging blockchain technology for enhancing financial monitoring is finding ways to manage development and implementation costs effectively. Financial institutions may consider using third-party blockchain solutions, such as blockchain-as-a-service (BaaS) providers, to reduce the cost and complexity of developing and implementing blockchain technology.

Feldman (2019) summarised different categories of indicators, which are the biggest barriers to adopting blockchain technology globally. They are 27% regulatory uncertainty, 25% lack of trust among users, 21% ability to bring networks together, 11% separate blockchain not working together, 6% inability to scale, 6% concerns of intellectual property, and 4% concerns of audit and compliance.

Addressing these challenges will require a collaborative effort between regulators, financial institutions, and technology providers. It will be essential to develop clear regulatory frameworks, ensure data privacy and security, improve scalability and interoperability, and promote adoption and standardisation across the industry.

[5] The hacker’s goal in a very phishing attack is to steal the user’s credentials. they'll send legitimate-looking emails to the owner of the wallet key

5. How to Overcome Main Challenges and Implement Blockchain Technology Effectively

Implementing blockchain technology effectively can be a complex task due to various challenges. However, with careful planning and consideration of these challenges, chances of success can be increased. Here are some critical steps that I outline as ways to overcome the main challenges and implement blockchain technology effectively:

(1) *Understand the technology*. All financial monitoring entities must begin by thoroughly understanding the fundamentals of blockchain technology: how it works, its benefits, and its limitations. This knowledge will help make informed decisions during the implementation process. Often, the most significant threats and "weakest links", when it comes to online security and data protection in the workplace, come from human error (Marcroft, 2019). All entities engaged to the process of financial monitoring have to invest in training and education programs to enhance team's understanding of blockchain technology (e.g., organising workshops, seminars, or online courses to familiarise with the concepts, terminology, and potential use cases of blockchain). Provide training and partner with blockchain experts to demystify the technology and ensure a smooth implementation process (Palma, 2023). All entities engaged in the financial monitoring process must invest in training and education programs to enhance the team's understanding of blockchain technology (e.g., organising workshops, seminars, or online courses to familiarise themselves with blockchain concepts, terminology, and potential use cases). Provide training and partner with blockchain experts to demystify the technology and ensure a smooth implementation. Entities should be familiarised with the relevant laws and regulations governing data privacy, protection, and commercial secrets in a jurisdiction and identify the specific requirements and restrictions related to disclosing personal data and commercial secrets.

(2) *Define clear objectives*. All objectives of using blockchain technology have to be clearly defined. This will help to stay focused and measure success accurately. I absolutely agree with the position of Marcroft (2019), that it shouldn't only be the IT team's responsibility to ensure all systems and applications across the entity are functioning securely. Board-level executives should be attending any discussion around implementing proactive prevention of cyber security vulnerabilities and treating them as a top business priority. It also helps ensure that resources are allocated efficiently. As if the entity clearly defines the goals and requirements of the blockchain technology, this will help prioritise features and functionalities.

(3) *Address scalability and performance*. As I noted, blockchain networks can face challenges related to scalability and performance, especially in public blockchains. In such cases, different blockchain platforms and consensus mechanisms must be analysed to determine which suits the needs best. Private or consortium blockchains may be more suitable for specific use cases that require faster transaction processing.

(4) *Research and stay updated*. Stay informed about the regulatory landscape surrounding blockchain technology in the jurisdiction. Monitor any proposed or existing regulations that may impact your implementation. Engage with industry associations, legal experts, and regulatory bodies for clarity and guidance. For example, an industrial engineer in DHL Supply Chain, Viraj Lele, highlighted that entities should stay informed about evolving regulations and engage with regulatory authorities to contribute to developing favourable frameworks. At

the same time, collaborating with industry peers and joining consortia or industry associations can help establish common standards and best practices (Lele, 2023).

(5) *Consult legal experts*. Entities should work closely with legal experts specialising in blockchain and understanding the regulatory nuances. They can help to navigate the legal requirements and ensure compliance with applicable laws.

(6) *Choose the right blockchain platform*. This decision is essential for overcoming scalability issues by selecting a blockchain platform that offers scalability solutions or is specifically designed to handle large-scale transactions.

