ISSN Print: 2707-1499 Online: 2707-1502
Advance in Law − 2025, 7(4)
https://doi.org/10.35534/al.0704026

Anti-Money Laundering Regulation: Strategies and Challenges of Australia and the United States in Digital Currency Legal Responses

Lei Wang

The University of New South Wales, Sydney, Australia

Abstract: With the rapid popularity of digital assets and the continuous expansion of the virtual currency market, traditional anti-money laundering (AML) regulatory methods and means are completely insufficient to deal with current problems. Regulatory mechanisms play a key role in disrupting criminal networks operating through digital means, so responses must be accelerated, and the development of anti-money laundering-related technologies must be accelerated. As a leading country in the field of global financial regulatory innovation, the United States' existing regulatory framework for digital assets and virtual currencies has continued to improve in recent years. In terms of the regulatory framework, we have achieved good results in various aspects. This article aims to compare the implementation of anti-money laundering supervision in Australia and the United States and explore how Australia, as a country, can use advanced technology and modify the regulatory framework to deal with the challenges posed by digital assets according to its conditions. In addition, because money laundering crimes have cross-border characteristics, we must also pay attention to the role of international cooperation in anti-money laundering law enforcement.

Keywords: Anti-Money Laundering; Cryptocurrency Regulation; Blockchain Analytics; Digital Assets; Financial Crime Enforcement

1 Introduction

The rapid growth of digital assets and virtual currencies has exposed gaps in traditional anti-money laundering regulatory frameworks. In this article, I employ a comparative analysis to compare anti-money laundering enforcement in Australia and the United States, focusing on the challenges posed by cryptocurrencies and decentralized finance. Key issues in anti-money laundering enforcement are analyzed, including gaps in virtual currency regulation, the use of blockchain analysis and machine learning for transaction monitoring, and the role of international cooperation in combating cross-border money laundering.

This comparison reveals that while both countries have established relatively comprehensive anti-money laundering legal frameworks, the United States has made greater progress in updating its legislation, continuously improving

Article Citation: Wang, L. (2025). Anti-Money Laundering Regulation: Strategies and Challenges of Australia and the United States in Digital Currency Legal Responses. Advance in Law, 7(4), 283-294.

transparency and strengthening penalties. In line with technological advancements, the United States has also integrated emerging technologies into its regulatory framework, adopting beneficial ownership registries and whistleblower incentives.

Despite strong laws, Australia still faces significant challenges in regulatory adaptability, technological lags, and cross-border enforcement. Therefore, this article proposes that, in order to enhance the effectiveness of anti-money laundering in today's evolving digital asset landscape, Australia should adopt a stricter regulatory regime and clarify the role of the Securities and Investments Commission in digital currency regulation. It should also accelerate technological advancement, adopt innovative data acquisition methods, and strengthen blockchain- and AI-driven monitoring. On the premise of protecting financial privacy rights, Australia should focus on strengthening cross-border cooperation.

2 Digital Assets: Spawning New Anti-Money Laundering Regulatory Enforcement Models

2.1 The Transformation of Digital Assets

Digital assets, also known as digital currencies, are virtual currencies that represent value digitally and can be used to trade goods and services or hold wealth. The utilization of digital assets has experienced substantial growth in recent years. Traditional approaches to conducting cross-border transactions are frequently slow, expensive, and not easily accessible. On the other hand, digital assets allow for nearly instant transfers at lower expenses, which makes them an attractive option for individuals and businesses engaged in global commerce and financial transfers. (Goldbarsht, 2023) Because digital currencies provide an online medium of exchange, their fast cross-border transfers and lack of globally coordinated supervision make them a powerful tool for money laundering. The darknet allows users to browse anonymously, attracting crypto-anarchists who seek to evade financial reporting requirements. Numerous instances of drug trafficking cases have been documented, which include the movement of funds into Bitcoin accounts and subsequently to websites. The accused in the case of R v Collopy acquired narcotics from the dark web and subsequently utilized Bitcoin for financial transactions, aiming to conceal the proceeds through money laundering. As a result, Bitcoin has become increasingly prevalent in cases involving drug trafficking, distribution of illicit funds, and conspiracy to distribute controlled substances (Latimer & Duffy, 2019).

