Electronic Evidence of Anti-Money Laundering Regimes: A Comparative Study Between United Kingdom, United States and Indonesia

Submitted: 5 May 2023
Reviewed: 24 June 2023
Revised: 1 July 2023
Accepted: 8 July 2023

Article submitted to peer blind review

John Richard Latuihamallo[*]
https://orcid.org/0009-0009-0133-2393
Pujiyono[**]
https://orcid.org/0000-0001-8244-8092
Irma Cahyaningtyas[***]
https://orcid.org/0000-0003-2911-1268

DOI: https://doi.org/10.26512/lstr.v16i1.48449

Abstract

[Purpose] To explore how comparing proof with countries with substantial cryptographic transaction volumes and preparedness to perpetrate crypto money laundering crimes, such as the US and UK, can revolutionise eradicating money laundering crimes in Indonesia.
[Methodology/approach/design] This study compares laws and regulations in Indonesia, the US, and the UK and examines how electronic evidence and expert witnesses can be crucial to crypto money laundering proof under each country's criminal procedural law. The study also examines how cryptocurrencies, blockchain systems, and emerging technologies impact law enforcement and legislators' approach to the AML regime.
[Findings] The research reveals that, unlike in the US and UK, electronic evidence is not regulated in formal criminal procedure law in Indonesia. The US and UK have defined criteria for gathering and removing electronic evidence to ensure authenticity, validity, and integrity so that it may be generally accepted in court. The study recommends standardised protocols for the collection and analysis of electronic evidence, international protocols to coordinate anti-money laundering efforts across jurisdictions, mechanisms to ensure transparency and accountability in the collection and use of electronic evidence, and investments in technology and training to ensure law enforcement agencies have the tools and knowledge to use electronic evidence effectively.

[*]Doctor in Law Candidate form Doctoral of Law Program, Universitas Diponegoro, Jalan Imam Bardjo, S.H., No. 1, Semarang City, Central Java 50241, Indonesia. Email: johnrichardundip2021@gmail.com.
[**]Full Professor in Criminal Law from Faculty of Law, Universitas Diponegoro, Jalan dr. Antonius Suroyo, Tembalang, Semarang City, Central Java 50275, Indonesia. Email: pujiyonofhundip@yahoo.com.
[***]Full Doctor in Law and Senior Lecturer from the Faculty of Law, Universitas Diponegoro, Jalan dr. Antonius Suroyo, Tembalang, Semarang City, Central Java 50275, Indonesia. Email: irmacahyaningtyas@yahoo.com.

[Practical implications] The study's recommendations have practical implications for the Indonesian government, law enforcement agencies, and legislators. Adopting international protocols, standardised protocols for electronic evidence, and investing in technology and training can improve the anti-money laundering regime and aid Indonesia's fight against money laundering crimes.
[Originality/value] This study contributes to understanding how electronic evidence and expert witnesses can be crucial to crypto money laundering proof under each country's criminal procedural law. The study's recommendations provide a roadmap for improving the anti-money laundering regime in Indonesia. They can be used as a reference for countries facing similar challenges in combating money laundering crimes.

Keywords: Electronic Evidence. Anti-Money Laundering. Cryptocurrencies. Comparative Law.

INTRODUCTION

The emergence of cryptocurrencies can have both beneficial and bad outcomes, such as using cryptocurrencies as investment commodities or transaction tools, respectively (OTHMAN et al., 2020). The characteristics of cryptocurrencies, which promote anonymous and decentralised transactions, present several options that can be used to fund various illegal activities (WANG & ZHU, 2021). Additionally, the use of encryption technology makes it more difficult for law authorities to investigate and prosecute crimes committed with cryptocurrencies as a means of payment. In addition to facilitating money laundering, these characteristics make it more difficult to enforce laws, particularly in the verification process. This is especially true in nations where cryptocurrencies are not regulated in the constitution, particularly concerning their status as legal tender, as is the case in Indonesia (PUTRA & PUTRANTO, 2022).

Although many nations do not regulate the legitimacy of cryptocurrencies as a form of legal cash, several nations have made it legally permissible to acquire and sell crypto assets in the same way that people can legally buy and sell stocks. The United States, the United Kingdom, Canada, Singapore, and South Korea are some of the countries that have legalised cryptocurrencies as transaction commodities on the stock market (ANTHONY DAS et al., 2018). In this instance, Japan and Australia provide legality to cryptocurrencies in the same way they do to fiat money, despite the fact that cryptocurrencies are still restricted by the obligation to report their ownership to the authorities in both countries. In this context, Japan provides a definition that is distinct from the definitions provided by other countries, which generally classify cryptocurrencies as virtual currencies. Instead, Japan defines cryptocurrencies as crypto assets through the Payment

Service Act and amendments to the Financial Instruments and Exchange Act (FIEA), particularly in opposition to Bitcoin (FUJIWARA, 2023). The bitcoin market is subject to income tax in Australia, which has a system quite similar to what we have here (TAN & LOW, 2017).

The supervision of various actions that use cryptocurrency is impacted in various ways by these two categories of legislation (CHAWKI, 2022). For instance, when the cryptocurrency is regarded as a tax object, its owner must report all transactions. In particular, when cryptocurrency is regarded as a tax object, the state is granted the authority to carry out more stringent oversight than when cryptocurrency is regarded as a stock commodity. This has implications for the possibility of using cryptocurrencies as a medium for criminal acts, such as what occurred in the United States with a money laundering (Bitcoin) value of $4.5 billion with the suspect Ilya Lichtenstein and his wife Heather Morgan (READ, 2022) or the Asabri money laundering case with allegations against three suspects who were hiding the results of their crime with the media in the form of cryptocurrency (TRISAKTI & SOPONYONO, 2021). Both of these cases involve suspects who hid the results of their crimes from the media in the form of cryptocurrency (Bitcoin). Even though the marketplace where buying and selling must first obtain permission from the government, in practice, the practices of these two nations do not regulate cryptocurrencies as a legal medium of exchange and legalise their transactions in a definite buying and selling (crypto) market (as a commodity), these two nations do not provide regulation of cryptocurrencies as a legal medium of exchange (BAINS et al., 2022). Continuing to engage in such actions puts one in jeopardy.

With a total value of more than $33 billion in proceeds from 2017 to the present, the growth of money laundering cases in the world that use cryptocurrency has been worrying globally since the corruption and money laundering cases involving PT. Asabri, which resulted in an estimated state loss of IDR 10.5 trillion, has increased awareness of money laundering cases in Indonesia involving cryptocurrencies (SIREGAR & SITORUS, 2022). However, not all the money that was laundered was made so under the guise of a cryptocurrency. The limited amount of data readily available on instances of money laundering through cryptocurrency is directly correlated with the challenges presented to detection and law enforcement (FLETCHER et al., 2021).

Concerns regarding law enforcement in the context of money laundering crimes, particularly those committed through cryptocurrency facilities, are linked to several factors (DUMCHIKOV et al., 2023). These factors include legal arrangements for money laundering and cryptocurrency crimes (legal material), law enforcement, facilities and infrastructure, and community factors. It is generally agreed upon that each of the facets mentioned above will make

eradicating crimes involving money laundering more difficult, particularly regarding the proof. The inference here is that cryptocurrencies are or are the consequence of a newly developed technology that includes anonymous aspects. This, in turn, has issues with tracking assets (proceeds of crime), leading to difficulty presenting evidence in court (WIDHIYANTI et al., 2023).

Experts have developed a method for tracing transactions within the crypto ecosystem. This method is called chain analysis, and it was developed after the experts realised the potential of the crypto space. However, chain analysis only applies to cryptocurrencies that carry encryption technology in blockchains, such as Bitcoin (HABIB et al., 2022). Third parties offer these analytical methods, each of which possesses a unique set of analytical procedures that can be quite distinct from those of the other parties. In addition, the anti-money laundering (AML) regime applies the KYC (know your customer) principle as a baseline criterion for all service providers. This is done in response to the growing tendency to employ cryptocurrencies in money laundering offences. The results of an analysis carried out using this method can be classified as electronic evidence, which, in some countries, can cause new problems due to their limited validity and strength. This is particularly the case in countries that have not regulated the distribution and supervision of cryptocurrencies, such as Indonesia, where this is not the case. The domain of money laundering in this context might be strongly tied to international crimes such as the distribution of illegal drugs, the financing of terrorist organisations, and even human trafficking. This is not enough (LEVI & GILMORE, 2002).

The nature and quality of the evidence that can subsequently be used to demonstrate a factual component of the crime of money laundering are at the root of the most fundamental difficulty with the evidence being examined, particularly in nations like Indonesia that are not yet equipped to deal with criminal activity involving cryptocurrencies, such as the ones mentioned above (MUTTAQIM & APRILIANI, 2019). Even nations that are regarded as having advanced technology, such as the United States and the United Kingdom, are confronted with the same challenges, except for gaining access to electronic evidence (the results of blockchain or analysis), which is, of course, much simpler to accomplish given the abundance of third parties that are capable of providing this type of analysis (ALAMMARY et al., 2019).