(7) *Shard or partition the blockchain*. Consider implementing sharding or partitioning techniques to divide the blockchain network into smaller subsets or shards. Sharding is a partitioning technique used to distribute the computational and storage effort across a peer-to-peer (P2P) network so that each node isn't tasked with handling the transactional load for the whole network. Instead, each node only keeps data about its division or shard (Fuentes, 2022). In such cases, this allows parallel processing of transactions and improves scalability. Each shard can process its transactions independently, increasing the network's throughput.

(8) *Continuous optimisation and upgrades*. Ongoing optimisation is an iterative process where we implement a set of simple, high-impact cost-reduction methods across all applications and then measure and report the cost savings results (Burns, 2018). Entities should monitor the performance of blockchain networks and regularly implement optimisations and upgrades. So, to overcome the challenge, entities should stay updated with the latest advancements in blockchain technology and implement new features or improvements that enhance scalability.

(9) *Implement robust security measures*. One possible solution to overcome the challenge of cyber threats is to implement robust security measures. For example, entities can employ robust encryption techniques to protect sensitive data at rest and in transit. Encryption helps ensure that data remains secure even if it is intercepted. Generally, encryption is a formula to turn data into a secret code. Each algorithm uses a string of bits known as a "key" to perform the calculations (Latronix, n.d.). Also, I found right position according to the strong security measures from the Greetly (2021). In the given article using the proper equipment was named as one of such tools. Investing in stronger firewalls and other equipment or software that encrypts the company's data is vitally important in securing its assets. The major ways through which fraudsters can gain access to the company assets' either by telecommunication applications, should be sealed to ensure that no one gets the information (Greetly, 2021). So, entities should keep all software, including the blockchain platform and associated applications, up to date with the latest security patches to address known vulnerabilities. To prevent cyber threats, the entities should deploy firewalls and intrusion detection systems to monitor network traffic and detect potential hazards or unauthorized access attempts. It also means that it is essential to implement secure basic management practices[6] (Saha, 2022) to protect cryptographic keys used in blockchain transactions and use hardware wallets or trusted robust management solutions to securely store and manage private keys.

(10) *Perform regular security audits and assessments to identify vulnerabilities and weaknesses* in blockchain infrastructure. Penetration testing, code reviews, and vulnerability scans can help uncover potential security gaps. Security audit helps to protect the activity of the entity from cyber-attacks, data breaches, and other security threats; it ensures that blockchain technology is operating efficiently (Twintech Solutions, n.d.).

[6] E.g., follow key generation best practices, use key expiration, use key revocation, centralise user rolesd and access, use key-encrypting keys and others.

(11) *Establish incident response plans*. The entity should develop and document a comprehensive incident response plan that outlines the steps to be taken in the event of a cyber-attack or security breach. This plan should include communication protocols, roles and responsibilities, and procedures for containing and mitigating the impact of an incident. At the same time, testing and updating the incident response plan regularly is strongly recommended to ensure its effectiveness.

(12) *Continuously monitor and respond to threats*. It is also necessary to deploy real-time monitoring tools and technologies to promptly detect and respond to potential cyber threats. The entities should use intrusion detection and prevention systems, security information, and event management (SIEM) solutions to monitor network activity and identify anomalous behaviour.

6. Conclusion

In conclusion, leveraging blockchain technology for enhancing financial monitoring and legal compliance offers several opportunities for the financial industry, including enhanced transparency, improved security, streamlined processes, reduced costs, and improved data quality. However, several challenges need to be addressed to fully leverage blockchain technology for these purposes. These challenges include regulatory frameworks, data privacy, scalability, interoperability, and adoption.

Addressing these challenges will require a collaborative effort between regulators, financial institutions, and technology providers to ensure that blockchain technology is deployed in a safe and effective manner. By overcoming these challenges and leveraging the opportunities provided by blockchain technology, financial institutions can improve their ability to detect and prevent financial crimes, ensure regulatory compliance, and improve customer trust and confidence. Overall, the benefits of leveraging blockchain technology for financial monitoring and legal compliance are significant, and the financial industry should continue to explore the potential of this technology.

Acknowledgement: The author would like to thank Professor Ana Aliverti and Professor James Harrison for their beneficial comments on the draft of this article. The research was undertaken according to the British Academy's Researchers at Risk Fellowships Programme. The author declares no conflict of interest.

