Areas of Technology That Helps in Combating Money Laundering: A Concept Paper

Yusri Hazrol Yusoff[1], Nur Ain Fatihah Azlan[2], Nurfarahin Nisa Mohd Zamzuri[3], Nurfarhin Sufian[4], Sarah Nadya Rudy Kurniawan[5], Razinah Hassan[6]

[1,3,4,5,6]Faculty of Accountancy, Universiti Teknologi MARA, Cawangan Selangor, Kampus Puncak Alam Selangor, Malaysia, [2]Jabatan Akauntan Negara Malaysia Negeri Selangor, Menara Naza TTDI, Aras 6, 12 & 13, No. 11, Jalan Judo 13/45, Seksyen 13, 40100 Shah Alam, Selangor.
Email: 2021189967@student.uitm.edu.my, 2019406298@student.uitm.edu.my, 2021119239@student.uitm.edu.my, 2021156103@student.uitm.edu.my

Abstract
Advances in information technology have the potential to make anti-money laundering more efficient and successful. It is a serious crime that can have a significant impact on the global economy, as it allows criminals to profit from their illicit activities and evade detection by law enforcement agencies. Technologies can help identify suspicious activity and detect patterns that may indicate money laundering. This can help financial institutions and other regulated businesses combat money laundering. The purpose of this study is to identify the areas of technology that help in combating money laundering. The study demonstrates how block chain, machine learning, and big data can help in monitoring, processing, and analyzing suspicious transactions and other illegal activity. This study also will be help policy maker to defined the money launder activities through block chain, machine learning and big data.
Keywords: Anti-money Laundering, Technology, Blockchain, Machine Learning, Big Data

Introduction
Over the past few years, money laundering has not been taboo in this century. Criminals nowadays have many ideas and ways of hiding illegal transactions by doing money laudering. Money laundering can be defined by law enforcement agencies in the United States as the activities of criminals using the self-service laundries as a way to give a legal appearance to the large amount of dirty money that the company wants.

According to section 3 of AMLATFA 2001: money laundering is the act of a person who:
a. Engages, directly or indirectly, in a transaction that involves proceeds of any unlawful activity

b. Acquires, receives, possesses, disguises, transfers, converts, exchanges, carries, disposes, uses, removes from or brings into Malaysia proceeds of any unlawful activity; or

c. Conceals, disguises or impedes the establishment of the true nature, origin, location, movement, disposition, title of, rights with respect to, or ownership of, proceedsof any unlawful activity.

The majority of unlawful transactions are completed in cash since there is the least danger of leaving one's mark. Nonetheless, there is a clear tendency to exploit the internet in order to conduct illegal transactions in the form of online-banking, cyber money, and electronic transactions. Therefore, suppressing money laundering through a variety of highly advanced technology is essential to combating terrorist financing, organized crime and corruption. Regardless, the money launderer itself has a lot of techniques on how to wash the money nowadays as the technique gets smarter than before.

Information technology plays an important role in combating money laundering and has attracted a lot of attention and concern from many researchers. The advancement of information technology has the potential to make anti-money laundering faster and more effective. Increased usage of digital anti-money laundering solutions based on Artificial Intelligence (AI) and its many subsets such as machine learning, blockchain and big data may assist in better detection of risks and react to, interact with, and monitor suspicious activities. The public sector can get the benefit of technology to prevent money laundering through improved live (real-time) monitoring and information exchange with counterparts that offer more informed oversight of regulated companies, which can improve supervision (Mayano, 2019). The advancement of technology in the private sector may enhance risk assessments, onboarding procedures, interactions with responsible authorities, auditability, accountability, and general good governance and saving money.

Background of Study

A systematic study of social, political, or other fact conditions with the purpose of identifying unknown or partially known factors that are at work behind a particular phenomenon is a process known as social research. In addition to this, it is able to understand why something occurs and to draw inferences and general conclusions.

This report focused on the ways in which upgraded technology may assist in combating money laundering cases all around the world. Therefore, the implementation of technology such as AI and machine learning in ordinary business is crucial because money laundering happens everywhere in any country. In particular AML/CFT regulations may be implemented more effectively if technology is used widely which can facilitate a better understanding, assessment and mitigation of risks, customer due diligence and monitoring, and communication with supervisors.