Proof of a crime relates to the criminal procedural law that is in force in each nation. Within the framework of crypto money laundering, the position of electronic evidence and expert witnesses has a highly important and prominent role. This is especially true when one considers that modern technology plays a direct role in the commission of the crime in question. The complication results in raising problems in proving money laundering, particularly in Indonesia. How,

then, does the comparison of evidence compare with countries that have large volumes of crypto transactions and are ready to eradicate crypto money laundering into a discourse that has the potential to revolutionise the eradication of money laundering crimes? In Indonesia, hence, there is a requirement for a comparative investigation of the evidence gathered in Indonesia, the United Kingdom, and the United States.

LITERATURE REVIEW

Due Diligence in Crypto Transactions in the Anti Crypto Money Laundering Regime

Because cryptocurrency can conceal evidence of criminal activity, the ability of law enforcement to combat crimes involving money laundering has become increasingly difficult since the advent of cryptocurrency (CAMPBELL-VERDUYN, 2018). In addition, several cryptocurrencies offer multilayer anonymous identity mechanisms that conceal the sender, recipient, and transaction amount. However, several cryptocurrencies offer only pseudo-anonymous identification mechanisms (relatively easier to identify). The anonymisation function, in other words, makes it more difficult to identify criminals and conduct investigations into crimes while at the same time making it easier for criminals to commit those crimes (DE HARO-OLMO et al., 2020).

In general, crypto transactions are classified as centralised transactions, which indicates that they are managed and controlled by a centralised operator. This is the case because they are controlled and controlled by a single entity (G. W. PETERS et al., 2015). Users will be able to create accounts and buy cryptocurrencies using fiat currency thanks to transactions, which will have a private key as a form of identity and will have a private key. There is one fundamental term that applies to cryptocurrency transactions, and that term is "buying from FIAT." This phrase refers to the process of exchanging USD currency for cryptocurrency. Additionally, it refers to the ability to exchange one cryptocurrency for another, such as exchanging Bitcoin (BTC) for Ethereum (ETH) for a fee. Percentage. In maintaining the anonymity of a cryptocurrency transaction, which is the fundamental service provided by every transaction centre and issuer of cryptocurrencies, possessing a private key is one of the most important factors to consider (PARTIDA et al., 2022).

Implementing KYC/CDD, which stands for "know your customer" and "customer due diligence," is a duty that cryptocurrency transaction centres must execute as a kind of prevention against hiding the proceeds of criminal activity. In the past, a person could create an account and make withdrawals or purchases with a relatively limited amount of comprehensive information about themselves (AKBAR, 2019). When Know Your Customer and Customer Due Diligence

policies were not in place, all one needed was an email account to engage in these activities. Due diligence and data alignment with institutions or companies that provide financial services are necessary for light of the rapid expansion of the exchanging goods and services industry. The most common forms of identification required by modern KYC procedures are an email address, a photograph of a government-issued ID card, a copy of the customer's most recent utility bill, and frequently a photograph of the customer carrying an ID card (a selfie of the ID holder with ID).

Centralised exchanges (CEX) are those headquartered in nations that are amenable to KYC and CDD, have high standards of AML laws, and have high standards of operation. Customers' safety can be guaranteed in general by adhering to stringent standards; this is especially important when irresponsible business practices threaten customers' safety. Despite this, centralised exchanges that do not impose such rules tend to be more attractive, as demonstrated by BTC-E and MtGox, which reported a profit value of approximately 200 million dollars.

In general, countries that do not follow stringent due diligence criteria in their operations are countries that are frequently used in the process of conventional money laundering. These nations typically have a lengthy history of corrupt practices and lax adherence to legal norms. A participant in cryptocurrency laundering may also consider the level of involvement or collaboration of the country in question with international financial institutions (CALAFOS & DIMITOGLOU, 2023).

In addition to being a centralised exchange, it is also known as a decentralised exchange, or DEX for short. DEX is a direct transaction, also known as a peer-to-peer transaction. When conducting transactions through the decentralised platform, users will not have custody of their private keys because the platform does not have custodial control (Zhou et al., 2021). DEXs use smart contracts, digital agreements that permit the recording of cryptocurrency asset transactions without the need for a central authority. As previously established, both platforms will continue to apply their due diligence processes to the information standards required to use platform services. Even though there has been a consistent push for the global implementation of KYC/CDD standards for cryptocurrency transactions or trading, there are still no common norms. This was not the case as predicted. Nevertheless, there is some convergence to the FATF's view that cryptocurrency payment service providers should be subject to the same obligations as non-crypto payment service providers. Furthermore, most jurisdictions that have issued rules or guidance on the subject have concluded that the commercial exchange of cryptocurrency for fiat currency must be subject to AML obligations (or, in the case of China, prohibited) (GOLDBARSHT & DE KOKER, 2022).

The extent to which KYC/CDD rules also cover administrators and service providers; the existence of special licencing requirements for virtual currency exchange (VCE); the degree to which an initial coin offering (ICO) is covered by securities laws or equivalent regulations with AML regulatory implications; and the nature of the licencing requirements for virtual currency exchangers. These are just some of the notable differences between the national regulations of different countries. The degree to which the exchange of one cryptocurrency for another is handled differently than trading one cryptocurrency for fiat currency.

The ability of providers of financial services, particularly those dealing in cryptocurrency, must have the capacity to check and authenticate each customer's identity, location, and destination, just as is done in the provision of traditional financial services. Although the ability to conduct transactions pseudonymously serves as the foundation or essential component of most cryptocurrencies, financial service providers can only engage in client relationships after the customers' genuine identities have been verified (WERBACH, 2018).

Implementing the Know Your Customer and Customer Due Diligence regime within the cryptocurrency business is essential in preventing and doing away with crypto money laundering (REYNOLDS & IRWIN, 2017). This is the fundamental component in the investigational strategy and gathering evidence that should be suspicious of money laundering with cryptocurrencies. Additionally, not every government has yet adopted the same viewpoint concerning cryptocurrencies, and there is no international cooperation to combat the laundering of cryptocurrency-based funds. Additionally, the implementation of the Know Your Customer (KYC) and Customer Due Diligence (CDD) regime in any activities involving cryptocurrencies, in addition to traditional financial activities, is an attempt to lessen the influence of or the potential for fraud brought on by the crypto ecosystem's reliance on anonymity or pseudo-anonymity. The potential for theft that is being questioned here is essentially that of money laundering.

Digital Evidence in Eradicating Crypto Money Laundering

Transactions in the context of cryptocurrencies or other digital assets take place at high speeds, such as transforming targets into victims in seconds or minutes, or they are immediate (DUPUIS et al., 2023). The commission of a crime is typically an irreversible process. This is especially true if the individuals responsible for the crime ensure that their activities are not recorded in the blockchain system. This makes the process of investigation and verification more difficult. For law enforcement to be able to battle crimes using cryptocurrencies and other digital assets effectively, they need to have the ability to quickly access evidence regarding the crimes that are currently under investigation as well as

transactions related to those crimes. Quite a few Virtual Asset Service Providers (VASPs) operate outside of law enforcement's authority. Because of this, the procedure of law enforcement, particularly the verification process, is made more complex (SHARMA, 2020).

First, VASPs that operate outside of the jurisdiction (overseas) will make it difficult for law enforcement to obtain records or evidence, particularly in countries that prohibit law enforcement from obtaining related documents directly (voluntarily) from these entities or through informal law enforcement. This is an issue because VASPs that operate overseas will make it difficult for law enforcement to obtain records or evidence. Law enforcers can try to do so through rogatory letters, foreign domestic legal mechanisms, or reciprocal relations between the two countries when the two countries have bilateral mutual legal assistance (MLA) agreements or through multilateral agreements (Budapest Convention). When these two alternatives are not possible, law enforcers can try to do so through reciprocal relations between the two countries. This formal inter-governmental request can be used to get evidence located overseas. However, because it takes a very long time, this will hamper the purpose of recovering assets in the framework of the asset forfeiture paradigm in dealing with crimes involving money laundering. Because the speed at which evidence can be obtained in cybercrime, and particularly in cases of cryptocurrency money laundering, plays an important role in the process of law enforcement, and of course, in the saving of assets, it can be said that neither mutual legal assistance nor other formal approaches are the best approach when dealing with cryptocurrency money laundering cases (AKBAR, 2019).

Second, even though it is possible to obtain digital records or related documents by making a formal request, either through a bilateral agreement or in another way, the associated documentation that the VASP owns may no longer be stored. This is the case even though obtaining digital records or related documents is possible. When a situation like this arises, the VASP is no longer in possession of the relevant documentation. The KYC and CDD rules in the countries where VASPs operate may differ, which could limit the breadth of the evidence that can be obtained. On the other hand, there is a possibility that VASP cannot disclose to account holders. This is certainly not to the advantage of law enforcement because of the potential for perpetrators to delete evidence, particularly while proving their innocence. Because collecting evidence determines the validity of evidence, haphazard efforts can eliminate the meaning of the evidence. Under these circumstances, the government and those charged with enforcing the law must work together to cooperate in the surveillance and investigation of transactions that have the potential to be acts of money laundering.