And the scale of the proliferation of cryptocurrencies is staggering. Bitcoin's market value will reach $385 billion in 2022. The rise in popularity of digital assets has led to the emergence of a new version of the Internet, known as Web3. Transactions in Web3 are carried out through a linear chain on the blockchain. In this system, users can conduct transactions without revealing their identity, as the blockchain provides only pseudo-anonymous information and publicly verifies transactions. The program's rapid growth in the financial sector has also provided multiple avenues for criminal activity. According to 2023 data, the proportion of confiscated assets relative to total criminal proceeds is less than 1% globally. In the first half of 2022, more than $2 billion was stolen from Web3 projects due to phishing scams, Ponzi schemes, brushing, and DApp attacks. (Goldbarsht, 2023) Criminals employ strategies for money laundering to conceal and transform stolen assets using different methods, intending to make them seem lawful.

2.2 The New Challenges Cryptocurrencies Pose to Regulation

In traditional financial systems, banks and other financial institutions serve as central authorities responsible for recording and verifying transactions, subject to specific AML regulations. Transaction records are stored centrally to ensure the legality of capital flows. This system allows regulators to monitor and investigate suspicious activity. But due to the decentralized nature of the cryptocurrency and DeFi fields. Based on cryptography, there is no central authority to regulate or verify transactions and ensure their security and anonymity. This offers enhanced privacy protection, enabling individuals to partake in a range of financial activities such as borrowing and earning interest without relying on conventional financial intermediaries. People lacking access to traditional banking services only require a smartphone and internet connection to take part in the global financial system, trading, saving, and investing in digital assets while bypassing traditional intermediaries. (Goldbarsht, 2023)

Although encryption technology itself has many positive application values, it also brings huge challenges to AML supervision. Excessive anonymity makes it difficult for AML to monitor and verify all transaction activities, and the technology is very likely to be used to hide the source and whereabouts of illegal funds, providing convenience for criminal activities such as money laundering. As the Web3 ecosystem grows, various blockchain-related security issues have also increased significantly. (Goldbarsht, 2023) The emergence of crypto-assets, blockchain technology, and decentralized finance platforms has led to a notable surge in the quantity and intricacy of transactions requiring examination. As a result, manual review processes and outdated rules-based standards are not enough to ensure effective enforcement of anti-money laundering measures. Despite efforts for international coordination and adherence to FATF guidelines, the regulators' insufficient identification and tracking, as well as the legislators' slow response, have limited the effectiveness of confiscating criminal assets. In this changing environment, traditional approaches to confiscation and anti-money laundering are not sufficient.

2.3 Exploiting Regulatory Loopholes in Virtual Currencies for Money Laundering Crimes

As technology advances rapidly, especially in the emerging field of virtual currencies, criminals are quickly adapting and exploiting these technologies to conduct money laundering activities. They find and exploit under-regulated loopholes or regulatory gaps in the cryptocurrency space to circumvent the scrutiny of traditional regulatory and law enforcement agencies.

For example, a money laundering method called "Chain Hopping"(Goldbarsht, 2023). Criminals often use complex obfuscation techniques to conduct complex trading operations on cryptocurrencies to evade regulatory and law enforcement scrutiny. Conduct rapid and multiple transfers within a short period between multiple cryptocurrency accounts under their control, disrupt transaction trails to obfuscate the source of assets, and hide the flow of funds, making it more difficult to trace the original flow of funds. Other strategies include using mixing services, also known as "coin mixers," which pool assets into a unified pool and implement multiple transactions that are layered, bundled, and mixed. Cryptocurrency assets of multiple users are pooled together and then redistributed. In this way, the original asset is split and mixed with multiple other transactions before being returned to the user. The purpose of this is to disrupt the chain of tracking of the funds, thus masking the source and destination of the funds.