References:

Akmeemana, C. (2017). Using Blockchain to Solve Regulatory and Compliance Requirements. https://medium.com/@akme_c/using-blockchain-to-solve-regulatory-and-compliance-requirements-16290f4b4ac1 Accessed 07 Jul 2023.

Albanese, J.S. (2021). Organized crime as financial crime: the nature of the organized crime as reflected in prosecutions and research. *Victims Offenders*, 16 (3), 431-443. https://www.tandfonline.com/doi/full/10.1080/15564886.2020.1823543 Accessed 15 Mar 2023

Aponte-Novoa, F., Orozco, A, Villanueva-Polanco, R. & Wightman, P. (2021). The 51% Attack on Blockchains: A Mining Behavior Study. *IEEE Access*. 9, 140549-140564. https://ieeexplore.ieee.org/document/9567686. Accessed 14 Mar 2023.

Artasanchez, A. (2023). The Role of Blockchain in Data Products : Ensuring Transparency and Trust. http://thedatascience.ninja/2023/06/11/the-role-of-blockchain-in-data-products-ensuring-transparency-and-trust/ Accessed 06 Jul 2023.

Banu, D.M., & Banu, S.M. (2013). *A Comprehensive Study of Phishing Attacks*. *International Journal of Computer Science and Information Technologies*, 4(6), 783-786.

Burns, J. (2018). Continuous Optimization. *AWS Cloud Enterprise Strategy Blog.* https://aws.amazon.com/blogs/enterprise-strategy/continuous-optimization/ Accessed 10 Jul 2023.

Cambridge Dictionary (n.d.). https://dictionary.cambridge.org/dictionary/english/bad-actor Accessed 25 Apr 2023.

Can blockchain turn the tide on financial crime compliance? *Deloitte*. https://www2.deloitte.com/mt/en/pages/financial-services/articles/mt-risk-article-can-blockchain-turn-the-tide-on-financial-crime-compliance.html Accessed 19 May 2023.

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. https://doi.org/10.1016/j.techfore.2020.120166 Accessed 13 Mar 2023.

COSO (2023). Blockchain and Internal Control. *The COSO Perspective*. https://www.coso.org/Shared%20Documents/Blockchain-and-Internal-Control-The-COSO-Perspective-Guidance.pdf Accessed 10 Mar 2023.

Crossman-Smith, J. (2020). Blockchain and AI: the Future of Anti-Money Laundering. Grant Thornton. https://www.grantthornton.co.uk/insights/blockchain-and-ai-the-future-of-anti-money-laundering/ Accessed 26 Feb 2023.

Deloitte (2022). Realizing the Future of Controls - Three steps for financial services organizations to take right now. https://www.deloitte.com/global/en/services/risk-advisory/blogs/realizing-the-future-of-controls-three-steps-for-financial-services-organizations-to-take-right-now.html Accessed 07 Jul 2023.

Deloitte (2023a). Can blockchain turn the tide on financial crime compliance?. https://www2.deloitte.com/mt/en/pages/financial-services/articles/mt-risk-article-can-blockchain-turn-the-tide-on-financial-crime-compliance.html

Deloitte (2023b). Blockchain for Financial Leaders: Opportunity vs. Reality. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-fei-blockchain-report-future-hr.pdf Accessed 04 Mar 2023.

Drescher, D. (2018). *Blockchain basics: a non-technical introduction in 25 steps*. Apress. https://doi.org/10.1007/978-1-4842-2604-9 Accessed 26 Mar 2023.

Feldman, S. (2019). What's blocking blockchain?. Retrieved from https://www.statista.com/chart/17948/worlwide-barriers-to-blockchain-adoption/. Accessed 07 May 2023.

Feng, Q., He, D., Zeadally, Sh., Khan, M.Kh., Kumar, N. (2019). A Survey on Privacy Protection in Blockchain System. *Journal of Network and Computer Applications*, 126, 45-58. https://doi.org/10.1016/j.jnca.2018.10.020. Accessed 26 Feb 2023.

Financial Act Task Force (FATF). Retrieved from http://www.fatf-gafi.org/faq/moneylaundering/ (2020, November, 18). Accessed 15 Apr 2023.

Financial Services Future Regulatory Framework Review. Call for Evidence: Regulatory Coordination. *HM Treasury*. (July 2019). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819025/Future_Regulatory_Framework_Review_Call_for_Evidence.pdf Accessed 05 July 2023.