Third, there is a trend for virtual private network service providers (VASPs) to move their business operations toward decentralisation. This can be accomplished by registering their business in one country, locating their personnel in another, or separating their technical and private key infrastructure in different countries. Because the VASP entity is located in two (or more), it would make any efforts to enforce the law more difficult if the business was run in such a way that it involved many jurisdictions. Because of these conditions, law enforcement officials need to use extreme caution when deciding which countries to formally and informally transmit demands for documents too.

The extraction of digital and electronic information for investigation and even verification can be accomplished through various procedures and tools. "Chainalysis" is an analysis that the public can use in the context of using the blockchain encryption method. This analysis uses machine learning algorithms to trace the flow of funds, senders, and recipients. In this context, the blockchain encryption method is used. Nevertheless, activities such as mixing coins might make the investigation process more difficult. Placement, layering, and integration are the three processes utilised in traditional money laundering, which are also generally utilised in the context of crypto money laundering (REEDY, 2023).

When users initially make purchases or transactions in cryptocurrency, the layering process is carried out. This procedure is carried out in different amounts and for different periods. There is a significant difference between traditional money laundering and cryptocurrency money laundering. Following the completion of the layering process, the money is finally returned to the financial system as clean money by using the exchange services that the VASP offers. This difference in nature makes it even more difficult to answer whether traditional AML regulatory regimes can be applied to efforts to control cryptocurrencies and the exchanges that trade them (SANZ-BAS et al., 2021).

In addition to the differences mentioned above, another implication comes into play about the ecosystem in which layering takes place. That implication is the significance of evidence within the context of law enforcement in the context of cryptocurrency money laundering. Many researchers believe that the position of evidence and its acquisition in the context of crypto money laundering is on a more complicated level than it is in the context of conventional money laundering, even though it has been stated that there are various obstacles in the process of obtaining evidence, both of which originate from related regulations, VASP policies, and limitations imposed by law enforcement. This is made even worse by concerns regarding implementing the AML regime, which calls for adjustments (WARDHANA & NUGROHO, 2021).

In proving a case, the evidence presented to the judge has the purpose of persuading the judge of the validity of the arguments that have been levelled against the defendant. To be admissible as evidence, these arguments must be gathered by the procedural law rules. In addition, any investigation that uses analysis tools is regarded as electronic interception, and every nation has a stringent policy regarding this subject. Furthermore, any interception efforts carried out without following the appropriate legal procedures will invalidate the evidence obtained by the returnee. There is no regulation of cryptocurrencies and the tools used to investigate them. The predominance of electronic evidence as a factor that complicates or hinders law enforcement efforts against crypto money laundering is expected to occur.

RESEARCH METHODS

The comparative legal technique is a research methodology utilised to compare and study the legal systems, laws, and regulations of other countries to uncover similarities, differences, strengths, and flaws. This strategy is especially helpful in research investigating legal frameworks' efficacy in resolving certain problems or difficulties (BHAT, 2015).

The comparative legal technique is a useful tool that may be utilised in this research project to investigate and evaluate the anti-money laundering (AML) policies of the three nations. In particular, the investigation might concentrate on the admissibility of electronic evidence in AML cases, such as emails, text messages, and other digital documents.

The study will be able to identify best practices, gaps, and obstacles in using electronic evidence in anti-money laundering cases if it compares the legal frameworks of the three nations. The study can, for instance, examine the criteria for the admissibility of electronic evidence in court, the forms of electronic evidence that are recognised, the burden of proof that is required, and the legal remedies that are accessible to the parties.

In addition, the comparative legal technique can be utilised to investigate the institutional frameworks, regulatory environments, and enforcement mechanisms in place to support the anti-money laundering regimes of the three nations. The study has the potential to provide valuable insights into the efficacy of AML regimes in preventing and identifying activities related to money laundering by comparing the roles and responsibilities of relevant actors. These relevant actors include law enforcement agencies, financial institutions, and regulators.

RESULTS

Electronic Evidence of Crypto-Money Laundering Crimes in the AML-Crypto Regime in the UK

In the United Kingdom's Anti-Money Laundering and Cryptocurrency Regulations (AML-crypto regime), electronic evidence plays a vital role in the ongoing fight against money laundering, particularly regarding the usage of cryptocurrencies. This is particularly important because the regulations were enacted in the United Kingdom. This point is driven home even further by a report submitted to the BBC by the National Crime Agency (NCA), which forecasted a thirty percent increase in the incidents of money laundering through cryptocurrency in 2021 alone. The research also disclosed that the total income from illegal activities involving cryptocurrency was estimated to be somewhere in the neighborhood of $8.6 billion.

In order to tackle this rising problem, law enforcement organizations heavily rely on analysis facilities and methodologies to determine the scale of bitcoin launderers and the value of the unlawful operations they engage in. The results of these investigations are beneficial in the process of creating efficient procedures for identifying transactions that have the potential to be linked to money laundering.

To collect the necessary evidence, law enforcement officials can make specific information requests to Virtual Asset Service Providers (VASPs) reporting suspicious activities. VASPs are companies that handle virtual assets. This request has the ability to include accounts that have been involved in transactions that exceed a predetermined minimum threshold. Law enforcement organizations can acquire access to transaction data, user information, and other pertinent records when they develop partnerships with VASPs. This allows them to track and investigate the movement of funds across the blockchain.

Using this coordinated strategy, law enforcement can collect the electronic evidence necessary for constructing cases against persons or organizations engaged in actions related to money laundering. When trying to prove a connection between illegal funds and the individuals or organizations responsible for their creation, having proof gathered through blockchain analysis and other methods is necessary.

The AML-crypto system in the UK places a significant emphasis on the collection and use of electronic evidence and collaboration with VASPs. By using these capabilities, law enforcement authorities will be able to more effectively battle the growing threat of money laundering through cryptocurrencies and work toward creating a more secure financial system.

The anonymity offered by cryptocurrencies and their lightning-fast transaction times frequently combines to cause problems. Since transactions take place quickly, there is a possibility that the proceeds of the crime may be moved before the investigation process and evidence collection can be carried out because of the anonymity that will be provided for the analysis, which will provide a time lag for the analysis to be carried out. In light of these issues, the British government decided to strengthen the regulations governing cryptocurrencies by imposing an anti-money laundering (AML) regime on all cryptocurrency service providers and making it mandatory for them to register with the Financial Conduct Authority (FCA). Within the confines of the regulation known as the Markets in Financial Instruments Directive II (MiFID II), the Financial Conduct Authority (FCA) is responsible for regulating the operating licences of cryptocurrency exchange centres. The FCA is the regulatory body that monitors exchange companies to ensure that they always adhere to the Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements.

The United Kingdom government generally takes a preventative stance against money laundering through crypto assets. This is accomplished by increasing the level of control placed on assets and exchange businesses. In addition, the United Kingdom government established the Crypto Asset Taskforce (CAT) in 2018 to prevent cryptocurrency from being used for money laundering. The CAT is the organisation that directly monitors the trading of cryptocurrencies and carries out risk assessments.

In the context of the evidential law of the United Kingdom, the term "electronic evidence" primarily refers to the form of electronically generated evidence typically produced by or through a computer or other mechanical equipment. Evidence obtained from individuals is in the form of documents obtained by a computer that are copies of the information provided, which humans use as input. This type of evidence is treated as news. Electronic evidence is divided into several different types, including first, concrete evidence, which is evidence obtained through analysis or calculations with computer devices such as calculations with certain software or hardware; second, evidence obtained from organisations, which is evidence obtained by organisations that are copies of the information provided that is used as input by humans; and third, derivative.

The admissibility of electronic evidence is not called into question by the requirements of either criminal or civil procedural law. In civil law, the validity of electronic evidence was legalised through the Civil Evidence Act of 1995, which regulates the receipt of electronic evidence, certain documents, and the acceptance and evidence of official actuarial tables in civil law proceedings. This act also legalised the validity of official actuarial tables as evidence in civil law proceedings. The provision of the law that governs the admissibility of electronic

evidence as legal evidence can be found in paragraph 3. In addition, by section 8 of the Act, evidence of a statement included in a document may be presented to the court as either the original document or a duplicate of it. In this regard, the document contains various planning documents, photographs, and models by Rule 33.6 Section 33 of the evidence regulations in the Civil Evidence Act of 1995.

In the meantime, the Police and Criminal Evidence Act of 1984 made it possible for prosecutors to use electronic evidence in court trials. All of the information stored in a computer is considered to be electronic evidence, which is why it is admissible as evidence in a legal proceeding. The next topic of discussion will be whether or not a document generated by a machine may be presented as evidence. The judge determined that the computer records can be used as evidence as long as it can be demonstrated that the machine is operating correctly and has not been misused.