2.3 The Application of Emerging Regulatory Technologies and Their Controversies

Blockchain analysis is an application related to cybercrime investigations and can also serve as an important

tool to help law enforcement agencies detect and track illegal activities. Conducting blockchain analysis requires domain-specific expertise and substantial computing resources. Blockchain data analysis often involves very complex data processing. Machine learning is a key technology in blockchain analysis. It is a branch of artificial intelligence. Algorithms can automatically identify patterns in data, make predictions based on these patterns, and identify patterns and anomalies in data. (Goldbarsht, 2023)

In the field of machine learning, algorithm training requires a large amount of data to improve the accuracy of imitation and prediction. Through analysis, machine learning models can identify specific wallet addresses and track transaction flow interactions between addresses. And the ability to perform extensive advanced analytics, segment transactions, define data scopes, and tag addresses. (Goldbarsht, 2023) Improve the accuracy of suspicious matter reporting by analyzing large amounts of data to identify transactions that match known money laundering patterns or discover new suspicious patterns. By reducing reliance on manual experts to review each transaction, financial institutions can more effectively monitor trading activity, improve the quality of information submitted to regulatory and law enforcement agencies, and ensure that the reports received by regulatory and law enforcement agencies are more reliable.

But machine learning technology has also been subject to some controversy, first of all, because its limited parameter capacity leads to poor performance in detecting complex human money laundering behavior patterns. If criminals' behavior changes or they adopt new money laundering strategies, current machine learning models may not be able to effectively identify and predict these activities. Secondly, obtaining enough real transaction data is crucial for the algorithm to accurately learn and identify suspicious transaction patterns. However, when financial institutions develop and train machine learning algorithms for money laundering detection, there is a lack of access to a large amount of real transaction data. Because real data is difficult to obtain, financial institutions may instead rely on synthetic (simulated) data. (Goldbarsht, 2023)

3 In-Depth Analysis of Australia's AML Regulatory Enforcement Methods

3.1 Overview of Major Legal Frameworks Related to AML in Australia

3.1.1 Anti-Money Laundering and Counter-Terrorism Financing Law (AML/CTF Law)

In Australia, the current AML regime is mainly stipulated in the AML/CTF Act, a major part of domestic legislation. The bill provides for specific regulation of industries that provide services that may be used to affect money laundering and terrorist financing. The new AML/CTF law explicitly brings within the scope of regulation for the first time providers of monetary services, including providers of services for trading cryptocurrencies such as Bitcoin. At the same time, the main focus is on transactions between virtual assets and legal currencies that may be involved in money laundering activities (Chawki, 2022). Legitimate users may use virtual assets for normal business transactions or fund storage. Still, criminal organizations may also use virtual assets to engage in illegal activities, such as money laundering or fund transfers. Whether legitimate users or criminals need to convert their virtual assets into legal currency, they must interact with qualified service agencies. When digital currency exchanges operate in Australia, they must register with the Australian Transaction Reports and Analysis Center (AUSTRAC) to ensure that the business complies with the

country's anti-money laundering and counter-terrorist financing (AML/CTF) legal framework. Not only are exchanges required to report all transactions over A$10,000, they are also required to actively monitor and promptly report any suspicious activity that may indicate money laundering. (Schmidt, 2021)

Exchanges must also take steps to verify customer identities, ensure the accuracy of customer information, and conduct continuous monitoring of customer activities to prevent customers from engaging in illegal conduct and enable rapid investigation after engaging in illegal conduct. They are also required to submit suspicious transaction reports and cash transaction reports to AUSTRAC to meet regulatory requirements. (Schmidt, 2021)

3.1.2 Proceeds of Crime Act 2002

The Proceeds of Crime Act provides Australia with a set of regulatory tools and procedures to address money laundering and asset confiscation, providing the most fundamental basis and direction for supervision. POCA provides that crime proceeds agencies, such as the Australian Federal Police Commissioner or the Commonwealth Prosecutor, can apply to the High Court to freeze, restrict, or confiscate assets that are directly or indirectly derived from or used in criminal activities. A person's property can be restricted when it is suspected that it is the proceeds of an indictable offence. The regulator has the option to seek a confiscation order based on non-conviction through the civil courts. Cryptocurrencies such as Bitcoin, Ethereum, Tether, Dogecoin, and Ripple are subject to confiscation under POCA. The court could issue a series of ancillary orders that would allow the official trustee to take control of a crypto 'wallet' and transfer any cryptocurrency in that wallet to its account. (Goldbarsht, 2023) And the court can hear and approve applications under POCA ex parte in a closed court or behind closed doors. In addition, POCA also provides for inspection orders and production orders when the disposal or trading of property violates the restraining order. Suppose such a disposal or transaction does not receive sufficient consideration or is not carried out in the capacity of a bona fide person. In that case, the court has the power to revoke the disposal or transaction. In the event of collaborative inquiries, results can be exchanged with states and territories. Upon receiving a request from another country, Australia has the authority to detect, immobilize, confiscate, or seize the profits or tools related to a foreign major offense.