Finck, M. (2018). Blockchain and Data Protection in the European Union. *European Data Protection Law Review*. 4, 17.

Freedman, R. S. (2014). Understanding the Complexity of Financial Systems of Systems. NYU Tandon Research Paper, (2512307). https://ssrn.com/abstract=2512307 Accessed 04 Jul 2023.

Friedman, N., Orminston, J. (2022). Blockchain as a Sustainability-Oriented Innovation?: Opportunities for and Resistance to Blockchain Technology as a Driver of Sustainability in Global Food Supply Chains. *Technological Forecasting and Social Change.* 175, 121403. https://doi.org/10.1016/j.techfore.2021.121403 Accessed 07 Jul 2023.

Fuentes, R. (2022). What is Sharding and How is it Helping Blockchain Protocols? https://www.rootstrap.com/blog/what-is-sharding-and-how-is-it-helping-blockchain-protocols#:~:text=Sharding%20is%20simply%20a%20partitioning,about%20its%20division%20or%20shard. Accessed 10 Jul 2023.

Gan, Q.Q., Lau, R. Y. K., & Hong, J. (2021). A critical review of blockchain applications to banking and finance: a qualitative thematic analysis approach. *Technology Analysis & Strategic Management*, 1-17. https://doi.org/10.1080/09537325.2021.1979509 Accessed 17 Mar 2023.

Gaspareniene, L., Gagyte, G., Remeikiene, R. & Matuliene, S. (2022). Clustering of the European Union Member States on Money Laundering Measuring Indices. *Economics and Sociology*, 15 (2), 153-171. https://doi.org/10.14254/2071-789X.2022/15-2/10 Accessed 28 Dec 2023.

General Data Protection Regulation (GDPR). 2018. Final text neatly arranged. https://gdpr-info.eu/ Accessed 9 Mar 2023.

Gensier, G. (2021). Remarks before the Aspen Security Forum, *US Securities and Exchange Commission*. https://www.sec.gov/news/speech/gensler-aspen-security-forum-2021-08-03 Accessed 05 Jul 2023.

Golden (n.d.). Blockchain scalability. https://golden.com/wiki/Blockchain_scalability-VWRG9JG Accessed 05 Jul 2023.

Greetly (2021). Keeping Your Company Assets Secure Through Robust Security Measures. https://www.greetly.com/blog/keeping-your-company-assets-secure-through-robust-security-measures Accessed 10 Jul 2023.

Hashem, R.E.E.D.R., Mubarak, A.R.I., & Abu-Musa, A.A.E.S. (2023). The impact of blockchain technology on audit process quality: an empirical study on the banking sector. International Journal of Auditing and Accounting Studies, 5(1), 87-118. https://doi.org/10.47509/IJAAS.2023.v05i01.04 Accessed 07 Jul 2023.

Hoffmann, V. H., Trautmann, T., & Hamprecht, J. (2009). Regulatory uncertainty: A reason to postpone investments? Not necessarily. *Journal of Management Studies*, 46 (7), 1227–1253. https://doi.org/10.1111/j.1467-6486.2009.00866.x Accessed 07 Jul 2023.

IBM (n.d.). Benefits of Blockchain. https://www.ibm.com/topics/benefits-of-blockchain Accessed 06 Jul 2023.

IMF (2007). Working together: improving regulatory cooperation and information exchange - [Washington, D.C.] : International Monetary Fund, Monetary and Financial, https://www.imf.org/external/pubs/ft/books/2007/working/0607.pdf

Javaid, M., Haleem, A., Singh, R.P., Suman, R., Khan, Sh. (2022). A Review of Blockchain Technology Applications for Financial Services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations (TBench)*, 2(3), 100073. https://doi.org/10.1016/j.tbench.2022.100073 Accessed 11 Mar 2023.

Krause, S.K., Natarajan, H., Gradstein, H.L. (2017). Distributed Ledger Technology (DLT) and blockchain: Fintech note no. 1. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/134831513333483951/distributed- Accessed 19 May 2023.