It is important to recognise that electronic evidence can be easily modified, overwritten, or even deleted, which challenges ensuring the authenticity and validity of electronic evidence (MOUSSA, 2021). Because electronic evidence can be easily modified, overwritten, or deleted, this presents a challenge. The authenticity of information generated by computers and stored on computers can create security vulnerabilities in operating systems and programmes that can threaten the integrity of digital information. Malicious actors can exploit these vulnerabilities to gain unauthorised access to sensitive data. When electronic evidence was presented, a strong focus was placed on "the necessity to demonstrate computer accuracy in the storing and retrieving the material at issue." If the building in question does not have a reliable security system, the credibility of any electronic evidence produced by a computer or computer system may be questioned. The British Standards Institute first released the exceptional standard known as BS 10008: Weight of evidence and legal acceptability of electronic information (specification) in 2008 to address the specific problem of the authenticity of electronic evidence in British courts. This standard was later revised in the year 2014 (MOHAMAD, 2019).

The standard tackles concerns relating to the authenticity and integrity of information and the requirements for the construction and operation of an electronic information management system, including the storage and transmission of information. Every electronic information that must be provided as proof of a business transaction is accorded the utmost evidentiary weight thanks to BS 10008, which assures this. The process is based on a requirements specification for an organisation's information management system, which is used for designing, implementing, operating, monitoring, and upgrading the system (AKHTAR & FENG, 2022).

Specific areas that are covered by the standard include the long-term management of electronic information, including information that has undergone a technological change in an environment where information integrity is a vital requirement, the management of various risks associated with electronic information, information on how to demonstrate the authenticity of electronic information, management quality issues associated with the document scanning process, as well as providing a complete life history of the object being scanned. Especially in the context of criminal trials, the presence of a security system in an instrument is critical in establishing the level of trust or the weight of evidence or evidence.

For digital evidence to be recognised in the legal system of the UK, it is important to obtain it under "appropriate authority." Before they are allowed to search, confiscate, or analyse digital devices, investigators must first acquire a search warrant or a subpoena. As was just said, any digital evidence obtained illegally cannot be used in court, and if it were valid evidence, to begin with, it would no longer be considered so. Warrants to conduct searches have a greater degree of leeway for interpretation in the United Kingdom than they do in the United States. Various kinds of warrants can be issued in the English court system. Some examples of these warrants are "particular premises warrants," "all-premises warrants," and "multiple entry warrants." When investigators have been permitted to examine a computer, electronic device, or system, they must confine their attention entirely to the case. If the investigator discovers evidence of other offences while searching, the evidence is inadmissible since it goes beyond the parameters of what was permitted by the warrant. In these situations, the investigators need to get a second warrant before utilising the evidence to bring charges against the person who committed the crime.

In addition, the investigators may be required to acquire two additional warrants for the computers seized: one for the machine itself and another for any digital data or documents found on the computer. Computers that have been confiscated are considered "real" evidence for the reception. On the other hand, individual files need to be acknowledged one at a time by article 117 of the Criminal Justice Act of 2003. This is of utmost significance in situations where more than one individual has access to a computer. The phrase "best evidence" relates to the idea that, under the law, original copies of documents are considered to be the most reliable and trustworthy form of evidence. However, with the development of technologies such as photocopiers, scanners, computers, and other devices that can effectively produce replicas or copies that are identical to the original, it is now possible to accept duplicates that are not only restricted to original documents. This opens up a whole new realm of possibilities (MONTASARI, 2016).

Evidence that has been copied, rather than evidence that has been presented in its original form, will be considered admissible if it can be demonstrated that it satisfies the other conditions for admission. The issue is not a major worry, and copies of the original are acceptable in courts in the UK because it is possible to recreate the majority of electronic forms of evidence with precision. Making identical pieces of electronic evidence is more typical to eliminate the chance of accidentally manipulating the original. This is done for several reasons. According to Article 114(1) of the Criminal Justice Act 2003, also known as the "Hearsay Rule," electronic evidence will not be accepted if the witness (digital forensic analyst) does not appear in court to verify the correctness of the evidence referring to the regulation. This is because the "Hearsay Rule" requires the witness to verify the accuracy of the evidence (STANFIELD, 2016).

In the AML-crypto system, notably in the UK, there are several important factors to consider when it comes to electronic proof, specifically: The requirement that suppliers of transaction services must submit their companies to register with the Financial Conduct Authority (FCA); Implementation of Know Your Customer and Customer Due Diligence in each transaction by giving personal information; FCA monitoring of AML/CTF compliance with VSPs Analysis of the blockchain or analysis as a basis for mapping the hazards of money laundering in cryptocurrency; Collecting evidence by law enforcement can only be done so based on a court order, in which case law enforcement has the power to seek for the cooperation of third parties, including crypto service providers and blockchain/analysis providers; The discussion on how strong the proof of electronic evidence is in this instance depends on three factors: the authenticity, the validity, and the integrity of the evidence. Additionally, an expert opinion is required to translate the findings of the blockchain/analysis so that the evidence can be presented in court.

In legal proceedings involving illegal activities related to the laundering of cryptocurrency-related funds, electronic evidence is collected within the context of the relevant legislation governing criminal law. The Police and Criminal Evidence Act of 1984 contains Section 69, one of the pertinent provisions for evidence collecting in the United Kingdom.

When it comes to situations involving cryptocurrency and money laundering, electronic evidence can be gathered through various methods, including the findings of a blockchain study (HM Treasury, 2015). The report from HM Treasury published in 2015 emphasizes how important it is to analyze user (account) and transaction data to obtain proof.

In order to get this evidence, law enforcement agencies frequently collaborate with Virtual Asset Service Providers (VASPs) in response to a court order. This allows the agencies to obtain the evidence more efficiently. Virtual

Asset Service Providers (VASPs) are organizations that make it easier to trade or transfer bitcoins. Cooperation with VASPs is necessary because they are the ones who can grant access to relevant transaction records and user information.

How the electronic evidence was gathered and presented in court plays a significant role in determining the weight assigned to it. It is helpful to the credibility of the evidence that the method of gathering evidence followed legal requirements, such as getting a court order and following the right processes. This helps to ensure that the evidence is accurate.

In addition, it is not uncommon for experts in blockchain analysis to be present in court while the judge is hearing the case. These experts can provide the judge and jury with an explanation of the conclusions made from the blockchain analysis research, assisting them in comprehending the technical components of the evidence provided and the ramifications of those features.

Electronic Evidence of Crypto-Money Laundering Crimes in the AML-Crypto Regime in the United States

Regarding regulating cryptocurrencies, the United States is among the most stringent countries in the world. It is explicitly stated that cryptocurrencies are not legal tender of exchange like fiat money within their legal frameworks, and the laws of each state are the only ones that recognise cryptocurrencies as a commodity of exchange. Notwithstanding this, there are responsibilities associated with licence registration, particularly for cryptocurrency issuers and exchange service providers registered with the Financial Crimes Enforcement Network (FinCEN). In this context, "other value that substitutes for currency" or "other commodities that can be substituted for currency" are acceptable definitions of cryptocurrency. When discussed in this manner, the term "currency" does not refer to cryptocurrencies as a kind of fiat money; rather, it is understood to mean something that possesses value in terms of fiat currency. At the same time, the Internal Revenue Service (IRS) defined cryptocurrency as "a digital representation of value that functions as a medium of exchange, a unit of account, and a store of value." Alternatively, the IRS defined cryptocurrency as a digital representation that functions as a medium of exchange and can have a certain value (ALKADRI, 2018).

The Bank Secrecy Act of 1970 applies to a wide variety of different kinds of crypto transactions, including exchanges. This law was passed in 1970 (DeWaal & Dempsey, 2015). The Act emphasises applying the AML regime to any form of financial transaction, which includes cryptocurrency transactions. While the Commodity Futures Trading Commission (CFTC) recognises Bitcoin as a "currency," the Securities and Exchange Commission (SEC) has fined several companies for issuing "commodities" without following the appropriate

procedures. This is even though the CFTC recognises Bitcoin as a "currency" (registering through FinCEN). In general, the emergence of cryptocurrencies produces substantial dialogue, is related to an increase in crypto-money laundering offences, and is associated with increased concerns regarding data privacy (FLETCHER et al., 2021).

As a direct response to the guidelines published by the FATF in June 2019, FinCEN has made it abundantly clear that cryptocurrency exchanges must comply with the "travel rule" and collect and share information regarding the senders and beneficiaries of cryptocurrency transactions. This places cryptocurrency (virtual currency) transactions in the same regulatory category as traditional money transfers and applies all of the same laws, including those outlined in the Bank Secrecy Act (ZWITTER & GSTREIN, 2021). The Financial Crimes Enforcement Network (FinCEN) will issue a Notice of Proposed Rulemaking (NPRM) in October 2020 concerning modifications to the Travel Rule. This will indicate the beginning of new compliance requirements for cryptocurrency exchanges. The "Travel Rule" stipulates the obligation of every service provider to screen, record, and communicate information from senders and recipients of cryptocurrency transactions, particularly for transactions worth more than $1,000 or a certain amount determined by FATF members. In particular, the "Travel Rule" focuses on transactions worth more than $2,000 because this is the threshold at which FATF members are required to screen, record, and communicate information (WIDHIYANTI et al., 2023).