This study focuses on the area of developed technology that can combat money laundering. We believe that the technology can help the government catch criminals that use many alternatives to create money laundering. The study showed the area of technology in focusing on block chain, machine learning, and big data that helps in recognizing the money laundering process.

Problem Statement

The technologies to combat money laundering aim to enhance the speed, quality, efficiency, and cost of some anti-money laundering (AML) measures, as well as the costs of

implementing the AML framework. This is different compared to the use of traditional techniques and procedures. The most relevant technologies are cross-cutting and allowing new digital methods of data collection, processing, and analysis. These technologies also enable the communication of data and information in a variety of specific solutions.

There are many legal and regulatory frameworks that have been enacted in response to the threat posed by money laundering in an effort to reduce the severity of its effects. According Bank Negara Malaysia (2022), Government of Malaysia recognises the importance of a coordinated national effort and a conscientious approach to combat money laundering. Therefore, Malaysia was set up the foundation of the Malaysian legal framework regulating money laundering came from policies and proposals initiated by the Financial Action Task Force (FATF). FATF is responsible to organize all financial and transaction data in Malaysia and this data must report to Bank Negara Malaysia to combat money-laundry activities in Malaysia.

When applied to large amounts of data, technological solutions based on artificial intelligence (AI) and machine learning (ML) have the potential to improve continuous monitoring as well as the reporting of suspicious transactions. This technology can automatically monitor, process, and analyze suspicious transactions and other illegal activity. The technology itself can differentiate illegal conduct from regular activity in real-time, minimizing the need for initial, front-line human review in the process. Tools or solutions based on AI may also create evaluations of continuing customer due diligence and customer risk that are more accurate and comprehensive. AI also can be updated to account for new and emerging threats in real-time. However, AI solutions vary greatly in both technology and use and may present significant risks.

In other part, the public and private sectors may both increase the efficiency of their risk with the help of new technology and innovative approaches which provide the company to make use of the advancement of technology in detecting money laundering. The development, implementation, and regulatory supervision of new technologies need to take into account both the potential and the risks. In addition, it must ensure that the use of technologies is compliant with international standards of data protection, privacy protection, and cybersecurity.

Chittum (2022) which stated that 'a global drug cartel used Binance to launder millions, the DEA says. As result, world's largest crypto exchange is reportedly working with investigators to track them down'. According to an ongoing US Drug Enforcement Action (DEA) investigation, a worldwide drug cartel utilized Binance to route millions of the gang's unlawful revenues. According to Brewster (2022), expectation transaction between $15 million to $40 million has been laundered through the world's biggest cryptocurrency exchange. Binance is a cryptocurrency exchange which is the largest exchange in the world in terms of daily trading volume of cryptocurrencies. The examples of cryptocurrency that are included in Binance are Bitcoin (BTC), Ether (ETH), Litecoin (LTC), Dogecoin (DOGE), and its own token Binance Coin (BNB).

Binance, which announced intentions earlier this year to acquire a minority investment in Forbes, Binance gave cooperation with police to assist in tracking down the suspects. According to Brewster (2022), the investigation into the cartel's usage of Binance started in 2020 where DEA informants on another crypto trading platform discovered a user providing bitcoin in return for fiat cash. The DEA found one suspect, Carlos Fong Echavarria, who eventually pled guilty to money laundering and narcotics selling charges. Binance supported the agency by tracking Echavarria's blockchain trading activities, which totaled $4.7 million.

Allowing to the warrant, they were able to uncover an additional account receiving cash from Echavarria through tracking on-chain activities.

Another account user, who has not been officially charged, reportedly purchased approximately $42 million in cryptocurrency which at least $16 million of which came from drug money. "This is an example of how the transparency of blockchain transactions works against criminal actors," said Matthew Price, Binance's senior director of investigations. He also stated that 'the bad guys are leaving a permanent record of what they are doing' Binance also assisted the DEA early 2022 in its endeavor to seize over 100 accounts linked to money laundering in Mexico. According to Reuters, Binance is apparently under investigation by the US Department of Justice. According to the report, the company's finances were like a "black box," and not even Binance's former chief financial officer had full access to accounts throughout his almost three-year employment. Binance's chief strategy officer told Reuters that the report's research and portrayals of its business groups were "categorically wrong."