POCA also introduces the unexplained wealth order, which reverses the burden of proof and requires individuals to prove the lawful source of their wealth, while defining 'proceeds of crime' and 'instruments of crime'. It is clarified that even after the property is transferred or exchanged, the property is still regarded as the proceeds of crime or the instrument of crime, except in other circumstances, such as when the property is acquired or inherited by a bona fide third party. (Goldbarsht, 2023)

3.2 Challenges Faced by Australia's AML Regulation

3.2.1 The Lag in Regulatory Technology

Digital currencies appear to be particularly well-suited for money laundering and terrorist financing, allowing large amounts of money to be raised and moved around the world in a short period (Latimer & Duffy, 2019). When digital currencies involve centralized intermediaries, such as cryptocurrency exchanges, they can theoretically be effectively managed by applying existing financial regulations to these intermediaries. However, virtual assets are not limited to transfers through intermediaries in the global financial system, and their peer-to-peer (P2P) nature brings additional risks. Peer-to-peer transactions are essentially conducted directly between individuals, without a centralized intermediary to monitor or control transactions. This kind of transaction risk is still difficult to manage through financial

surveillance. Although it may not be a high risk currently, it may quickly evolve into a high risk. (Schmidt, 2021)

However, regulatory technology is currently lagging, although Australia's existing regulatory approach is aware of the current risks. To follow the development and changes in technology, we want to try to apply a technology-neutral approach to solve current problems and design rules based on regulatory purposes and risks. However, this approach focuses on issues and risks rather than on specific technologies.

3.2.2 The Inadaptability of the Regulatory Framework

As virtual assets gain mainstream adoption, more people are using virtual assets directly without exchanging them for fiat currency. This trend will reduce transactions between virtual assets and fiat currencies, thereby reducing the opportunities for regulators to monitor and control the flow of virtual assets. Moreover, virtual assets have developed rapidly and erratically since their birth. The regulatory framework must be able to adapt to such rapid changes, which will also lead to intensified regulatory challenges (Schmidt, 2021). The virtual asset market has increased in size and complexity, but regulatory measures have not been adjusted accordingly. The current regulation of virtual assets under the AML/CTF Act leaves significant risks, and simply strengthening the enforcement of existing regulations is not an effective solution. There are problems with some regulations, such as the ban or payment limit measures proposed for physical cash. The Australian government once considered implementing a bill that would limit cash payments in economic activities to A$10,000, although it has cracked down on black market economic activities. However, doing so will limit investment and innovation opportunities related to virtual assets, and the net benefits virtual assets provide in terms of investment and innovation should not be ignored.

Additionally, although Bitcoin users can transact anonymously via private keys, all cryptocurrency transactions are recorded on the blockchain. This provides regulators with a potential surveillance and audit tool, but also raises concerns about the erosion of the concept of financial privacy (Hossain, 2023).

3.2.3 The Role of Australian Regulatory Authorities and Their Uncertainty

There is uncertainty about the role of the Australian Securities and Investments Commission. Digital currency may potentially be subject to regulation by ASIC in Australia, as it could be considered a financial product under section 763A of the Corporations Act, serving as a means to create non-financial products. However, this interpretation is currently uncertain and has not been tested in court. In addition to ASIC, various regulatory authorities in Australia may also be involved in supervision related to digital currency operations, such as the ACCC, Reserve Bank of Australia, ATO, and AUSTRAC. It can be seen that the supervision of this emerging field is very complex, and cooperation with multiple agencies is necessary. (Latimer & Duffy, 2019)

The Australian Financial Complaints Authority (AFCA) and the Australian Bankers Association are both involved in the regulation and standards of practice for digital currencies. The Australian Bankers Association has set up the Banking Code of Practice to standardize the relationship between banks and customers and the quality of services. (Latimer & Duffy, 2019) If hackers are organizing crimes, the use of digital currencies provides them with a very convenient way. Suppose a digital currency platform or transaction is suspected of criminal activities, such as money laundering, misappropriation of funds, or unknown sources of funds. In that case, the federal police will investigate and enforce the law. In the face of security threats such as hacker attacks and organized crime, it also has corresponding law enforcement mechanisms and capabilities.