The majority of cryptocurrency systems are also essentially "disintermediation" tools or service providers, which means that they offer a secure method of holding and controlling property and financial assets in a "direct" way, without the need for trusted intermediaries such as banks, notaries, or other similar entities. This is accomplished using cryptographic keys kept in a security device within the user's direct control (their crypto wallet). Hence, based on these factors, VASP must report on the transactions they serve annually, and this report is one of the bases for limiting the danger of money laundering and terrorist funding through the use of cryptocurrencies (GARCIA-TERUEL & SIMÓN-MORENO, 2021).

Each exchange service provider and cryptocurrency issuer is expected to use the KYC/CDD concept as a persuasive approach to the risk of crypto money laundering. This obligation is based on suggestions made by FinCEN. In this scenario, VASP also offers information on potentially dangerous parties or accounts in addition to the requirement to disclose annual transaction activity. As a result, the CDD review will most likely be expanded. The findings of certain analyses, which in this context are the findings of blockchain analysis, can show which accounts have the potential to engage in cryptocurrency money laundering.

Based on these findings, the authorities can then carry out developments concerning money laundering cases that have already occurred. Based on the findings of this investigation, additional inquiries can be conducted by sending a notification to the VASP or the provider, requesting that they disclose the account and transaction data for the very first time to carry out inquiries by the principle of enhanced due diligence (EDD) (COELHO et al., 2021).

The use of digital evidence is conceptually equivalent to the use of other types of evidence in the sense that both types of evidence consist of information that is utilised to locate persons and events in time and location to prove the causation of criminal acts. Compared to physical evidence, digital evidence has a broader scope, is more personally sensitive, is mobile, and requires different training and tools. This is especially true in the cryptocurrency ecosystem, which has several transaction data security safeguards. In this instance, the extraction or method of obtaining evidence relating to a crime is critical in determining whether a piece of evidence has the strength of evidence, as regulated in criminal procedural law in many other countries. This is the case because the extraction or method of obtaining evidence relates to a crime. The National Justice Institute (NJI) defines "electronic evidence" as "valuable information and data for investigations that are stored, received, or sent by electronic devices." Given that the results of blockchain/analysis can be classified as "electronic evidence" that can show valuable information in an investigation of crypto money laundering crimes, it follows that the National Justice Institute (NJI) defines "electronic evidence" as "information and data that is valuable for investigations that are stored, received, or sent by (KARAGIANNIS & VERGIDIS, 2021).

The United States Supreme Court increased the use of electronic evidence by introducing the concept of pervasiveness as a trait differentiating electronic evidence from definitive evidence. It is claimed in these qualities that three components are differentiating features, and they are as follows: The reach of electronic evidence is expansive; The evidence relates to sensitive information, both personal and physical; and Relating to or concerning interconnected aspects of criminal justice that extend beyond the traditional duty of law enforcement in the amassing of evidence (MASON & SENG, 2017).

These three features show that electronic evidence is not restricted to recordings in either analogue or digital formats. Instead, it can also include other types of data. What can be observed in an electronic device or the findings of an analysis that uses particular procedures and various other forms of technology can be used as forms of electronic evidence. In this context, the findings of blockchain analysis are classified as belonging to the second category of electronic evidence. This is because their acquisition requires the development of code using an algorithm and the need for specialised expertise. In addition, the process of

obtaining electronic evidence differs from the way it is regulated in England. Suppose law enforcement discovers evidence of another crime during the collection of evidence. They do not need to obtain a new warrant. Instead, in this scenario, law enforcement has more leeway to obtain evidence of a crime.

Despite having wider leeway, the acquisition of evidence, particularly electronic evidence, is governed by the Fourth Amendment to the Constitution of the United States and the Privacy Law, which may be found in sections 2510-22, 2701-12, and 3121-27 of Title 18 of the United States Code. The reliability of the evidence, particularly that which was acquired using specialised tools or apparatuses, is a recurring issue that needs to be addressed. When recreating evidence, those who enforce the law are responsible for ensuring the dependability and integrity of the instruments they use. It is important to note that FinCEN, by the regulations of Section 314(a), authorises federal, state, local, and foreign (EU) law enforcement agencies to be able to reach financial institutions through FinCEN in order to find accounts and transactions about interested parties. This is something that FinCEN can do. May be involved in terrorist activities or the laundering of illicit funds, except for maintaining bank secrecy (JONES et al., 2020).

The Currency and Foreign Transactions Reporting Act of 1970, often known as the Bank Secrecy Act (BSA), stipulates that financial institutions in the United States must assist government authorities in the United States in order to detect and prevent instances of money laundering. More specifically, the law mandates that financial institutions keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and report any suspicious activity that may indicate money laundering, tax evasion, or criminal activity. Other. A common synonym for the BSA is "anti-money laundering" (AML) laws, and the two are sometimes referred to jointly as "BSA/AML." Several laws, such as those found in Title III of the Act to Unite and Strengthen America by Providing the Appropriate Tools Needed to Deter and Deter Terrorism (USA PATRIOT) of 2001 and the Anti-Money Laundering Act of 2020, have been in effect up until the present time in order to renew the BSA (See 12 USC 1829b, 12 USC 1951-19600, 31 USC 5311-5314, 5316-5336, and 31 CFR Chapter X [formerly 31 CFR Part 103]) (GELEMEROVA, 2009).

As a general rule, by the regulatory framework that is now in place in the United States, electronic evidence possesses the same evidentiary power as evidence in general so long as the validity, authenticity, and integrity of the evidence can be assured. It is particularly emphasised that there are no obstacles in the instruments and techniques for obtaining evidence, which is stated: "[A] search can be as much an art as a science," in the United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005), which has the implication that in obtaining such

evidence law enforcers can partner with competent parties who, in this context, are blockchain/analysis experts by ensuring the three defining elements that have already been mentioned In the context of the government obtaining evidence that is located outside the jurisdiction of the United States, they can do so by making an official request or by going through a third party as long as the service provider is registered in the jurisdiction of the United States. This is about section 2703 of Title 18 of the United States Code (f) (ELIZONDO et al., 2012).

When evaluated based on the factors of legislative rules, law enforcement authorities, resources, facilities, and infrastructure, the anti-money laundering and cryptography (AML-crypto) regime in the United States is deemed to have high levels of integrity. In this regard, the United States is better prepared to deal with money laundering crimes committed through cryptocurrencies. This is especially the case given that the United States and the United Kingdom have collaborated in collecting electronic books, which can be carried out through third parties in each country. This collaboration was ratified on October 3, 2019. The United States and the United Kingdom are better prepared to deal with the mode of money laundering crimes that are committed through cryptocurrencies (Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data to counter Serious Crime) (KHAN et al., 2006; R. J. PETERS et al., 2021).

The enforcement of the Anti-Money Laundering (AML) regime in the United States is intricately connected to the examination of electronic evidence that is conducted through the analysis of blockchain technology. Every Value-Added Service Provider (VASP) is required to give assurances for information disclosure in order to maintain compliance with the Financial Crimes Enforcement Network (FinCEN) under the Bank Secrecy Act (BSA). This is particularly important in situations involving the users of the VASP's services engaging in illegal activities such as money laundering.

When it comes to detecting and prosecuting incidents of cryptocurrency money laundering, the inherent anonymity of cryptocurrencies presents a unique set of obstacles. However, the results obtained from the analysis of blockchain data and those obtained from other analytical methods play an essential part in establishing evidence of these crimes. By examining the blockchain, investigators can track the movement of funds, identify questionable transactions, and relate them to individuals or businesses involved in money laundering activities.

The BSA offers a legal framework in the United States that permits investigators to omit bank secrecy protections from the investigative process. This is possible because of the framework. This indicates that financial institutions, especially VASPs, must fully collaborate with the authorities, reveal necessary

information, and assist in investigating potential money laundering actions. In the investigation and prosecution of crypto money laundering cases, the information collected through blockchain analysis can be utilized to support the investigation and prosecution of these cases, offering significant insights into the identities and activities of those involved.

By utilizing the authority afforded to them by the BSA, law enforcement agencies can make information requests to VASPs. These requests can include a request for transaction records, user data, and any other pertinent information required to investigate possible money laundering operations. In order to guarantee that the AML regulation is carried out efficiently, VASPs are required by law to comply with these requests and give the information being asked.

