GRIFFITH UNIVERSITY

Submission to Attorney-General's Department Consultation Paper on Modernising Australia's Anti-Money Laundering and Counter-Terrorism Financing Regime

To: Attorney-General's Department
3/5 National Circuit,
Barton ACT 2600
Australia

15 June 2023

Dear Sir/Madam,

Re: Submission to the Attorney-General's Department concerning the Proposal to modernise Australia's anti-money laundering and counter-terrorism financing regime

We appreciate the invitation to participate in the consultation exercise proposed by the Attorney-General's Department regarding the reforms to Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regime. This submission was co-authored by the following researchers and practitioners:

- Professor Andreas Chai, Director of the Academy of Excellence in Financial Crime Investigation and Compliance, Griffith Business School, Griffith University
- Associate Professor Jacqueline M. Drew, Deputy Director of the Academy of Excellence in Financial Crime Investigation and Compliance, School of Criminology and Criminal Justice, Griffith University
- Professor Ernest Foo, Deputy Director of the Academy of Excellence in Financial Crime Investigation and Compliance, School of Information and Communication Technology, Griffith Sciences, Griffith University
- Professor Shireenjit Johl, Deputy Head of Department and Deputy Director of the Academy of Excellence in Financial Crime Investigation and Compliance, Griffith Business School, Griffith University
- Josh Murchie, Co-founder of Social Impact Group and Industry Fellow at the Griffith Centre for Systems Innovation, Griffith University
- Professor Michael Townsley, Director of the Social Analytics Lab, School of Criminology and Criminal Justice and member of the Academy of Excellence in Financial Crime Investigation and Compliance, Griffith University
- Dr Tom Verhelst, Director of the Relational Insights Data Lab, Griffith University

Objectives of the Inquiry

The overall objective of the proposal is to simplify and modernise AML & CTF Regulation. Current challenges as noted by the Department include:

- The distinction between Part A and Part B of AML/CTF programs is complex
- Obligations related to simplified due diligence were assessed in Australia's 2015 FATF Mutual Evaluation as being non-compliant, and
- The lack of an express statements in the Act or Rules setting out the requirement for regulated entities to conduct a money laundering and terrorism financing assessment, despite many of the requirements for risk-based systems and controls which implicitly require it.

We strongly support the overall aim of the proposal to simplify and streamline the AML/CTF regime while expanding it to cover Designated Non-Financial Businesses & Professions (DNFBP), thereby aligning Australia's practices with that of more than 200 other jurisdictions who already regulate DFNBPs. These efforts will enhance the AML/CTF regulatory framework and provide more significant protection to Australian communities while encouraging greater compliance with AML/CTF obligations. These reforms help address several widely held observations by industry, regulators, and researchers:

1. Australia's AML/CTF regime lags that of its counterparts in other countries, particularly when considering Australia's position in the international arena (Attorney-General's Department, 2016).

2. The efficacy of AML/CTF frameworks internationally lacks a credible evidence base, raising questions about the appropriateness of the costs imposed by regulatory oversight and its ability to deter financial crimes (Levi, 2020).

The proposal raises the question of what kind of national research and training capacity is required in Australia for the new regime to work effectively? Specifically, consideration should be given to what training and resources do DNFBPs require to effectively identify, asses, and understand the risks of financial crimes. DNFBPs will require access to an ongoing knowledge base that delivers insights into the constantly evolving nature of financial crime typologies. These reforms will also increase demand for training and education packages to ensure that reporting entities are not faced with emerging skills shortages (SMH 2021).

1. Growing the knowledge foundations for effective risk assessment

In relation to question 1 "How can the AML/CTF regime be modernised to assist regulated entities address their money laundering and terrorism financing risks?" and question 5 "What

are your views on the proposal to expressly set out the requirement for entities to identify, mitigate and manage their proliferation financing risks?"

For regulated entities to effectively mitigate financial crime and financing the proliferation of weapons of mass destructions, it is crucial that they identify, assess, and understand the risks and how circumstances of the business are linked to these types of activities.

A key challenge in this effort is that there exists limited research available to regulate entities about financial crime typologies and how they evolve as new technologies emerge. This challenge will grow as the number and variety of reporting entities will increase. This poses a serious challenge as understanding risks can push regulated entities to engage in the relatively costly services of advisory firms that further adds to the financial cost of regulation.

We encourage the Department to consider how University researchers across Australia can play a key role in helping contribute towards the knowledge base required for regulated entities to identify, assess and mitigate risks associated with financial crime.