4 In-Depth Analysis of the U.S. AML Regulatory Enforcement Methods

4.1 Regulatory Framework and Legal Foundations

Since the "USA Patriot Act" in 2001, the United States has continuously introduced AML laws, and the "Anti-Money Laundering Act of 2020" AMLA introduced amendments and enhancements to AML/CFT. This update is the largest legislative update in the area of anti-money laundering and counter-terrorist financing in the United States since the Patriot Act. In addition to amending and strengthening some provisions in the existing law, the legislative update has the purpose of introducing new tools and technologies. Improve capabilities to monitor, detect, and combat financial crime and ensure adequate resources and technical support to meet challenges. The bill strengthens the ability of U.S. regulators to combat money laundering, terrorist financing, and other financial crimes. By ensuring that regulators better understand and monitor corporate ownership structures, they can identify and disrupt the flow of illicit funds. (Hausfeld et al., 2021) The new CTA and AMLA became effective on January 1, 2021, as part of the 2021 National Defense Authorization Act.

In addition to expanding and updating the Bank Secrecy Act and the federal AML/CTF regime. The CTA and AMLA also formalized existing FinCEN guidance related to digital assets. Amend the Bank Secrecy Act to include "substitute currency values."(Hossain, 2023) Reaffirms FinCEN's authority over digital assets, and stipulates that exchanges of such assets must register with FinCEN. It also mandates that transactions involving certain types of digital assets must be reported and recorded.

4.2 Eight Major Measures of AMLA Reforms Worth Discussing

On January 1, 2021, Congress passed the National Defense Authorization Act (NDAA), a comprehensive statute covering various defense and security matters and addressing a variety of defense and national security issues. Through annual adoption, it provides authorization and guidance for U.S. Department of Defense policies, programs, and activities. There is much to discuss about this latest reform.

(1) The first is to establish a non-public registration agency that tracks actual beneficiaries, improves the transparency of corporate ownership, helps regulatory agencies identify and prevent money laundering and terrorist financing risks, and enables law enforcement agencies to more effectively track and prevent the flow of illegal funds (Hausfeld et al., 2021). The AMLA mandates specific companies or entities to disclose their beneficial owners' details to the Treasury Department's Financial Crimes Enforcement Network (FinCEN). Failure to report or provide false information can result in civil fines, criminal penalties, and potential imprisonment. Unauthorized disclosure or use of beneficial ownership information also carries severe civil and criminal consequences.

(2) The second is the Whistleblower Rewards Program. Reporting is encouraged to report activities that may involve anti-money laundering, and the whistleblower can receive a 30% bonus of the total amount. At the same time, the law provides that the whistleblower is protected from any form of retaliation and can file relevant lawsuits if it occurs. Courts can impose fines and compensate the whistleblower while requiring the company to reinstate them and prohibit employers from retaliating or discriminating against employees who report suspected anti-money laundering violations. If there is any salary owed to the whistleblower, double compensation will be required, and interest will also be added. The relevant employer will also be responsible for the final litigation costs and attorney's fees. (Hausfeld et

al., 2021)

(3) It also strengthens the ability to supervise international money laundering and terrorist financing activities by allowing U.S. regulators to request documents from foreign financial institutions related to investigations within the United States (Hausfeld et al., 2021). Foreign financial institutions are banks and other financial service providers that operate outside the United States but have transactions or connections with the U.S. financial system.

(4) The modernization of the system is worth learning from Australia. AMLA incorporates emerging financial technologies into the regulatory framework and expands the definition of financial institutions and money transmission businesses under the Bank Secrecy Act (BSA). Includes entities that provide services involving 'alternative monetary value', such as stored value and virtual currency instruments (such as cryptocurrencies). (Hausfeld et al., 2021) The emergence of emerging financial products and services requires accelerating adaptation, updating existing AML/CFT rules, investing more resources and developing new tools to overcome the challenges posed by the traditional AML/CFT framework. Recognizing the potential money laundering risks associated with non-traditional financial activities, antiquities dealers, advisers, and advisors have also been added to the definition of "financial institution" subject to the BSA and FinCEN customer due diligence rules. AMLA requires FinCEN to establish streamlined processes, including automated processes, for reporting certain non-complex suspicious activity reports (SARs), which may include organized transactions. Law enforcement agencies must submit feedback to FinCEN when they observe transactions that may involve money laundering, and FinCEN needs to obtain feedback on time from law enforcement agencies and provide feedback information to the institutions that submitted the information.