DISCUSSION

Depending on the context, cryptocurrencies may be referred to as either electronic currency or virtual currency within the framework of Indonesia's legal system. This language is utilized not only in the United Kingdom but also in the United States. This interpretation is based on the fact that cryptocurrencies are understood to be a form of digital currency that may function as a means of trade, much like traditional fiat currencies. However, it is essential to remember that cryptocurrencies' value is derived from fiat currencies such as the Indonesian Rupiah, the United States Dollar, or the British Pound. Because of this, cryptocurrencies are not considered to be a currency in and of itself (ROVITA & IMANULLAH, 2018).

Additionally, the United States and the United Kingdom have acknowledged that virtual currencies are assets subject to taxation. This indicates that persons or businesses participating in transactions involving cryptocurrencies may be subject to taxation on their earnings or profits from participating in such transactions. The regulatory framework for the taxation of cryptocurrencies is still being developed and may differ from nation to nation.

Even if cryptocurrencies are not acknowledged as a medium of exchange in these three countries, they can be dealt with as digital commodities. This is an important distinction to make. Because of this, cryptocurrencies can be purchased, sold, and traded in a manner analogous to that of stocks, bonds, or other assets. Their value shifts constantly in response to shifts in supply and demand on the market, much like traditional commodities trading.

Because cryptocurrencies are also referred to as virtual currencies, the existence of crypto-currencies generally falls under the purview of Bank Indonesia Regulation No. 11/12/PBI/2009 concerning Electronic Money. However, there are currently no regulations in place in Indonesia that specifically regulate cryptocurrencies. This refers to the definition of electronic money, which

states that currency can be created by depositing money through a rupiah or other currencies with the issuer. When discussing cryptocurrency as a form of payment, one should refer to Article 34 of Bank Indonesia Regulation No. 18/40/PBI/2016 concerning the Implementation of Payment Transaction Processing (SUKARNO & PUJIYONO, 2020). This section explains that payment system service providers are not permitted to process transactions using virtual currency. In the context of these regulations, the term "virtual currency" refers to a kind of digital money produced by entities other than monetary authorities and obtained through mining (SANTOSO et al., 2019).

However, the issuance of Minister of Trade Regulation Number 99 of 2018 concerning General Policy for Organizing Crypto Asset Futures Trading, in general, has implications for the legality of crypto money as a commodity on futures exchanges and is supervised by the Agency (MUTTAQIM & APRILIANI, 2019). Although not all forms of cryptocurrency can be used in all forms of payment, it is important to note that this regulation was issued because all forms of cryptocurrency cannot be used in all forms of payment. Supervisor for the Trading of Commodities Futures. In the process of its development, concerning Law Number 4 of 2023 About the Development and Reinforcement of the Financial Sector, the Financial Services Authority is responsible for regulating further distribution and transactions of cryptocurrencies (OJK). This has repercussions for the anti-money-laundering framework that exists within the cryptocurrency ecosystem.

The AML regime, in this instance, is covered by OJK Regulation Number 12/POJK.01/2017 (POJK 12/2017) concerning implementing Anti-Money Laundering and Prevention of Terrorism Funding Programs in the Financial Services Sector (SARUNGU, 2020). This regulation stipulates that crypto financial service providers, subject to OJK supervision, must comply with the KYC/CDD requirements outlined in the regulation. The application requires users to provide certain information, including their identity, the beneficial owner's identity, information on sources of funds and average income per year, and the goals and objectives of using crypto financial services. This information can be found in the application.

The emergence of the money laundering crime case involving PT Asabri, allegedly also carried out through transactions involving cryptocurrencies (specifically Bitcoin), became a flash point that prompted increased attention directed towards the possibility of cryptocurrencies being used in money laundering. Because of the system embedded in cryptocurrency services, criminals who use nominees, and the level of familiarity with blockchain analysis technology/analysis, law enforcement has a difficult time disclosing and collecting evidence. This is a lesson that law enforcement has learned from this

case. Meanwhile, this analysis can be a solid foundation for revealing or investigating crypto money laundering offences because it can expose the number of transactions, the time, and the transaction address. In other words, it can reveal all of the details. Meanwhile, assistance from PJK is required to disclose accounts that make transactions, although bank confidentiality is not one of the requirements.

The results of anti-money laundering (AML) regimes and analysis play a significant role in implementing AML regimes and enforcing money laundering legislation. The investigation findings can, in a general sense, be considered evidence in light of the topic that has already been offered. According to Article 184, paragraph 1 of the Criminal Process Code, the following items are considered to be "evidence" under Indonesian criminal procedural law: witness statements; expert testimony; letters; instructions; and the testimony of the accused themselves. It is stated in Article 5, paragraph 2 of Law Number 19 of 2016 concerning the Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions that electronic information and electronic documents and their printouts are an extension of electronic evidence. This is pertinent to the topic of electronic evidence. Valid legal proof in line with the legislation that governs the procedures that can be used in Indonesia. As a result, evidence in criminal procedural law in Indonesia has increased and expanded. As a result, electronic information and documents have been placed on an equal footing with evidence, as is provided in paragraph 1 of article 14 of the Criminal Process Code (MANSHUR et al., 2019).

Asimah has stated that problems frequently emerge in using electronic evidence, concentrating on authentication concerns, methods for acquiring and submitting electronic evidence, and signatures. The fact that a kind of interference with information, in the form of alterations, can be produced so that there is a chance of discrepancies or changes in the contents of the evidence is one of the reasons why this evolved as a problem. The procedure for making, using, and assessing the strength of proof as electronic evidence is not adequately covered in electronic evidence. Even when referring to the laws already in place in the Electronic information and transactions Law that regulate the addition and growth of the evidence described above, on a practical level, basic challenges linked to the reliability of the electronic evidence occur.

Article 5, paragraphs 3 and 4 of the Electronic information and transactions Law regulate the standards that must be completed for a piece of electronic evidence to be admitted in court. Despite this, the lack of well-defined laws and procedures governing electronic evidence can have ramifications for the problem of legal uncertainty for law enforcement officials, forensic professionals, criminals, and victims of crimes. Especially when referring to Article 28 of the

Judicial Powers Act, which mandates that all legal arrangements related to procedural law be regulated in the form of a law, the need to formulate electronic evidence in (formal) criminal procedural law will become apparent at the level of evidentiary practise involving electronic evidence. Act. Several perspectives might be found regarding electronic evidence among law enforcement officials and judges. As indicated earlier, this variability might essentially obscure the value of legal certainty.

This differs from the arrangements made regarding electronic evidence in the United States and England. Those arrangements have been regulated in (formal) criminal procedural law so that their implementation can guarantee the value of legal certainty, particularly in the case of proving a crime, specifically regarding the gathering and analysis of authenticating electronic evidence. It is true that electronic information and transactions. The law requires that electronic evidence fulfil various requirements, including its integrity. However, in practice, all such examinations are completely handed over to each institution that examines electronic evidence, making it difficult for the judge to see the integrity of the electronic evidence so that it is not admissible. It is peculiar thing that different people have different opinions regarding electronic evidence.

Only digital records can serve as clues or evidence that some form of money laundering has occurred, so electronic evidence is becoming increasingly important in the context of crimes involving the laundering of cryptocurrency funds, where all transactions or flows of funds occur. The findings of a blockchain or analysis are crucial in determining whether or not a money laundering crime has been committed. The results of such an analysis can provide an early indication of transaction anomalies, which are then forwarded to Financial Sector Business Actors (PUSK), particularly VASPs, in order for them to disclose information related to the account. In addition, money laundering using cryptocurrencies might occur on a larger scale, involving VASPs or PUSKs beyond law enforcement's authority. Hence, international collaboration is required in order to combat this issue. Despite this, this initiative may be hampered because Indonesia is not yet a permanent member of the FATF. As a result, the country is forced to rely on bilateral cooperation and Mutual Legal Assistance (MLS) with other nations.

CONCLUSSION

Cryptocurrencies enable users to exercise control over their assets in a manner that is either entirely decentralised or completely new. Blockchain systems and cryptocurrencies present a continuing challenge for law enforcement, particularly in the AML regime. This is forcing all parties to reconsider the idea of how the focus of law enforcement and legislators should be on continually

adapting to new technologies. Blockchain systems and cryptocurrencies are also a growing concern for regulators. One of the important factors contributing to success is the existence of electronic evidence in law enforcement efforts and the elimination of money laundering through the use of cryptocurrencies. However, electronic evidence is not regulated in a (formal) criminal procedural law. This is in contrast to the United States of America and the United Kingdom, which regulate this situation in their criminal procedural law, particularly concerning preventing crypto money laundering through regulations. Both the United States and the United Kingdom have developed standard guidelines for collecting and submitting electronic evidence. These guidelines ensure that issues about electronic evidence's authenticity, validity, and integrity are more reliably addressed, thereby increasing the likelihood that such evidence will be widely accepted in court.

According to the study's conclusions, electronic evidence is an important instrument that may be utilised in the battle against money laundering. Nevertheless, the quality of the AML regime that is now in place will determine how effective it is. Both the United Kingdom and the United States have shown that a comprehensive anti-money laundering framework backed by highly advanced electronic monitoring technologies can produce excellent results in the fight against money laundering. In contrast, the scant use of electronic evidence in Indonesia implies that the country has not yet developed a solid AML regime capable of effectively combating money laundering.