Referring Federal Court Report (2022), in the case of PP v. Dato' Sri Mohd Najib Hj Abd Razak in which he became the first former Prime Minister to be convicted of abuse of power, breach of trust, and money laundering. He was found guilty of all seven charges related to the 1Malaysia Development Berhad (1MDB) scandal. The first charge relates to abuse of power under section 23 of the Malaysian Anti-Corruption Commission Act, 2009. The next three charges are on criminal breach of trust under section 409 of the Penal Code while the last three charges are under section 4(1)(b) of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 ('AMLATFAPUAA 2001'). The prosecution alleged that the accused had committed money laundering by receiving a total of RM42 million, which was the proceeds of unlawful activity, into his personal bank accounts. In his defense, the accused claimed that he had not abused his position, that he had no knowledge of the RM42 million transferred into his personal accounts, and that he was under the assumption that the said funds in the account were given as donations to him by King Abdullah of the Kingdom of Saudi Arabia.

The evidence showed that he transferred billions of dollars to his personal account which can be detected from the transaction banks that used the technology itself. The transaction from a bank account is the part that shows the advancement of technology helps in detecting money laundering. Thus, the technology can improve continuous monitoring as well as the reporting of suspicious transactions.

Gap in Research

In this study, we will focus on a few technologies that are helping in combating money laundering which are machine learning, blockchain and big data. The goal for this study is to view how these technologies are being implemented and impact on money laundering. However, there are more technologies that can be used to help the anti- money laundering compliance which we did not include in this research.

Literature Review
Blockchain

Blockchain is a decentralized digital ledger that is designed to record or store information of transactions across many computers in a data structure called blocks. In blockchain everyone can access the database. Blockchain has the characteristic of immutability which is the ability of the ledger to remain unchanged. This is because blockchain is using cryptographic hashes. Each block contains a unique code, called a hash which is generated using the data in the block

as well as the hash of the previous block in the chain. Thus it linked together the block and generated a blockchain. Any attempt to modify the data in the block will be immediately detected and rejected because the hash of the modified block will not match the hash of thenext block.

Although bitcoin is the most famous application, blockchain can be applied into diverse applications far beyond cryptocurrencies. Since it allows payments to be finished without any bank or any intermediary, blockchain can be used in various financial services such as digital assets, remittance and online payment (Peters et al., 2015). Because of blockchain technology's ability to present the "truth" of atransaction to all parties with access, there have been many proposals about how to best adopt blockchain to other uses. Reported by O'Niell (2016), Julio Faura, head of R&D in the Innovation Division of Santander Bank was defined block chain's distributed ledger is very elegant way to solve financial problems in the financial services industry.

Usage of blockchain in improving KYC process

According to Mayano et. al (2019), member firms must use reasonable diligence when opening accounts to know the essential facts concerning the customer and the authority of each person acting on behalf of the customer. Thus, Know Your Customer(KYC) has become a mandatory practice that requires financial institutions to verify acustomer's identity when opening their account. KYC is the backbone in the fight against financial crime and money laundering and helps businesses know who theyare dealing with. KYC is used to ensure that their customers are legitimate and have the right to make a transaction. KYC process is initiated when a customer andfinancial institution's relationships are created based on certain terms of the agreement. Then, the customer will provide the documents like an ID card so the financial institution can make verification on the authenticity of the document given. After analysis of the documents, the institution will generate certification where the customer is either validated or rejected to open their account. This process will be repeated every time a customer intends to make a relationship with a new financial institution which is actually time consuming. Not only that, the current KYC process also has other drawbacks such as high risk of error and duplication.

Blockchain technology has emerged as a solution to make the KYC process become more efficient. As blockchain is a data storage that can be shared, customers will only have to undergo the KYC process once. Then, this KYC information will be stored in blockchain and can be distributed with other financial institutions. Applying blockchain to KYC decreases the onboarding time, improves customer experience andminimizes cost overhead and associated risks.

Any illegal activities like money laundering can be identified easily with the help of blockchain. Usually when the criminals perform money laundering, they will try to make the money obtained come from legitimate sources in order to avoid detection from legal authorities. These criminals will split the large amount of money into smaller chunks then deposit it into many different accounts. Therefore, an efficient process of KYC blockchain based can make it difficult for these criminals to convert money obtained from illegal activities.

Machine Learning

The FATF (2021), has long advocated for the use of technology to monitor and detect money laundering and terrorism financing activity. Financial transactions other than direct cash payments leave electronic traces, which can be processed and analyzed to get insight into the

financial behaviors of persons involved in illegal activities, or even to establish criminal affiliation (De Goede, 2012). As a result, it is not surprising that technical solutions such as big data analytics, natural language processing, and distributed ledger technology have been promoted as critical components of money laundering detection. Machine learning advocates stress the machine learning technology's ability to manage enormous amounts of data, both organized and unstructured, as well as its potential to uncover patterns of financial behavior used by people involved in illegal conduct.

However, the industry is still wary, and the use of these technologies is yet experimental rather than systematic (Canhoto, 2021). In terms of AML programs, artificial intelligence and machine learning are viewed as expensive technology solutions whose benefits have not yet been proven. Additionally, there are risks for organizations using artificial intelligence and machine learning for anti-money laundering as well as for the people whose financial behaviors are being examined due to a lack of experience in understanding and using these technologies.

The machine learning algorithm, which processes the data inputs, is a key component of artificial intelligence solutions. Machine learning differs from classical programming as the former's goal of the computational process is to seek out patterns in the data set which are the rules that connect inputs to outputs (OECD, 2021). On the other hand, the objective of the computational process in classical programming is to apply the rules to the input data in order to produce an output. The rules are developed a priori.

Machine learning comes in a variety of types, each of which is appropriate for a particular situation. Supervised machine learning should be used when there are known inputs and known outputs (Kute et. al., 2021). The analyst provides the computer training datasets, with data labeled as either input or output. For example, this method use data where the label (whether it is money laundering or not) is known, in an effort to identify the patterns that distinguish between money laundering and lawful activities. The algorithm's function is to study the patterns that link the inputs to the outputs and to create rules that can be used to solve similar problems in the future.

Unsupervised machine learning, on the other hand, is recommended for data sets where it is not known which data points refer to inputs and which ones refer to outputs (Mayano, 2019). For instance, it attempts to find patterns in data without knowing which data correspond to money laundering, and which do not. The analyst provides the unlabeled training data sets to the computer. The algorithm's job is to figure out the best method to group the data points and create rules for how they might be related.

Financial institutions are using Anti-Money Laundering (AML) profiling to recognize the distinctive patterns of behavior used by clients to hide the illegal source or the illegal purpose for their money. The preferred method for developing algorithms for AML detection is to use factual information that law enforcement authorities have provided regarding actual cases of criminal activity. For example, when prosecutors succeed in getting a conviction, details about the traits and financial behavior of the convicted person's are made public. Hence financial institutions such as banks have access to historical information on established connections between a particular crime and a transaction pattern. Banks value this information because it offers verified inputs (the person's traits and behaviors) and verified outputs (what crimes the person was convicted of) (OECD, 2021). Therefore, it may be analyzed using supervised learning. For instance, banks looked into the transaction patterns of a particular type of business account after receiving verified reports that several terrorist financers had lived in a certain region and engaged in that particular business activity.

The second preferred method to develop a money laundering detection algorithm is to use Court Production Orders (CPOs) (Kute et al, 2021). CPOs are tools the court uses to obtain particular information about someone being investigated for suspected criminal activity. The court gets in touch with the financial institution where the suspect has accounts and requests their history of transactions. After receiving the CPO, the bank looks into the pattern of financial activity for the accounts flagged.

The third strategy employed by banks is finding variances in the financial behavior of specific customer groups, which is appropriate for unsupervised learning (Kute. et. al, 2019). For instance, banks employed this strategy to examine the financial activity of business accounts related to a specific type of trade suspected of indulging in tax evasion. The analysis showed two clusters of accounts with differing behavioral tendencies in terms of cash deposits. One cluster with a big number of accounts where traders typically placed round amounts such as $1230. In contrast, the other cluster with a small number of accounts where traders preferred to deposit exact amounts, for example, $1237.50. These clusters were then subjected to further investigation by experts in order to identify clients who may be seeking to avoid paying taxes on purpose.

The last approach is identifying accounts with suspicious patterns of financial transactions by combining pattern analysis of data sets with criterion matching. It is the approach used for everyday financial transaction analysis, and it is ideal for using reinforced learning approaches. Every day, banks use this algorithm to analyze the transactions that occurred during a particular time, giving more weight to those that match known money laundering methods, such as depositing large quantities of cash. Banks also focus on transactions that violate rules concerning the usual use of a given product and the expected behavior of a particular group of customers. The output is a collection of transactions that appear to follow an unusual pattern and that are flagged for further investigation by analysts.