AMLA also provides for increased resources and measures to strengthen cooperation within law enforcement and national security agencies and with foreign countries (Hausfeld et al., 2021). Promote information sharing through collaboration with the private sector and establish information security and innovation officers in relevant regulatory agencies. To promote the development of regulatory technology, improve the speed of monitoring and responding to financial crimes, while protecting the data security of the financial system, ensuring the security of sensitive information, and preventing data leaks. At the same time, only staff of foreign financial intelligence agencies were photographed, cooperating with financial intelligence units of other countries to jointly combat transnational financial crimes. This not only helps to improve the detection and punishment of anti-money laundering activities but also strengthens the crackdown on related predicate crimes.

(5) The fifth is to increase penalties, including fines and other legal consequences, for financial institutions and individuals who violate the Bank Secrecy Act and anti-money laundering regulations (Hausfeld et al., 2021). The Treasury Secretary can levy additional civil penalties for repeat violations, up to three times the profits gained or losses avoided, or twice the maximum penalty for the violation. Certain partners, directors, officers, or employees of financial institutions found in violation must repay any bonuses received during or after the violation. Additionally, individuals guilty of a "serious violation" of the BSA face a 10-year ban from serving on the board of directors of a U.S. financial institution from the date of conviction or sentencing.

(6) It allows financial institutions to share SAR reporting information with their branches or affiliates in other countries, helping companies operating globally to manage and mitigate risks more effectively (Hausfeld et al., 2021). Current FinCEN guidance restricts the sharing of SARs by financial institutions to only their parent companies located outside the United States. However, AMLA introduced a three-year pilot program that allows financial institutions to share special administrative areas with foreign branches, subsidiaries, and affiliates.

(7) The seventh is to identify key areas or priorities for anti-money laundering and counter-terrorism financing work to make AML/CFT policies more targeted and efficient, and ensure that resources are effectively allocated to key areas. Within six months of the AMLA being enacted, the Treasury Department is required to engage in discussions with the DOJ, pertinent state and federal oversight bodies, and national security agencies (Hausfeld et al., 2021).

(8) The last one requires the Department of Justice to report to Congress annually on all cases involving Bank Secrecy Act resolutions, increasing the transparency of regulatory actions and allowing lawmakers and the public to better understand the enforcement of AML laws. Section 6311 of the AMLA mandates the Department to annually report to the Congressional Committees on Judiciary and Banking regarding all deferred prosecution agreements and non-prosecution agreements (BSAs) entered into during the preceding year concerning any violation or suspected violation. (Hausfeld et al., 2021) The report must detail the reasons for the actions, the factors weighed, and the level of coordination with other regulators by the Justice Department before settling.

These modifications are significantly helpful in governing and supervising virtual currency (cryptocurrency) money laundering activities in the United States. The existing anti-money laundering (AML) framework has been strengthened to ensure that it can adapt to the rapidly evolving digital economic environment.

5 Necessary Reform Directions for Anti-Money Laundering Regulation in Australia

5.1 Innovative Data Acquisition Methods

Ensuring effective regulation and the prevention and detection of illegal activities in the digital space is critical, and Australia has adopted government-private sector collaboration to face the above challenges. For example, there are private companies that specialize in blockchain analysis, such as Chainalysis, Elliptic, and CipherTrace (Goldbarsht, 2023), which have developed tools to identify, track, and investigate cryptocurrency transactions. These companies have found success in the market by working with law enforcement agencies and regulators, filling financial institutions' technology and resource gaps in money laundering detection.

However, obtaining sufficient, real transaction data is crucial for the algorithm to accurately learn and identify suspicious transaction patterns. However, when financial institutions develop and train machine learning algorithms for money laundering detection, there is a lack of access to a large amount of real transaction data (Goldbarsht, 2023). Regulators need to develop and adopt new strategies and methods to effectively supervise specific areas, especially such rapidly developing and changing areas as virtual assets (Schmidt, 2021), in addition to incorporating publicly available historical data, such as sanctions lists, into the analysis of machine learning algorithms.