University researchers are in a position to conduct foundational research that regulators and law enforcement are not equipped to conduct. Academic researchers from various disciplines, such as Criminology, Forensic Accounting, and ICT, can generate new knowledge about financial crimes such as money laundering, terrorist financing, and fraud. Increasing the depth and scope of publications on financial crime typologies can help ensure a wide variety of regulated entities have cost effective access to knowledge that can help improve their approaches to monitoring and reporting suspicious behaviour, as well as conducting risk assessments.

In addition, regulators themselves have an increasing need to understand how new technologies may be exploited for financial gain (Akartuna et al., 2022; Trozze et al., 2022). As technology advances, financial crime moves to newer and more complex technology applications, like cryptocurrency. More research is necessary to ensure policymakers have the knowledge to develop efficient policies to combat these evolving crimes. Such type of research will strengthen and enhance Australia's financial system and enable Australia to become a world leader in combatting financial crimes. These capabilities can potentially assist Australia's performance in its effectiveness ratings that are part of the FATF's mutual evaluations.

Overall, prioritising financial crime as a new national research priority in Australia's Science and Research priorities is essential. Australia's Science and Research Priorities serve to incentivise researchers to focus on areas of strategic national importance (Australian Government, 2015). The overall goal of this initiative is to help Australia achieve its economic, social, and environmental objectives by supporting research that tackles important national policy issues. Encouraging researchers to focus on financial crime can help to create a more action-oriented and responsive research environment, something sorely needed. Additionally, this would help strengthen Australia's reputation as a leader in the fight against financial crime.

RECOMMENDATION 1: Research into financial crime, in particular money laundering and terrorist financing, be added as a new national priority in Australia's Science and Research Priorities.

The proposal will increase the number of reporting entities by a factor of four (Attorney-General's Department, 2023). Considering this significant increase, it is imperative that AUSTRAC and law enforcement have a clear understanding of the implementation and compliance issues surrounding the expansion. Additional assessments, monitoring, and evaluation should be conducted to ensure the new system is effective. As researchers are well-suited to perform such analyses, they are ideal candidates for carrying out these studies.

Integrity testing plays a crucial role in corporate governance by testing the strength of an organisation's internal controls (USAID, 2005), going beyond the traditional approach of verifying their existence. Profiling businesses, in terms of their program effectiveness related to AML/CTF will assist in identifying areas that require further research and guidance. It will enable a more targeted strategy to be developed for the purpose of improved compliance.

Such research can also be harnessed to evaluate compliance with AML/CTF regulation (Findlay et al. 2012). Fostering a culture of compliance among reporting entities could be a key objective of this program of research. Developing a program of research to assess preparedness and monitor the performance of reporting entities could help support Australia's performance in FATF mutual evaluations. Overall, there is a need for continued development of more effective AML/CTF policies, innovative monitoring techniques, and improved capabilities to detect and deter financial crime.

RECOMMENDATION 2: It is recommended that a program of research be developed to assess preparedness and monitor the performance of reporting entities.

2. Promoting Greater Information Sharing Arrangements between regulated entities and universities

For the new AML/CTF regime to work effectively, it is important to create an institutional environment that is conducive to enabling research and collaboration that can be used by reporting entities to identify and mitigate the risks of financial crime. The Department should consider what provisions can be made to encourage regulated entities, regulators, and universities to work together to share information and collaborate. As recently noted by the FATF:

> "Collaboration and information sharing helps financial institutions to build a clearer picture of criminal networks and suspicious transactions, and better understand, assess, and mitigate their money laundering (ML), terrorist financing (TF) and proliferation financing (PF) risks. It can also provide authorities with better quality

intelligence to investigate and prosecute these crimes and ultimately help prevent crime from reaching our streets." (FATF 2022)

We encourage the Department to consider how to promote greater data sharing arrangements between regulated entities and universities. Universities can play a crucial role in establishing connections between government, regulators, and businesses, thereby ensuring a fair and impartial approach. In the same manner that universities' research expertise is harnessed to support Australia's Defence and Cybersecurity capabilities, their expertise in Machine Learning, Criminology and Forensic Accounting could also be harnessed to support the risk assessment capabilities of reporting entities. Furthermore, their unwavering dedication to ethical principles and autonomy instils confidence when facilitating data sharing among competitors.