Big Data

Big Data tools are used for anti-money laundering. For example, SAS Anti-Money Laundering System (SAS AML). This system can easily monitor bank operations, consolidate information, and detect suspicious activities. In addressing issues relating to financial security Big Data technologies can be used to quickly receive and handle enormous data sets (Jullum et al, 2019). Big Data not only saves time but is also good in terms of collecting, sorting data, filling different databases, processing and analyzing the data. Some priority of Big Data includes notifying of unusual behavior when working with this data and performing a preliminary evaluation of a suspicious action's nature and potential harm. Additionally, it also analyzes current events to predict the probable execution of a specific criminal activity.

Big Data tools also can determine the level of potential vulnerabilities that can be leveraged to accomplish criminal schemes. Next, creating remedial actions and evaluating their efficacy and last but not least, as general evaluation of organizational practices for maintaining the privacy of financial and personal data and others.

Jullum et. al (2019) suggest the following tasks can be accomplished with the aid of big data technologies, according to the author.

- Video surveillance system data analysis in conjunction with access control systems
- Transactions data analysis in financial institution systems to identify fraud
- Hardware and software event logs analysis to find links and forecast potentially risky behavior of individuals or programmes

• Automated detection of incidents among all the events that have occurred and so on

The Proposed Conceptual Framework For Areas of Technology That Helps in Combating Money Laundering
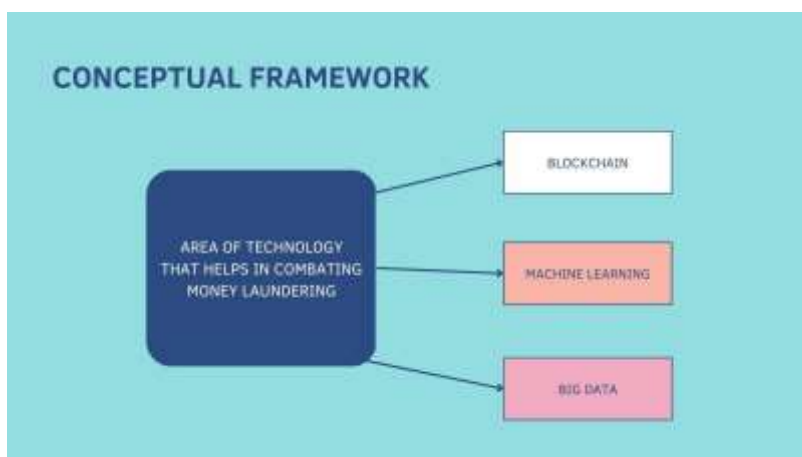

Figure 1: The Proposed Conceptual Framework for Areas of Technology That Helps in Combating Money Laundering

A conceptual framework is needed to place the study. A conceptual framework integrates research into crucial knowledge bases, laying the foundation for the significance of the issue statement and research questions. The above conceptual framework is developed while doing the study in order to properly comprehend how technology helps in preventing money laundering. This conceptual framework emphasizes how technology could help in combating money laundering. Blockchain, machine learning, and big data contribute to detecting money laundering.

Recommendation
This present study shows that every company and department needs an anti-money laundering security system for early detection of money laundering so we can reduce money laundering crimes in the future. However, there are also weaknesses where there are chances that the system may be hacked by professionals. This may cause the risk of money laundering crimes to occur during that time. Other than that, the company needs to spend a lot of money to provide, install and hire professionals to train employees so that they can use and control the system in well. Moreover, the company needs to choose a more advanced system to get satisfactory results because the common system may not be strong enough to protect the company's data.

However, this study believes that there are ways to prevent this weakness. Where the company may have backup data to make sure that even if the system got hacked, they still have information about every transaction inside the company. Other than that, the company may choose the best security based on the risk of money laundering. If the company is a small company and does not do many transactions, the company may choose a system that is cheaper and easier to use.

Audit Committee in company also must serious to combat this illegal activity. They must develop a good policy to make sure this activity can be detected in beginning stage. It will he help to protect company financial to involves with illegally transaction. In other part, they also can protect investor money from involving and related with money laundry business.

Conclusion

Technologies are used in preventing money laundering by improving the speed, quality, efficiency, and cost of various anti-money laundering (AML) procedures. AML requirements may be more efficiently executed if technology is widely used to allow a better understanding, evaluation, and mitigating risks, customer due diligence and monitoring, and communication with supervisors. There are three areas that helps in combating money laundering.

This study found blockchain, machine learning, and big data among the area of technologies that help in anti-money laundering. Firstly, blockchain technology has emerged as a tool for improving the efficiency of the Know Your Customers (KYC) process. The use of blockchain in KYC reduces onboarding time, enhances the client experience, and reduces cost overhead and associated risks. Next, machine learning advocates emphasize the technology's ability to manage massive volumes of data, both structured and unstructured, as well as its potential to detect patterns of financial activity employed by criminals. Lastly, big data can also be used in helping to quickly receive and handle enormous data and analyzes current events to predict the probable execution of a specific criminal activity.

This research also proposed a framework to help future researcher to understand the relationship between technologies and blockchain, machine learning and big data in part of combat money–laundering activities. Many study focus on financial transaction or money trail to detecting money laundering, but this study suggest in other option to make enforcement agency can have planned and develop a good policy to control this activity.

References

Bank Negara Malaysia. (2022), National Coordination Committee to Counter Money Laundering (NCC), BNM Annual Report 2022). https://amlcft.bnm.gov.my/domestic-coordination

Brewster, T. (2022), Global Drug Conspiracy Used Binance to Launder Millions in Crypto, DEA Investigation Finds, Forbes, https://www.forbes.com/sites/thomasbrewster/2022/12/19/mexican-drug-gang-money-laundering-over-binance-crypto-exchange/?sh=167f96554a59

Canhoto, A. I. (2021). Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. *Journal of Business Research*, *131*, 441–452.

Chittum, M. (2022). A global drug cartel used Binance to launder millions, the DEA says. Here's how the world's largest crypto exchange is reportedly working with investigators to track them down. Markets Insider, https://markets.businessinsider.com/news/currencies/global-drug-cartel-binance-launder-millions-crypto-exchange-dea-investigation-2022-12

De Goede, M. (2012). Speculative Security. The Politics of Pursuing Terrorist Monies. Minneapolis, MN: University of Minnesota Press. https://www.upress.umn.edu/book-division/books/speculative-security

Demetis, D. S. (2018). Fighting money laundering with technology: A case study of Bank X in the UK. Decision Support Systems, 105, 96–107.

FATF. (2021). Opportunities and Challenges of New Technologies For Aml/Cft. https://www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf

Federal Court, Putrajaya. (2022), Dato' Sri Mohd Najib Abd Razak V. Pp & Other Appeals (No 2), eLaw Journal Express, https://www.elaw.my/JE/01/JE_2022_37.html.

https://www.fatf-gafi.org/en/publications/Methodsandtrends/Professional-money-laundering.html

Jullum, M., Loland, A., Huseby, R. B., Anonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. Journal of Money Laundering Control, 23(1), 173–186.

Kumar, V. (2012). Money Laundering: Concept, Significance and its Impact. https://core.ac.uk/download/pdf/234624157.pdf

Kute, D., Pradhan, B., Shukla, N., and Alamri, M. (2021), Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering–A Critical Review, IEEE Access PP(99):1-1.

Mayano, P. M., Ross, O., and Thoroddsen, T. (2019), Optimized and Dynamic KYC System Based on Blockchain Technology, International Journal of Blockchains and Cryptocurrencies 1(1):1

Naheem, M. A. (2019), "Exploring the links between AML, digital currencies and blockchain technology", Journal of Money Laundering Control, Vol. 22 No. 3, pp. 515-526.

O'Neill, K. M. (2016), Santander executive outlines the case for blockchain disruption, MIT Sloan School of Management, https://mitsloan.mit.edu/ideas-made-to-matter/santander-executive-outlines-ca

OECD. (2021), Artificial Intelligence, Machine Learning and Big Data in Finance: Opportunities, Challenges, and Implications for Policy Makers, https://www.oecd.org/finance/artificial-intelligence-machine-learningbig-data-in-finance.htm.

Peters, G. W., Panayi, E., & Chapelle, A. (2015). Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2646618