We can also learn from the U.S. actual beneficiary registration system to improve the transparency of corporate ownership, such as establishing a non-public registry that tracks actual beneficiaries, using this data in specific circumstances, and sharing it with law enforcement agencies (including foreign agencies). (Hausfeld et al., 2021) Improve the transparency of corporate ownership, help regulators identify and prevent money laundering and terrorist financing risks, and enable law enforcement agencies to track and prevent the flow of illicit funds more effectively. It can even support cross-border information sharing and law enforcement collaboration, which will help regulators access

large amounts of real data to track and prevent illicit financial flows, especially when complex corporate structures and cross-border transactions are involved.

5.2 The Application of Blockchain and Machine Learning Technologies

The development of new regulatory technologies must be accelerated. Technical tools to assist regulatory and law enforcement agencies in identifying, tracking, and analyzing digital assets have turned to blockchain networks, leveraging technical tools, including the use of private blockchain analytics and asset tracking companies, to assist in identifying and investigating the illicit origins of assets. Track real-time financial transactions and reconstruct the detailed records leading up to the illicit flow of assets to reveal the complete path of illicit asset flows and address the ever-changing landscape of criminal enterprises. Financial institutions can employ machine learning techniques to enhance their transaction monitoring systems. Specifically, machine learning algorithms can be used to review and analyze alerts generated by transaction monitoring systems to identify suspicious transactions more efficiently. In this way, financial institutions can leverage big data through analytical techniques to improve the accuracy and efficiency of anti-money laundering monitoring.

Although the development of blockchain analysis technology is not fully mature today, the use of machine learning technology to combat digital assets and money laundering has been effective. Researchers believe that these technologies can effectively identify, track, and analyze criminal assets, and may later be extended to confiscation and seizure activities. Ensuring technology is at the leading edge of identifying, tracking, and seizing digital assets involved in illegal activity is critical.

Therefore, policymakers and law enforcement agencies must actively take measures to adopt specific laws and regulations. Use advanced analytical tools and algorithms to establish more specific and advanced data analysis systems to enhance its regulatory capabilities, while providing feedback on system usage to financial institutions to improve measures and improve the transparency and interactivity of AML measures. Regulators also need to continuously update their technical tools and training procedures to ensure that the skills and knowledge of relevant personnel keep pace with technological developments.

5.3 Ensuring Regulatory Strategies for Financial Privacy

When formulating regulatory rules, the sensitivity of the data and the importance of protecting personal information should be considered. Monitoring activities should be carried out without infringing on personal privacy. While strengthening anti-money laundering monitoring measures, users' financial privacy rights must be protected. Monitoring activities need to be conducted within a clearly defined legal and policy framework, ensuring that all regulatory measures comply with existing laws when accessing and using blockchain data. Therefore, it is necessary to define the specific scope and conditions for regulatory agencies to access and use blockchain data to ensure that these activities comply with both anti-money laundering requirements and privacy protection standards. Blockchain technology can be effectively used to enhance anti-money laundering efforts without sacrificing privacy protection.

5.4 Enhancing International Cooperation to Combat Cross-Border Money Laundering Activities

Money laundering crimes are often transnational, with criminals tending to commit predicate offenses in one

jurisdiction and then launder the illicit proceeds through another jurisdiction to make the proceeds more difficult to trace (Keesoony, 2016). In addition to having strong domestic laws to combat money laundering, countries must also focus on international cooperation, including cooperation with the private sector, especially financial technology companies and blockchain analysis service providers, which can provide key technology and data support.

Money laundering should be recognized as a specific crime under international law. In March 2023, FATF stated that jurisdictions must utilize various approaches (Goldbarsht, 2023), such as involving the private sector, to help identify potentially suspicious transactions within the digital asset ecosystem.

Establishing and strengthening harmonized laws and procedures at the international level, particularly in dealing with the confiscation of assets derived from crime, can weaken the emergency foundations of criminal organizations through the confiscation of illegally obtained property. There should also be the ability to use technical means to monitor and record the movement of property to ensure that it can be effectively controlled and prevented from being illegally transferred or disposed of before any criminal investigation is concluded. However, it is worth discussing that achieving such globally unified laws is not without obstacles. Differences in economic development levels, legal system maturity, and regulatory capabilities among countries have created complexity and challenges in implementing globally unified standards. Countries with less developed economies may lack the resources and technology to implement complex financial surveillance systems, which may lead to uneven global anti-money laundering efforts.