Kuzmenko, O., Suker, P., Lyeonov, S., Judrupa, I., Boiko, A. (2020). Data Mining and Bifurcation Analysis of the Risk of Money Laundering with the Involvement of Financial Institutions. *Journal of Interdisciplinary Studies*, 13(3), 332-339. https://doi.org/10.14254/2071-8330.2020/13-3/22 Accessed 28 Dec 2023.

Lai, K. (2018). Blockchain as AML tool: a work in progress. *International Financial Law Review*.

Latronix (n.d.). Encryption and Its Importance to Device Networking. https://www.lantronix.com/wp-content/uploads/pdf/Encryption-and-Device-Networking_WP.pdf Accessed July 2023.

Lele, V. (2023). Stay Informed and Collaborate for Regulatory Compliance. How Can Businesses Overcome the Implementation Challenges of Blockchain Technology? https://blocktelegraph.io/businesses-blockchain-tech-implementation/ Accessed 09 Jul 2023.

Lewis, R., McPartland, J., & Ranjan, R. (2017). Blockchain and financial market innovation. *Economic Perspectives*, 41(7), 1-17. https://www.google.com/url?sa=i&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=0CAIQw7AJahcKEwjg5sCmnPr_AhUAAAAAHQAAAAAQAg&url=https%3A%2F%2Fwww.chicagofed.org%2F~%2Fmedia%2Fpublications%2Feconomic-perspectives%2F2017%2Fep2017-7-pdf.pdf&psig=AOvVaw0YVt134xS062-oxQ1b6oih&ust=1688737338001341&opi=89978449 Accessed 6 Jul 2023.

Liberto, D. (2021). Auditability. *Investopedia*. https://www.investopedia.com/terms/a/auditability.asp Accessed 07 Jul 2023.

Lyeonov, S., Zurakowska-Sawa, J., Kuzmenko, O. & Koibichuk, V. (2020). Gravitational and intellectual data analysis to assess the money laundering risk of financial institutions. *Journal of International Studies*, 13 (4), 259-272. https://doi.org/10.14254/2071-8330.2020/13-4/18 Accessed 28 Dec 2023.

Marcroft, G. (2019). Six Steps to a Robust Cyber Security Strategy. https://www.continuitycentral.com/index.php/news/technology/4517-six-steps-to-a-robust-cyber-security-strategy Accessed 10 Jul 2023.

National Money Laundering Risk Assessment (2022). *U.S. Department of Treasury.* https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf Accessed 05 Jul 2023.

OECD (2018). Blockchain Primer. https://web-archive.oecd.org/2018-10-25/492841-OECD-Blockchain-Primer.pdf Accessed 06 Jul 2023.

Open Access Government (2018). Blockchain technologies for automatic regulation and compliance. https://www.openaccessgovernment.org/blockchain-technologies-automatic-regulation-compliance/41885/ Accessed 07 Jul 2023.

Ozili, P.K. (2019). Blockchain Finance: Questions Regulators Ask, Choi, J.J. and Ozkan, B. (Ed.) Disruptive Innovation in Business and Finance in the Digital World (International Finance Review, Vol. 20), *Emerald Publishing Limited, Bingley*, pp. 123-129. https://doi.org/10.1108/S1569-376720190000020014 Accessed 20 Mar 2023.

Palma, M.G. (2023). Demystify Complex Integration Through Education. *How Can Businesses Overcome the Implementation Challenges of Blockchain Technology*? https://blocktelegraph.io/businesses-blockchain-tech-implementation/ Accessed 9 Jul 2023.

Pratt, M.K. (2021). Top 10 benefits of blockchain technology for business. *TechTarget.* https://www.techtarget.com/searchcio/feature/Top-10-benefits-of-blockchain-technology-for-business Accessed 07 Jul 2023.

Reznik, O., Utkina, M., & Bondarenko, O. (2023). Financial intelligence (monitoring) as an effective way in the field of combating money laundering. *Journal of Money Laundering Control,* 26(1), 94-105. https://doi.org/10.1108/JMLC-09-2021-0102

Rooney, H., Aiken, B., & Rooney, M. (2017). Q. Is the Internal Audit Ready for Blockchain? *Technology Innovation Management Review*, 7(10), 41-44.

Saha, P. (2022). 10 Enterprise Encryption Key Management Best Practices. *Key Management*. https://www.encryptionconsulting.com/10-enterprise-encryption-key-management-best-practices Accessed 10 Jul 2023.