Case Study: A proposal for a Financial Crime Data collaborative

The Academy of Excellence in Financial Crime Investigation and Compliance is seeking to establish a national data collaborative for financial crime in partnership between multiple organisations across the public and private sector. This would utilise a secure air gapped data facility designed to DISP Level 2 Certification. The facility has securely housed sensitive data for close to a decade and is currently pursuing accreditation as Accredited Data Service provider under the DAT Act. Similar to Transaction Monitoring Netherlands (TMNL), linking data across multiple financial institutions and government entities can help highlight the need for a 'multibank' monitoring approach (FATF 2022). In addition, combining data from public entities with private data has the potential to generate highly innovative and world first insights into international financial crime typologies. In Australia, there exists an opportunity to pursue such a project under the Australian Data Availability and Transparency (DAT) Act, which is a legislative framework that was introduced in 2020 to improve the accessibility and transparency of data held by government agencies. The DAT Act sets out a number of objectives including promoting the sharing and use of public sector data, ensuring appropriate privacy safeguards are in place, and enabling the creation of new products and services that benefit the public.

To better facilitate such public private partnerships, the Department should consider making provisions in the new regime that encourages regulated entities to share information with universities. As highlighted by FATF (2022), a good example of such a provision is the Section 314(b) of the USA PATRIOT ACT:

> *Section 314(b) of the USA PATRIOT ACT provides that two or more financial institutions and any association of financial institutions may share information with one another regarding individuals, entities, organisations, and countries suspected of possible terrorist or money laundering activities. A financial institution or association that transmits, receives, or shares such information for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities shall not be liable to any person under any law or regulation of the US, any constitution, law, or regulation of any State or political subdivision thereof, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such*

disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure, or any other person identified in the disclosure.

RECOMMENDATION 3: We encourage the Department to implement a similar provision to the Section 314(b) of the Patriot Act, in a manner that enables reporting entities and public entities to share information and collaborate with universities.

3. RegTech and FinTech approaches to reducing AML/CTF financial burden for Sole Trader, NPOs and small business

RegTech (regulatory technology) and FinTech (financial technology) infrastructure have the potential to significantly decrease the costs and risks associated with vetting and supporting non-profit organisations. As emphasised by the Productivity Commission's recent information policy on Regulatory Technology (PC 2020), RegTech can support the improved targeting of regulation and reduce the costs of administration and compliance. Regulating sole traders and small to medium sized organisations (both for profit and non-profit) with more stringent AML/CTF requirements may place unreasonable time and financial burdens on the organisations and lower competitiveness with larger firms and organisations.

Small to medium business enterprises (SMEs) comprise 98% of Australian registered businesses (ABS, 2021). Industry estimates place the typical cost of a retail Know Your Customer (KYC) at $18 ($12USD) and a corporate customer at $454 ($300USD) (PWC, 2021). In an increasingly global, digital, and connected world organisations should no longer be assuming all customers will be local, and that the chance of dealing with international or online-only customers or clients is increasingly likely.

The proposal has the potential to significantly impact the profitability of SMEs that are DFNPBs. The new proposal creates a new challenge to business owners as they need to consider when in the customer onboarding process KYC/AML processes are implemented in order to reduce the risk of overall costs.

The cost of conducting a KYC check on every prospective customer can be prohibitive for SMEs who lack the internal resources and budgets. This may result in these types of organisations discriminating and rejecting prospective customers in fear of the likelihood of incurring costs of a failed KYC/AML. This provides an unfair competitive advantage for larger organisations. It can also result in smaller organisations having to increase their costs to cover the KYC costs and the costs of acquiring prospective customers that have failed KYC (costs for advertising, marketing, overheads, and KYC check).

- For example, larger reporting entities may have internal databases and heavily reduced costs for bulk KYC checks to external providers. Whilst SMEs would be required to commit to a minimum number of checks or pre-purchasing checks to reduce the cost, and then may lack the internal cybersecurity and data privacy systems in order to retain that information securely for future reference. Larger reporting entities have the ability to KYC a customer once, securely store that information on internal databases and provide access to their associates at no additional cost.

Beyond DNFBPs, some consideration should be given to what extent charities and other non-profit organisations (NPOs) should be included in Tranche 2. There are over 60,000 registered non-profits and estimates of over 600,000 unregistered non-profits in Australia alone (ACNC, 2023). Non-profit organisations contribute over $143 billion dollars to the Australian Economy or around 8% of GDP (Australian Treasury, 2017). Non-profits also employ around 11% of the total Australian workforce or 1.38 million people (McKinsey, 2021). The charity sector has been exploited by terrorist groups to fundraise (US Treasury, 2023, UNODC, 2023). Scammers also target the generosity of the public sector, especially after high profile disasters and events, such as COVID-19, Bushfires and Earthquakes (US FBI, 2023). In 2022, the Australian Charities and Not for Profit Commission (ACNC) and Scamwatch reported that Australians lost over $336,000 to Charity related scams (ACNC, 2022), whilst the United Kingdom reported an increase of 44% in the number of Charity Scams, with the public losing over $4.35 million (£2.3 million) (CivilSociety, 2023). At the same time, including NPOs in Tranche 2 can potentially put at risk the operations of NPOs and reduce the flow of charitable donations to vulnerable Australians. A lack of expertise, accessible technology and financial resources also place undue pressure on NPOs.

Case Study 1 - Verified Non-profit Financial Transactions with FinTech & RegTech Infrastructure:

Little Phil (short for little philanthropist), a social enterprise technology platform has developed infrastructure technology that allows non-profits to register an account, undertake a completely digital KYC/AML process and have their registration details cross-checked with the government's databases to confirm the legitimacy of the organisation and the identities of the responsible persons. The technology integrates into numerous live databases that include the ACNC, the Australian Business Registry, and financial grade Know Your Customer identification checks.

This allows any donor, business, or financial supporter to make financial contributions to the organisation via the Little Phil technology infrastructure with a high degree of certainty that the organisation and its authorised representative are legitimate and that extensive KYC/AML checks have been conducted.

This case study demonstrates the use of RegTech and FinTech to lower the costs of conducting financial transactions with entities as donors, businesses, and philanthropic foundations can be confident that a stringent KYC/AML policy is implemented when conducting the transaction via the Little Phil technology infrastructure.

This also reduces the costs for non-profit organisations to request funding and prove their legitimacy. The verification process for a large donor to ensure that the request and the recipient are legitimate can now be completed in seconds and at no additional cost simply by using the Little Phil technology.

Web2 based solutions (see glossary) such as this may be developed using similar technology architecture to create affordable and reliable KYC/AML access for SMEs and sole traders. However, as the world continues to embrace emerging technologies in the Web3 (see glossary) sector, we recommend that a comprehensive forward-thinking approach be considered to allow flexibility for future integrations.

These integrations may include currencies such as:

1. Central Bank Digital Currencies (CBDC's) - the RBA along with many countries around the globe are actively researching and testing these technologies (RBA, 2022)
2. Private Industry Digital Currencies such as the recently tested Australian Dollar Stable Coin (AUDN) launched in partnership with National Australia Bank (NAB) (NAB, 2023), which is built on top of the public decentralised blockchain protocol Ethereum
3. Other NGO and private sector digital currencies - these may include digital utility currencies that are used to pay for goods or services.

Web3 solutions are built using blockchain technology and have the potential to increase privacy, reduce the risk of fraud and lower the costs of transactions, including dealing with KYC/AML verified parties.

RECOMMENDATION 4: Consider the use of RegTech and FinTech to lower the financial and time burdens on SMEs and supports their competitiveness.

Case Study 2 - Blockchain Enabled KYC/AML Smart-contract Oracle

Social Impact Group Pty Ltd has been researching and developing smart-contract based solutions on the public decentralised blockchain protocol Ethereum that integrate with existing KYC/AML solutions to create an oracle that allows for transactions to take place with verified and approved users, without the need to perform additional KYC/AML costs for each party that wishes to transact with the party.

How does it work?

A potential customer or client will use their Ethereum wallet address (unique) to sign a transaction (similar to logging in) and then apply for a KYC/AML check using a secure online application form. The form will collect the required identification and capture other current data points to ensure that the user is real and matches the identity documents provided. This information is then cross-checked with global databases that check sanctions, PEPS (politically exposed persons) and other relevant AML/CTF databases. Once the check is complete, the user's unique Ethereum wallet address will either be whitelisted or rejected. If the wallet is whitelisted, it is added to a database of approved addresses that can be dealt with.

A smart-contract can then be launched as the low cost solution that will cross-check the whitelist and will allow for transactions to those users who have been whitelisted. This requires no additional third-party checks and can be customised with variables such as expiry dates for how long a KYC/AML check is considered valid (ie. a check must be conducted within 12 months).

The user's unique wallet address is now attached to the user's verified KYC/AML result, and external parties can request that the customer signs an on-chain (blockchain interaction) transaction that provides access to verified details of the customer and displays the KYC/AML result, date etc.

Multi-factor verification systems can be implemented to decrease the risk of unauthorised attempts to use the person's or business' unique wallet should the private keys (password) fall into the wrong hands.

This case study highlights how smart contacts can be harnessed to provide a more secure system for identification checks, specifically with financial lending products where there is a high incentive and low barrier for criminals to acquire fraudulently obtained personal identification documents from data breaches. Retail loan applications rarely ask for any permission or verification outside of uploading identification and checking a box to agree to conduct a credit check. In this scenario, a check could not be conducted without the applicant signing (approving) the transaction to access their proof of identity check results.

RECOMMENDATION 5: Consider making provisions in the AML/CTF regime to enable regulated entities to use cost effective emerging technologies such as blockchain and smart contracts.

RECOMMENDATION 6: Establish a diverse advisory board that comprises professionals ranging from sole traders, researchers, and professional firms - history has shown that relying on one technology provider or consulting firm does not necessarily yield the best outcomes.

4. Growing the national skills base in AML/CTF compliance

Compared to the US and EU, currently the training landscape for Financial Crime Investigation and Due Diligence is relatively underdeveloped in Australia. The proposal has the potential to add increased pressure on skills shortages among reporting entities that require specialist skills to conduct due diligence and associated risk assessments. Griffith University's Academy of Excellence in Financial Crime Investigation and Compliance has recently launched a Graduate Certificate and Graduate Diploma in Financial Crime Investigation and Compliance to address the potential skills shortages.

We encourage the Department to consider a further audit to determine what skills are required by reporting entities (both financial and DNFPBs) to ensure they are positioned to effectively meet their obligations under the new AML/CTF regime. These risks should be catalogued and incorporated into the Australian Skills Classification (Jobs and Skills Australia). Based on our own assessment, such skills for financial entities should include:

- Investigative techniques and practical skills required to investigate and report suspicious activity in written form.

- A basic understanding of victims and offenders typically involved in financial crimes, as well as the reporting obligation of reporting entities under the new regime.

- Skills in forensic analysis of financial transactions and financial statements typically used in KYC processes to identify Source of Funds/Source of Wealth (SoF/SoW).

- Skills to employ data analysis and visualisation techniques for transaction monitoring to analyse risks associated with financial crimes.

- Skill required in conducting risk assessments of customers, and producing, as well as implementing, a risk-based approach from an enterprise perspective. This should include a basic understanding of the probability distribution and payoffs associated with financial crime.

PART B: What professional services are proposed to be covered?

Our response will address Questions 23-25 with specific emphasis on the services by the accounting sector.

Australia is one of the few developed countries that has not enacted legislation to extend anti-money laundering and counter-terrorism financing (AML/CTF) laws to cover the accounting and legal professions. Accountants can potentially play a critical role in preventing money laundering and counter terrorism financing by ensuring compliance with AML/CTF laws and regulations.

It is clear that their specialist expertise in financial systems can be harnessed to facilitate money laundering by creating and manipulating transactions to obscure the origins and destinations of illicit funds. In fact, the involvement of accountants is vital as large amounts of money cannot be easily laundered without their direct or indirect participation (Mitchell et al. 1998). Additionally, auditors may be unwilling or unable to disclose and report such illicit activities due to confidentiality or fear of revenue loss. Thus, accountants face a higher risk of being targeted by criminal elements due to the nature of their services (Compin, 2008).

Based on this literature, auditing services need to be regulated under the AML /CTF regime. While external audits are already heavily monitored through ASIC annual inspection, it is unclear how many quality review assessments are carried out each year and percentage of deficiencies is not made known to public (other than ASIC yearly inspections). Thus, there is a lack of transparency around the consistency of supervision of the accounting sector, and the levels of compliance among regulated professionals.

The inspection of audit firms and surveillance of auditors via ASIC are essential tools for ensuring compliance and influencing the behaviour of registered company auditors and audit firms. Through its audit inspection program, ASIC assesses adherence to requirements concerning audit quality and auditor independence. Registered company auditors and firms are obligated to comply with the Corporations Act and adhere to all relevant auditing standards and other applicable requirements for each engagement.

Further, auditing standards that are applied in Australia has the force of law. One standard that is relevant is ASA 250 Consideration of Laws and Regulations in an Audit of a Financial Report.

Reporting Identified or Suspected Non-Compliance to an Appropriate Authority outside the Entity

29. If the auditor has identified or suspects non-compliance with laws and regulations, the auditor shall determine whether law, regulation or relevant ethical requirements: (Ref: Para. A28–A34)

    (a) Require the auditor to report to an appropriate authority outside the entity.

    (b) Establish responsibilities under which reporting to an appropriate authority outside the entity may be appropriate in the circumstances.

Additionally, accounting bodies such as CPA Australia and the Chartered Accountants Australia and New Zealand (CAANZ) bear the responsibility of regulating the conduct of professional accountants - CPAs. As part of their regulatory function, these professional bodies typically address complaints concerning the ethical and professional conduct of CPAs, CPA practices and registered students. Adherence to the professional standards set by the respective bodies is a membership requirement. The compliance and disciplinary processes serve as crucial mechanisms through which the professional bodies ensure the proper conduct of their members, including the imposition of sanctions for serious breaches or violations of professional standards. Additionally, these bodies have a quality review program that are integral to CAANZ and CPA Australia. The program is designed to assess whether Australian members who hold a public practice certificate have implemented appropriate quality control procedures in their practices. To ensure these accounting bodies are effective in enforcing professional standards among their members, we recommend the establishment of a separate oversight body dedicated to professional services, akin to the UK's Office for Professional Body Anti-Money Laundering Supervision (OPBAS).

In summary, we acknowledge and support the inclusion of accounting services and other Designated Non-Financial Businesses and Professions (DNFBPs) within the scope of the AML/CTF Act.

We also suggest that the covered business activities should align with the requirements specified in FATF Recommendation 22. It is essential to highlight that Australia is not under international obligation or bound by national policy to exceed the provisions outlined in FATF Recommendation 22.

RECOMMENDATIONS

1) **The development of a specific guidance documents for the accounting profession, similar to the UK AML guidance for Accountancy Sector (Consultative Committee of Accountancy Bodies, 2022).**

2) **The establishment of a separate oversight body dedicated to professional services, akin to the UK's Office for Professional Body Anti-Money Laundering Supervision (OPBAS). The primary objective of OPBAS is to enhance the overall standards and consistency of supervision; and ensure supervisors and law enforcement work together more effectively.**

Glossary

The following provides a brief outline of common terminology along with case studies to clearly convey the recommendation.

Blockchain is a decentralised and transparent digital ledger that records and verifies transactions. It enables secure and tamper-proof storage of data, making it highly resistant to fraud or unauthorised changes. Each transaction or record, called a block, is linked to previous blocks, forming a chain of information. Blockchain offers increased efficiency, transparency, and trust in various industries.

Digital Wallet, for the purpose of this submission, is referred to as a software application that allows a user to transact and interact (send and receive tokens and sign transactions for verification) on a blockchain protocol (Ethereum in this example).

Smart Contract is a digital agreement that automatically executes itself once certain conditions are met. It's a computer program that runs on a blockchain, such as Ethereum, and is designed to facilitate and enforce the terms of an agreement between multiple parties. Unlike traditional contracts that require intermediaries like lawyers or banks to ensure compliance, smart contracts eliminate the need for intermediaries by automatically executing actions based on predefined rules. These rules are written in code and stored on the blockchain, making them transparent, tamper-proof, and verifiable.

- Smart contracts can be used for various purposes, such as transferring digital assets, making payments, or establishing conditions for the release of funds. They provide a secure and efficient way to conduct transactions without relying on a central authority.

Web2, or Web 2.0 refers to the current generation of the internet that emerged in the early 2000s. It is characterised by user-generated content, social media, and interactive web applications. Web2 introduced a shift from static web pages to dynamic platforms that enable users to actively participate, create, and share information. It emphasises social collaboration, user engagement, and the integration of various web services and APIs.

- In Web2, users primarily consume content and interact with centralised platforms owned and controlled by companies or organisations. These platforms often collect and monetise user data for targeted advertising and other purposes. Web2 has facilitated the rise of social media networks, online communities, e-commerce, and various web-based services that have become an integral part of everyday life for billions of people worldwide.

Web3, or Web 3.0 is the next generation of the internet characterised by decentralisation and user empowerment. It leverages technologies like blockchain, smart contracts, and cryptographic security to create a more open, transparent, and peer-to-peer network. Web3 aims to shift control from central authorities to individuals, allowing them to have greater ownership and control over their data, digital assets, and online identities. It envisions a future where users can interact, transact, and collaborate in a trustless and interoperable manner, fostering innovation and enabling new economic models.

References

Akartuna, E. A., Johnson, S. D., & Thornton, A. (2022). Preventing the money laundering and terrorist financing risks of emerging technologies: An international policy Delphi study. *Technological Forecasting and Social Change*, *179*, 121632.

Attorney-General's Department. (2016). *Report on the Statutory Review of the AML/CTF Act and Associated Rules and Regulations*. Australian Government. https://www.austrac.gov.au/about-us/corporate-information-and-governance/reports-and-accountability/report-statutory-review-amlctf-act-and-associated-rules-and-regulations

Attorney-General's Department. (2023). *Modernising Australia's anti-money laundering and counter-terrorism financing regime: Consultation paper on reforms to simplify and modernise the regime and address risks in certain professions*. Australian Government. https://consultations.ag.gov.au/crime/aml-ctf/

Australian Charity and Not For Profit Commission (2023). ACNC charity data: A comprehensive and valuable resource for the sector. https://www.acnc.gov.au/media/news/acnc-charity-data-comprehensive-and-valuable-resource-for-sector#:~:text=The%20Charity%20Register%20has%20information,programs%2C%20their%20location%20and%20beneficiaries

Australian Bureau of Statistics (2022). ABS Counts of Australian Business, Table 13a. https://www.asbfeo.gov.au/sites/default/files/202208/Contribution%20to%20Australian%20Business%20Numbers_August%202022%20_4.pdf

Australian Government. (2015). Science and Research Priorities. *Fact Sheet*.

Consultative Committee of Accountancy Bodies. (2022) *Anti-Money Laundering and Counter-Terrorist Financing Guidance for the Accountancy Sector.* https://www.ccab.org.uk/anti-money-laundering-and-counter-terrorist-financing-guidance-for-the-accountancy-sector-2022/

FATF (2022), Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing, FATF, Paris, France.

FATF (2012-2023), FATF Recommendations. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, France. https://www.fatf-gafi.org/recommendations.html

FBI United States (2023). Charity and Disaster Fraud. https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/charity-and-disaster-fraud

Levi, M. (2019). *Combatting financial crimes, misconduct and mistrust in Australia: Some reflections on what criminologists can contribute*.

Levi, M. (2020). Evaluating the control of money laundering and its underlying offences: The search for meaningful data. *Asian Journal of Criminology*, *15*(4), 301–320.

Levi, M., & Reuter, P. (2006). Money Laundering. In M. Tonry (Ed.), *Crime and Justice: A Review of Research* (Vol. 34, pp. 289–375). University of Chicago Press.

McKinsey & Company (2021). Building from purpose: Unlocking the power of Australia's not-for-profit sector. https://www.mckinsey.com/au/our-insights/building-from-purpose-unlocking-the-power-of-australias-not-for-profit-sector

Mitchell, A., P. Sikka, & H. Willmott (1998). Sweeping it under the carpet: The role of accountancy firms in money laundering. *Accounting, Organizations and Society*, 23(5–6), 589-607.

National Crime Agency. (2022). Suspicious Activity Annual Report. United Kingdom Financial Intelligence Unit.

Price Waterhouse Cooper (2022). Perpetual KYC: A new approach to periodic reviews. https://www.pwc.com/sg/en/consulting/assets/pkyc-a-new-approach-to-periodic-reviews.pdf

Productivity Commission (2020), Regulatory Technology, Information Paper.

Sydney Morning Herald (2021) Absolutely fundamental': Financial crime skills shortage sparks calls for law change , article published July 1 2021, accessed at: https://www.smh.com.au/business/banking-and-finance/absolutely-fundamental-financial-crime-skills-shortage-sparks-calls-for-law-change-20210630-p585ii.html

The Treasury, Australian Government (2017). Review of Australian Charities and Not-for-profits Commission (ACNC) legislation. https://treasury.gov.au/consultation/c2017-t246103

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*, 1–35.

USAID. (2005). *Tools for Assessing Corruption & Integrity in Institutions: A Handbook*. USAID.

GRIFFITH UNIVERSITY
QUEENSLAND AUSTRALIA

CRICOS: 00233E | TEQSA: PRV12076

griffith.edu.au

MAKE IT MATTER