5.5 Enhancing Business Certainty in Australian Digital Currency Regulation and the Role of ASIC

An Australian digital currency must have commercial certainty so that participants understand the rules. This is even though ASIC's current remit is already broad. But the functions and powers under the ASIC Act are to "maintain, promote and improve the performance of the financial system" and "promote the confident and informed participation of investors and consumers," positioning it as the regulator closest to the operation of digital currencies (Latimer & Duffy, 2019).

Given that ASIC is the financial services regulator, the consumer credit regulator, the market regulator, the corporate regulator, and the agency with overall responsibility for financial literacy, ASIC has a good track record as a financial regulator and has accumulated experience in dealing with some digital currencies.

Despite widespread claims that digital currencies are not securities, financial products, or legal tender, ASIC acknowledges the existence of 'virtual currencies' and issues a warning to consumers on its MoneySmart website. With the rapid development of the digital currency industry, it is necessary to increase the federal government's financial support for ASIC to expand its regulatory capabilities. ASIC is the appropriate regulator and best placed to achieve this objective.

6 Conclusion

By comparing the current performance of Australia and the United States in anti-money laundering regulatory enforcement, as well as the main measures of the two countries in the face of the rapidly developing digital assets and virtual currency markets. It can be seen that both Australia and the United States have established relatively mature anti-money laundering regulatory frameworks and have made certain progress in using new technologies such as blockchain

and machine learning for transaction monitoring and risk assessment. However, the regulatory framework in the United States is relatively new and is developing at a faster pace. There are still many regulatory loopholes and challenges in the specific implementation process of this framework.

In a globalized economic environment, virtual assets are highly cross-border and require stronger international cooperation and information-sharing mechanisms to contain them. Australia should further strengthen cooperation with international anti-money laundering organizations such as the Financial Action Task Force (FATF) to ensure the global consistency and effectiveness of anti-money laundering policy measures. At the same time, we must increase investment in advanced technologies such as machine learning, artificial intelligence, and blockchain, and at the same time, strengthen supervision or increase penalties in all aspects, so that we can flexibly adapt and plug regulatory loopholes as much as possible. Through these conclusions and recommendations, this paper provides specific policy directions for Australia to improve its efficiency and effectiveness in the area of anti-money laundering, address technical challenges, and promote broader international cooperation to maintain the security of Australia's financial system.

References

[1] Chawki, M. (2022). Cybercrime and the Regulation of Cryptocurrencies. In K. Arai (Ed.), *Advances in Information and Communication* (pp. 694). Springer International Publishing.

[2] Goldbarsht, D. (2023). Adapting Confiscation and Anti-Money Laundering Laws to the Digital Economy: Exploring the Australian Interplay Between Proceeds and Technology. *Journal of Money Laundering Control, 27*(3), 472.

[3] Hausfeld, K. A., Newman, M. E., Stratton, G., Hamid, D., Hare, J. L., & Krystek, B. (2021).*The New Anti-Money Laundering Act of 2020: A Potential Game-Changer for Enforcement and Compliance.* DLA Piper. https://genesiscompliance.com/wp-content/uploads/2021/01/New-AML-Act-2020-United-States-of-America.pdf.

[4] Hossain, M. B. (2023). Acquiring an Awareness of the Latest Regulatory Developments Concerning Digital Assets and Anti-Money Laundering. *Journal of Money Laundering Control, 26*(6), 1261.

[5] Keesoony, S. (2016). International Anti-Money Laundering Laws: The Problems with Enforcement. *Journal of Money Laundering Control, 19*(2), 130.

[6] Latimer, P., & Duffy, M. (2019). Deconstructing Digital Currency and Its Risks: Why ASIC Must Rise to the Regulatory Challenge. *Federal Law Review, 47*(1), 121.

[7] Schmidt, A. (2021). Virtual Assets: Compelling a New Anti-Money Laundering and Counter-Terrorism Financing Regulatory Model. *International Journal of Law and Information Technology, 29*(4), 332.