The study findings have several important consequences for scholars and policymakers. To begin, the decision-makers in Indonesia should think about bolstering the country's anti-money-laundering (AML) framework by extending its purview beyond the confines of the banking industry and creating more efficient procedures for collecting and analysing electronic data. Second, governments in the United Kingdom and the United States should continue to invest in the creation of advanced electronic monitoring systems capable of keeping up with technological and financial innovation improvements.

The study's findings also point in various directions that could be explored in further research. The efficiency of anti-money-laundering (AML) regimes in many parts of the economy is an essential topic that requires additional research. According to the study, the United Kingdom and the United States have developed comprehensive AML frameworks encompassing various financial operations, such as banking, securities dealing, and insurance. On the other hand, it is unclear whether these frameworks are equally effective in all areas of the economy. There is a need for additional research to evaluate whether or not AML regulations that are particular to a sector would be more effective in detecting and preventing money laundering.

Another subject worthy of further investigation is the role that international collaboration plays in the battle against the laundering of illicit funds. According to the study, one of the most significant flaws in AML regimes is a lack of coordination and cooperation across government entities. More research is required to understand which procedures are the most effective in fostering international collaboration and the exchange of information between nations.

Even though the study contributes to the existing body of literature on electronic evidence and AML regimes, it is important to note that the research has several limitations that should be considered. The research has several flaws, but one of them is that the scope of the study is too narrow. The scope of the study is limited to just three countries, and it is possible that the findings cannot be extrapolated to other nations due to differences in their regulatory frameworks, legal systems, and cultural norms. To provide a more in-depth understanding of electronic evidence's role in the fight against money laundering worldwide, the researchers should broaden the scope of the study to encompass a greater number of nations and regions.

Another shortcoming of the investigation is that it only uses a limited number of data sources. In order to analyse how anti-money laundering policies use electronic evidence, the majority of the research in this study draws on secondary sources such as reports and academic literature. Even while these sources are helpful, it is possible that they may not provide a comprehensive picture of how electronic evidence is used on the ground. For researchers to provide a more nuanced understanding of electronic evidence in anti-money laundering operations, primary data sources, such as interviews with law enforcement authorities and financial institution representatives, should be incorporated into their studies.

The third flaw in the research is that it did not consider the ethical implications of using electronic evidence to combat money laundering. The ethical issues that must be considered when using electronic evidence to investigate and prosecute money laundering offences are not addressed in the study because its primary focus is on the legal and regulatory frameworks that govern the gathering and use of electronic evidence. The researchers' analyses should incorporate ethical considerations, such as the potential influence on individual privacy rights, civil liberties, and due process.

The research suffers from several flaws, one of which is that it does not consider the difficulties connected with the utilisation of electronic evidence in international probes. Electronic evidence in one jurisdiction may be subject to different legal and regulatory frameworks than in another since money laundering offences sometimes involve numerous jurisdictions. Researchers need to

investigate the difficulties related to the use of electronic evidence in international investigations and develop solutions for overcoming these difficulties.

The fifth shortcoming of the research is a limited assessment of the potential biases connected with the use of electronic evidence in efforts to combat money laundering. The accuracy and reliability of the evidence may be compromised due to biases present in electronic evidence. These flaws include cognitive bias and confirmation bias, among others. Researchers need to investigate the possibility of biases being introduced by using electronic evidence and develop techniques to reduce the impact of these biases.

REFERENCES

AKBAR, D. L. (2019). Criminal Law Policy in Handling Digital Asset-Based Money Laundering in Indonesia. *Journal of Law and Legal Reform*, *1*(1), 129–176. https://doi.org/10.15294/jllr.v1i1.35543

AKHTAR, M., & FENG, T. (2022). Using Blockchain to Ensure the Integrity of Digital Forensic Evidence in an IoT Environment. *EAI Endorsed Transactions on Creative Technologies*, 174089. https://doi.org/10.4108/eai.3-6-2022.174089

ALAMMARY, A., ALHAZMI, S., ALMASRI, M., & GILLANI, S. (2019). Blockchain-Based Applications in Education: A Systematic Review. *Applied Sciences*, *9*(12), 2400. https://doi.org/10.3390/app9122400

ALKADRI, S. (2018). Defining and Regulating Cryptocurrency: Fake Internet Money or Legitimate Medium of Exchange? *Duke Law & Technology Review*, *17*(1), 71–98.

ANTHONY DAS, C., PRASAD, K., & SADIQUE, M. S. (2018). Cryptocurrency a Bit Unregulated? *International Conference on Business and Banking V (ICBB V)*. https://doi.org/10.2139/ssrn.3298609

BAINS, P., ISMAIL, A., MELO, F., & SUGIMOTO, N. (2022). Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets. *FinTech Notes*, *2022*(007). https://www.imf.org/en/Publications/fintech-notes/Issues/2022/09/26/Regulating-the-Crypto-Ecosystem-The-Case-of-Unbacked-Crypto-Assets-523715

BHAT, P. I. (2015). Comparative Method of Legal Research: Nature, Process and Potentiality. *Journal of the Indian Law Institute*, *57*(2), 147–173. JSTOR.

CALAFOS, M. W., & DIMITOGLOU, G. (2023). Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency. In K. DAIMI, I. DIONYSIOU, & N. EL MADHOUN (Eds.), *Principles and Practice of Blockchains* (pp. 271–300). Springer International Publishing. https://doi.org/10.1007/978-3-031-10507-4_12

CAMPBELL-VERDUYN, M. (2018). Bitcoin, Crypto-Coins, and Global Anti-Money Laundering Governance. *Crime, Law and Social Change*, *69*(2), 283–305. https://doi.org/10.1007/s10611-017-9756-5

CHAWKI, M. (2022). Cybercrime and the Regulation of Cryptocurrencies. In K. Arai (Ed.), *Advances in Information and Communication* (pp. 694–713). Springer International Publishing.

COELHO, R., FISHMAN, J., & OCAMPO, D. G. (2021). *Supervising Cryptoassets for Anti-Money Laundering*. Bank for International Settlements, Financial Stability Institute.

DE HARO-OLMO, F. J., VARELA-VACA, Á. J., & ÁLVAREZ-BERMEJO, J. A. (2020). Blockchain from the Perspective of Privacy and Anonymisation: A Systematic Literature Review. *Sensors*, *20*(24), 7171. https://doi.org/10.3390/s20247171

DEWAAL, G., & DEMPSEY, G. (2015). New York BitLicense regulations virtually certain to significantly impact transactions in virtual currencies. *Journal of Investment Compliance*, *16*(4), 59–65. https://doi.org/10.1108/JOIC-08-2015-0047

DUMCHIKOV, M., REZNIK, O., & BONDARENKO, O. (2023). Peculiarities of Countering Legalization of Criminal Income with the Help of Virtual Assets: Legislative Regulation and Practical Implementation. *Journal of Money Laundering Control*, *26*(1), 50–59. https://doi.org/10.1108/JMLC-12-2021-0135

DUPUIS, D., SMITH, D., & GLEASON, K. (2023). Old Frauds with a New Sauce: Digital Assets and Space Transition. *Journal of Financial Crime*, *30*(1), 205–220. https://doi.org/10.1108/JFC-11-2021-0242

ELIZONDO, D. A., SOLANAS, A., & MARTINEZ-BALLESTE, A. (2012). *Computational Intelligence for Privacy and Security*. Springer Berlin Heidelberg.

FLETCHER, E., LARKIN, C., & CORBET, S. (2021). Countering Money Laundering and Terrorist Financing: A Case for Bitcoin Regulation. *Research in International Business and Finance*, *56*, 101387. https://doi.org/10.1016/j.ribaf.2021.101387

FUJIWARA, B. (2023). *A study on Non-Performing Assets Cases and Cryptocurrency in Japan* (arXiv:2302.07619). arXiv. http://arxiv.org/abs/2302.07619

GARCIA-TERUEL, R. M., & SIMÓN-MORENO, H. (2021). The Digital Tokenization of Property Rights. A Comparative Perspective. *Computer Law & Security Review*, *41*, 105543. https://doi.org/10.1016/j.clsr.2021.105543

GELEMEROVA, L. (2009). On the Frontline Against Money-Laundering: The Regulatory Minefield. *Crime, Law and Social Change*, *52*(1), 33–55. https://doi.org/10.1007/s10611-008-9175-8

GOLDBARSHT, D., & de Koker, L. (2022). *Financial Technology and the Law: Combating Financial Crime*. Springer International Publishing.