Schott, P.A. (2006). Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism. *The World Bank*. 292 p.

Siderska, J., Alsqour, M. & Alsaqoor, S. (2023). Employees' Attitudes Towards Implementation Robotic Process Automation Technology at Service Companies. *Human Technology*, 19 (1), 23-40. https://doi.org/10.14254/1795-6889.2023.19-1.3 Accessed 28 Dec 2023.

Singh, A., Click, K., Parizi, R., Zhang, Q., Dehghantanha A., Choo K.-K.R. (2020). Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications*, 149, 102471. https://doi.org/10.1016/j.jnca.2019.102471 Accessed 07 Jul 2023.

Singh, M. (2020). Blockchain Technology for Corporate Reporting: An Investor Perspective. *CFA Institute*. p. 16. https://www.cfainstitute.org/-/media/documents/article/position-paper/cfa-blockchain-wp_text.pdf Accessed 07 Jul 2023.

Smith, B. (2020). The Opportunities and Challenges of Blockchain Adoption in Supply Chain Management. Walker College of Business in partial fulfilment of the requirements for the degree of Bachelor of Science in Business Administration. https://core.ac.uk/download/pdf/345094329.pdf Accessed 6 Jul 2023.

Thommandru, A., Chakka B. (2023). Recalibrating the Banking Sector with Blockchain Technology for Effective Anti-Money Laundering Compliances by Banks. *Sustainable Futures.* 5, 100-107. Accessed 19 Mar 2023

Tian, Y., Lu, Z., Adriaens, P., Minchin, R. E., Caithness, A., & Woo, J. (2020). Finance infrastructure through blockchain-based tokenization. *Frontiers of Engineering Management*, 7, 485-499. https://doi.org/10.1007/s42524-020-0140-2 Accessed 14 Mar 2023.

Twintech Solutions (n.d.). Blockchain Security Audit. Smart Contract Audit. https://www.twintechsolution.com/blockchain-security-audit-smart-contract-audit-sample-report/ Accessed 8 Jul 2023.

United States. The Health Insurance Portability and Accountability Act (Hipaa). *Washington D.C: U.S. Dept. of Labor Employee Benefits Security Administration*; 2004. http://purl.fdlp.gov/GPO/gpo10291. Accessed 28 Mar 2023.

US Department of the Treasury (2022). National Money Laundering Risk Assessment. https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf

Vedrenne, G. (2021). European FIUs Often Understaffed, *Unequipped Against Financial Crime*. https://www.moneylaundering.com/news/european-fius-often-understaffed-unequipped-against-financial-crime/ Accessed 05 Jul 2023.

Wanjau, B. M., Muturi, W.M., Ngumi P. (2018). Effect of Financial Transparency on Financial Performance Companies Listed in Easted Africa Securities Exchanges. *Research Journal of Finance and Accounting*, 9(4), 7-10. https://core.ac.uk/download/pdf/234632243.pdf Accessed 05 Jul 2023.

Weerawarna, R., Miah, S. J., & Shao, X. (2023). Emerging advances of blockchain technology in finance: a content analysis. *Personal and Ubiquitous Computing*, 1-14. https://doi.org/10.1007/s00779-023-01712-5 Accessed 07 Jul 2023.

World Bank (2018). Blockchain & Distributed Ledger Technology (DLT). https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt Accessed 06 Jul 2023.

Yaga, D., Mell, P., Roby, N. & Scarfone, K. (2018). Blockchain Technology Overview. *NISTIR 8202.* https://doi.org/10.6028/NIST.IR.8202 Accessed 27 Mar 2023.

Yeoh, P. (2017). Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance* 25(2), 196-208. https://doi.org/10.1108/JFRC-08-2016-0068 Accessed 03 Jul 2023.

Zafar, D. (2022). 8 Blockchain Security Issues You Are Likely To Encounter. https://cybersecurity.att.com/blogs/security-essentials/8-blockchain-security-issues-you-are-likely-to-encounter Accessed 07 Jul 2023.

Zheng, Z., Xie, Sh., Dai, H.-N., Chen, X. & Wang, H. (2018). Blockchain Challenges and Opportunities: A Survey. *International Journal of Web and Grid Services*, 14(4), 352-357. https://doi.org/10.1504/IJWGS.2018.095647 Accessed 24 Mar 2023.