HABIB, G., SHARMA, S., IBRAHIM, S., AHMAD, I., QURESHI, S., & ISHFAQ, M. (2022). Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing. *Future Internet*, *14*(11), 341. https://doi.org/10.3390/fi14110341

HM TREASURY. (2015). *UK National Risk Assessment of Money Laundering and Terrorist Financing*. HM Treasury and Home Office,. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Ml-tf-risks.html

JONES, N., GEORGE, E., MERIDA, F., RAMUSSEN, U., & VOLZOW, V. (2020). *Electronic Evidence Guide-A Basic Guide for Police Officers, Prosecutors, and Judges*. Cybercrime Division Directorate General of Human Rights and Rule of Law. https://rm.coe.int/c-proc-electronic-evidence-guide-2-1-en-june-2020-web2/16809ed4b4

KARAGIANNIS, C., & VERGIDIS, K. (2021). Digital Evidence and Cloud Forensics: Contemporary Legal Challenges and the Power of Disposal. *Information*, *12*(5), 181. https://doi.org/10.3390/info12050181

KHAN, A. S., SUMAILA, U. R., WATSON, R., MUNRO, G., & PAULY, D. (2006). The nature and magnitude of global non-fuel fisheries subsidies. In *Fisheries Centre research reports*. Fisheries Centre, University of British Columbia.

LEVI, M., & GILMORE, W. (2002). Terrorist Finance, Money Laundering and the Rise and Rise of Mutual Evaluation: A New Paradigm for Crime Control? In M. PIETH (Ed.), *Financing Terrorism* (pp. 87–114). Springer Netherlands. https://doi.org/10.1007/0-306-48044-1_6

MANSHUR, M., RODLIYAH, R., & AMIRUDDIN, A. (2019). Analysis of Electronic Evidence as an Evidence Tools in Criminal Case Post Decision of Constitutional Court Number: 20/PUU-XVI/2016. *International Journal of Multicultural and Multireligious Understanding*, *6*(2), 770–783. https://doi.org/10.18415/ijmmu.v6i2.819

MASON, S., & SENG, D. (Eds.). (2017). *Electronic Evidence*. University of London Press; JSTOR. http://www.jstor.org/stable/j.ctv512x65

MOHAMAD, A. M. (2019). Admissibility and Authenticity of Electronic Evidence in the Courts of Malaysia and United Kingdom. *International*

Journal of Law Government and Communication, *4*(15), 121–129. https://doi.org/10.35631/ijlgc.4150013

MONTASARI, R. (2016). Digital Evidence: Disclosure and Admissibility in the United Kingdom Jurisdiction. In H. JAHANKHANI, A. CARLILE, D. EMM, A. HOSSEINIAN-FAR, G. BROWN, G. SEXTON, & A. JAMAL (Eds.), *Global Security, Safety and Sustainability—The Security Challenges of the Connected World* (pp. 42–52). Springer International Publishing.

MOUSSA, A. F. (2021). Electronic Evidence and Its Authenticity in Forensic Evidence. *Egyptian Journal of Forensic Sciences*, *11*(1), 20. https://doi.org/10.1186/s41935-021-00234-6

MUTTAQIM, M., & APRILIANI, D. (2019). Analysis of The Probability of Money Laundering Crimes toward the Development of Crypto-currency Regulations in Indonesia. *IJCLS (Indonesian Journal of Criminal Law Studies)*, *4*(1), 29–40. https://doi.org/10.15294/ijcls.v4i1.18714

OTHMAN, A. H. A., ALHABSHI, S. M., KASSIM, S., & SHAROFIDDIN, A. (2020). The Impact of Cryptocurrencies Market Development on Banks' Deposits Variability in the GCC Region. *Journal of Financial Economic Policy*, *12*(2), 161–184. https://doi.org/10.1108/JFEP-02-2019-0036

PARTIDA, A., GERASSIS, S., CRIADO, R., ROMANCE, M., GIRÁLDEZ, E., & TABOADA, J. (2022). Modeling Bitcoin plus Ethereum as an Open System of Systems of Public Blockchains to Improve Their Resilience against Intentional Risk. *Electronics*, *11*(2), 241. https://doi.org/10.3390/electronics11020241

PETERS, G. W., PANAYI, E., & CHAPELLE, A. (2015). Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective. *CoRR*, *abs/1508.04364*. https://doi.org/10.48550/arXiv.1508.04364

PETERS, R. J., LOY, A. D., OSTEEN, M., REMY, J., & FITZSIMMONS, J. (2021). Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data. *Mitchell Hamline Law Review*, *47*(3), 1072–1128.

PUTRA, S. E., & PUTRANTO, R. D. (2022). Legal Analysis of the Crime of Money Laundering Through Cryptocurrencies. *Jurnal Hukum Sehasen*, *8*(2), 135–140. https://doi.org/10.37676/jhs.v8i2.3101

READ, C. L. (2022). No More Duffel Bags Full of Cash. In C. L. Read (Ed.), *The Bitcoin Dilemma: Weighing the Economic and Environmental Costs and Benefits* (pp. 113–119). Springer International Publishing. https://doi.org/10.1007/978-3-031-09138-4_11

REEDY, P. (2023). Interpol Review of Digital Evidence for 2019–2022. *Forensic Science International: Synergy*, *6*, 100313. https://doi.org/10.1016/j.fsisyn.2022.100313

REYNOLDS, P., & IRWIN, A. S. M. (2017). Tracking Digital Footprints: Anonymity Within the Bitcoin System. *Journal of Money Laundering Control*, *20*(2), 172–189. https://doi.org/10.1108/JMLC-07-2016-0027

ROVITA, A., & IMANULLAH, M. N. (2018). Electronic Money as a Legal Payment Instrument in Indonesia. *South East Asia Journal of Contemporary Business, Economics and Law*, *15*(5), 207–213.

SANTOSO, W. Y., PUTRA, A. A., PASSAGI, J. H., HANINDYA, Y. R., & TAGAR, A. A. (2019). Governing Blockchain-Based Token in Indonesia: Legal and Technical Perspective. *Brawijaya Law Journal: Journal of Legal Studies*, *7*(1), 108–128. https://doi.org/10.21776/ub.blj.2020.007.01.08

SANZ-BAS, D., DEL ROSAL, C., NÁÑEZ ALONSO, S. L., & ECHARTE FERNÁNDEZ, M. Á. (2021). Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain. *Laws*, *10*(3), 57. https://doi.org/10.3390/laws10030057

SARUNGU, C. M. (2020). Digital Lending High Level System Architecture in Indonesia. *2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE)*, 159–164. https://doi.org/10.1109/ICITAMEE50454.2020.9398429

SHARMA, A. M. (2020). *Cryptocurrency and Financial Risks* [PhD Thesis]. Liberty University.

SIREGAR, F. R., & SITORUS, N. T. (2022). Analisis Hukum Terhadap Pertimbangan Hakim Atas Vonis Nihil Kepada Pelaku Tindak Pidana Korupsi. *Jurnal Ilmiah Penegakan Hukum*, *9*(2), 200–206. https://doi.org/10.31289/jiph.v9i2.7076

STANFIELD, A. R. (2016). *The Authentication of Electronic Evidence* [PhD Thesis]. Queensland University of Technology.

SUKARNO, K. S. & PUJIYONO. (2020). The Use of Cryptocurrency as a Payment Instrument. *Proceedings of the 3rd International Conference on Law and Governance (ICLAVE 2019)*, 366–370. https://doi.org/10.2991/aebmr.k.200321.048

TAN, B. S., & LOW, K. Y. (2017). Bitcoin – Its Economics for Financial Reporting. *Australian Accounting Review*, *27*(2), 220–227. https://doi.org/10.1111/auar.12167

TRISAKTI, A., & SOPONYONO, E. (2021). Upaya Pencegahan Tindak Pidana Pencucian Uang Dalam Bentuk Uang Kripto (Bitcoin) Menggunakan Prinsip Kehati-Hatian Perbankan. *Jurnal Belo*, *7*(1), 37–54. https://doi.org/10.30598/belovol7issue1page37-54

WANG, S., & ZHU, X. (2021). Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing. *Policing: A Journal of Policy and Practice*, *15*(4), 2329–2340. https://doi.org/10.1093/police/paab059

WARDHANA, A. T., & NUGROHO, B. W. (2021). Abuse of Cryptocurrency to Funding International Terrorism Activities. *Proceedings University of Muhammadiyah Yogyakarta Undergraduate Conference*, *1*(1), 353–362.

WERBACH, K. (2018). Trust, but Verify. *Berkeley Technology Law Journal*, *33*(2), 487–550. JSTOR.

WIDHIYANTI, H. N., HUSSEIN, S. M., & GANINDHA, R. (2023). Indonesian Cryptocurrencies Legislative Readiness: Lessons from the United States. *Sriwijaya Law Review*, *7*(1), 150–172. https://doi.org/10.28946/slrev.Vol7.Iss1.2138.pp150-172

ZHOU, L., QIN, K., & GERVAIS, A. (2021). A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges. *CoRR*, *abs/2106.07371*. https://doi.org/10.48550/arXiv.2106.07371

ZWITTER, A., & GSTREIN, O. J. (Eds.). (2021). *Identity and Privacy Governance*. Frontiers Media SA. https://doi.org/10.3389/978-2-88971-413-1

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET