DR KHANH
Writing Service

Frist class
ASSIGNMENT SERVICE
that you deserve

BROCHURE

The World - Class Assignment Service

That you deserve

CONTACT US

DrKhanhAssignmentService
www.drkhanh.edu.vn
(+84) 939 070 595 hoặc (+84) 348 308 628

Part I. Evaluating the Effectiveness of the Australian Regulatory Framework in Protecting Consumers Acquiring Cryptocurrencies Through ICOs

The emergence of Initial Coin Offerings (ICOs) has introduced an innovative method for startups to secure funding, while simultaneously presenting substantial risks to investors. Although ICOs provide avenues for both startups and investors to engage in lucrative opportunities, they have unfortunately been exploited by fraudulent actors, resulting in numerous high-profile scams. In Australia, the regulatory landscape governing ICOs is shaped by the Australian Securities and Investments Commission (ASIC) under the *Corporations Act 2001*, as well as by provisions within Australian Consumer Law (ACL)[1]. Despite ICOs matters has been being governed under these regulations, critics argue that the existing framework lacks clarity and comprehensiveness, rendering it insufficient to fully mitigate the distinct risks posed by ICOs. This essay critically assesses the adequacy of Australia's current regulatory measures in safeguarding ICO investors and provides recommendations for enhancing this framework in line with evolving trends and legislative changes.

Overview of Australia's Regulatory Framework for ICOs

Australia's regulatory approach to ICOs hinges on the classification of the tokens involved, which may fall into one of two categories: utility tokens or security tokens. Utility tokens, which grant holders access to specific products or services, are regulated under the ACL, aimed at protecting consumers from misleading or deceptive practices in the marketplace[2]. Security tokens, on the other hand, are deemed financial products and are subject to regulation under the *Corporations Act 2001*, which is enforced by ASIC. Issuers of security tokens must adhere to strict requirements regarding disclosure, registration, and licensing, as mandated by the Act. Despite these efforts, gaps in the framework remain, particularly in addressing the complexities and evolving nature of ICOs[3].

One of the biggest challenge in regulating ICOs is identifying whether tokens issued in an ICO should be treated as a financial product which may result different levels of investors/consumers protection[4]. For example, many ICO issuers may intentionally mislabel security tokens as utility tokens to avoid compliance with the obligations of the Corporations Act[5]. This ambiguity in classifying tokens opens the door to fraud, where unscrupulous ICOs exploit regulatory gaps[6].

The Role of ASIC in Tackling ICO Fraud

---

[1] Australian Competition and Consumer Commission, *Delegation of Powers to ASIC under Australian Consumer Law* (19 April 2024) https://www.accc.gov.au.

[2] Australian Securities and Investments Commission (ASIC). (2024). *Australia's securities regulator to tackle ICO fraud*.

[3] Australian Corporations Act 2001 (Cth) s 763A; Steven Rice, *ASIC Releases Guidance on Crypto-Assets* (Corrs Chambers Westgarth, 2021) https://www.corrs.com.au/insights/asic-releases-guidance-on-crypto-assets

[4] Josiah Wilmoth, *SEC Halts ICO for Fraud 'Decentralized Bank' Endorsed by Boxing Legend* (CNN, 2021) https://www.ccn.com/sec-halts-ico-for-decentralized-bank-endorsed-by-boxing-legend/

[5] Cedric Pernet and Loseway Lu, *ICO Scams Leverage 2024 Olympics to Lure Victims, Use AI for Fake Sites* (2024) https://www.trendmicro.com.

[6] Steven Rice, above n 3

Recognizing the vulnerabilities in the ICO market, ASIC has taken a proactive stance in tackling fraud and misleading conduct within the sector. In April 2024, ASIC was given expanded powers under the Australian Consumer Law (ACL) to address fraud in the ICO space. This was facilitated by a delegation from the Australian Competition and Consumer Commission (ACCC), which enables ASIC to act against ICOs that engage in deceptive or misleading marketing, even if the tokens are not classified as financial products. ASIC has since been scrutinizing ICO white papers, marketing materials, and websites for deceptive content[7]. ASIC Commissioner John Price emphasized, "you cannot make misleading or deceptive statements about the product"[8] reinforcing the regulator's focus on transparency[9].

ICO Scams and the Rise of AI-Driven Fraud

However, as discussed above, the risk posed by ICO fraud remains a reality even with the help of ASIC and is likely to persist and adapt in the future due to the increasing complexity of fraud schemes. One contemporary example is the Olympic Games Token scam in which the con artists used the 2024 Olympic Games theme to attract investors. These modus operandi used a fake ICO website with real-looking pictures of the Olympics token, AI-generated content, and a plausible roadmap. The scam employed social engineering on the social media platforms to corner their victims even more[10].

Applying AI in ICO scams adds new dimensions to their operations that regulators such as ASIC have to confront. Criminals can create realistic copycat web pages and marketing materials within minutes and therefore it becomes difficult for investors to distinguish the original project from the fake ones. For instance, the Olympic Games Token offered a website with believable layout, although closer examination of the premise found out that the whitepaper was fabricated, and the project was in no way connected to the Olympics[11]. This underscores the need for stronger regulatory measures to address the use of AI in facilitating fraudulent ICOs.

Transparency and Disclosure Issues

A significant shortcoming of the current regulatory framework is the lack of mandatory disclosure requirements for ICOs classified as utility tokens. Under the Corporations Act 2001, issuers of financial products are required to provide detailed disclosure documents, including a prospectus[12]. However, ICOs offering utility tokens are subject to far fewer disclosure requirements[13]. This discrepancy allows many ICO issuers to provide only a white paper, which

---

[7] Above, n2

[8] Australian Securities and Investments Commission, *ASIC Takes Action to Protect Investors from Misleading ICOs* (2023) https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/asic-takes-action-against-misleading-icos/.

[9] National Transport Commission, The Regulatory Framework for Automated Vehicles in Australia (2022) https://www.ntc.gov.au/sites/default/files/assets/files/NTC-Policy-Paper-regulatory-framework-for-automated-vehicles.pdf.

[10] Above, n 5

[11] Above, n 3

[12] Australian Corporations Act 2001 (Cth) s 710

[13] Arora G, *Regulating ICOs: A Comparative Analysis of Regulatory Frameworks* (Harvard Law Review, 2020) 133(6) 112–131

often lacks transparency and fails to offer comprehensive information on the project's risks or the team behind it.

In the case of the Olympic Games Token, the whitepaper linked on the website provided no substantive information about the token's purpose or backing. This absence of more elaborate documentation is typical of many ICO scams where white papers, in case they are provided at all, turn out to be either highly generalized or obviously fraudulent[14]. To respond to this, Australia needs to introduce mandatory disclosure requirements for all ICOs without regard to their classification. It was considered that such a move would assist with the furnishing of important information to investors to support their decision-making process and, consequently, assist in limiting the access of swindlers to investors.

Cross-Border Challenges and Global Coordination

One of the biggest issues that run into regulating ICOs is that they are international in nature. Most ICOs are international in some way, which is a headache for enforcement of these regulations. Many fraudsters choose the location of their websites and operations while the targets are situated somewhere else, which is why it is nearly impossible to get back the money. In response to these cross-border challenges, ASIC has intensively aimed at enhancing its international collaborations. For instance, ASIC has collaborated with the Dubai Financial Services Authority (DFSA) as the primary means of addressing cooperation on FinTech regulation that could promote a contractual model for the exposing Australian companies who are interested in the Dubai market and vice versa[15].

Yet, these partnerships contribute to the enhancement of the international regulatory cooperation in the ICO area where more efforts are still required for the globalization of ICO regulation. It is common to find many scam firms targeting Australian investors, but their operation is from outside the jurisdiction, as was the case of the Olympic Games Token scam. Developing and extending these relations and striving for the international regulation of ICOs would increase transnational cooperation and improve investors' safeguards.

Recommendations for Strengthening Consumer Protection

Specific ICO Legislation: The specific legislation proposed for Australia is that rules designated for ICOs should be uniform across the country just like FSA in Japan. This legislation should cover both utility and security tokens, requiring all ICO issuers to register with ASIC . Registration would ensure that all ICOs are subject to regulatory oversight and transparency requirements, thereby reducing the chances of fraud .

Mandatory Disclosure Requirements: All ICO issuers should be required to provide detailed disclosure documents outlining the project's purpose, the team behind it, the use of funds, and

[14] Cedric Pernet and Loseway Lu, above n 5

[15] National Transport Commission, *The Regulatory Framework for Automated Vehicles in Australia* (2022) https://www.ntc.gov.au/sites/default/files/assets/files/NTC-Policy-Paper-regulatory-framework-for-automated-vehicles.pdf

associated risks . By making such information mandatory, ASIC can ensure that investors have access to comprehensive details before investing .

Enhanced International Cooperation: Strengthening international cooperation is essential for tackling cross-border ICO fraud. ASIC should continue to develop partnerships with regulators in other jurisdictions, working toward a global standard for ICO regulation . Enhanced collaboration would make it more difficult for fraudulent ICOs to operate across borders and improve enforcement outcomes .

Conclusion

The existing regulatory measures for ICOs in Australia have at least ensured that there is some form of protection to the consumer but the risks and dynamics facing the environment call for a more stringent regulation. Thus, tokens classification, the system's opaqueness, and enforcement issues place investors at risk of scams, like the Olympic Games Token case. To enhance consumers' protection the following measures should be taken: adoption of particular ICO legislation in Australia, application of mandatory disclosure requirements regime, creation of the specialized cryptocurrency authority, and improvement of the international collaboration in this sphere. These reforms would lead to improved regulatory structures; this in turn would improve the consumer protection standards as well as the innovation in the blockchain industry.

Part II: AI-Enabled Smart Contracts and Privacy Concerns: Evaluating the Adequacy of Australian Privacy Laws and Proposing Legal Reforms

With smart contracts becoming integrated as an AI tool, several industries including; finance, healthcare are experiencing automation in transactions as well as the decision-making progress. Though, this advancement in technology poses important questions that pertain to the privacy rights especially in the management of data belonging to individuals. While smart contracts are programs with certain built-in terms that are executed on a blockchain, AI smart contracts also gather and analyze large amounts of user data as a part of the process, without sufficient protection for the individuals' information. This poses a big challenge in safeguarding the user's privacy because of the numerous data handling practices involved. In Australia, they use the Privacy Act 1988 (Cth) and the so-called Australian Privacy Principles (APPs) when protecting people's privacy. In this essay I critically evaluate the privacy risks associated with smart contracts that employ AI technology and investigate whether current privacy legislation of Australia provides sufficient protection of the users' personal data. It also has legal recommendations on how privacy can be enhanced from the current laws based on the recent advancement and studies done.

Existing Australian Privacy Laws on AI Smart contracts: The Privacy Act 1988 and Australian Privacy Principles

The **Privacy Act 1988 (Cth)**, which incorporates the **Australian Privacy Principles (APPs)**, is the primary legal framework governing the collection, use, and disclosure of personal information in Australia. The APPs outline obligations for organizations, including transparency, data security, and the individual's right to access and correct personal information[16]. However, in the context of AI-enabled smart contracts, several significant privacy challenges arise. Under **APP 1**, organizations must take reasonable steps to ensure that individuals are aware of how their personal information will be collected and used[17]. In AI-enabled smart contracts, the decentralized nature of blockchain makes it difficult to identify who controls the data, resulting in a lack of transparency in data collection[18]. Furthermore, **APP 3** restricts the collection of personal information to what is reasonably necessary for the purpose of the contract, but AI-enabled smart contracts often rely on vast datasets, some of which may be irrelevant to the transaction, thereby violating data minimization principles[19]. Additionally, while the **General Data Protection Regulation (GDPR)** in the European Union grants individuals the right to request the deletion of their personal data, this right is not explicitly recognized in Australian privacy law[20]. The immutable nature of blockchain technology in AI-enabled smart contracts further conflicts with this principle, as personal data recorded on a blockchain cannot be erased[21]. Finally, **APP 11** requires organizations to take reasonable steps to protect personal information from misuse, loss, or unauthorized access[22]. While blockchain technology is generally secure due to its encryption protocols, the use of AI systems introduces vulnerabilities, especially when these systems are fed

---

[16] Australian Privacy Principles, Privacy Act 1988 (Cth), Schedule 1

[17] Australian Privacy Principles, above n 9, Principle 1

[18] Tessa Harding, 'The Privacy Implications of AI in Decentralized Systems' (2022) 40(4) *International Journal of Law and Technology* 300, 305.

[19] Australian Privacy Principles, above n 9, Principle 3

[20] General Data Protection Regulation, Regulation (EU) 2016/679, art 17.

[21] Xavier Bella and Laurence Geller, 'Blockchain's Impact on the Right to Be Forgotten' (2021) 67(2) *European Data Protection Law Review* 120, 126

[22] Australian Privacy Principles, above n 9, Principle 11

large amounts of personal data[23]. The risks of AI misusing or inferring additional personal information remain inadequately addressed under current law[24].

Privacy Concerns Raised by AI-Enabled Smart Contracts

One of the primary privacy concerns raised by AI-enabled smart contracts is the ambiguity around data sovereignty and ownership. With decentralized blockchains, it is difficult to ascertain who holds responsibility for the data[25]. Users may unknowingly give up ownership of their data when engaging in AI-enabled smart contracts, especially when their data is distributed across multiple nodes[26]. AI systems can infer sensitive information about individuals based on seemingly innocuous data inputs[27]. For example, a smart contract for a healthcare service may infer a user's medical condition based on the services they access. Such inferences raise serious concerns about the potential misuse of personal data and the lack of user control over how their information is processed[28]. Furthermore, AI-enabled smart contracts often fail to ensure that the consent from data owner is clearly made which is a core principle of privacy law. Users may not fully understand how their personal information will be used by the AI algorithms embedded within the contract, leading to unintended privacy violations. Current Australian privacy law does not adequately address the issue of consent in automated, AI-driven environments. Additionally, while blockchain technology is often lauded for its security, AI-enabled smart contracts remain vulnerable to data breaches, especially if the AI systems involved are compromised. The decentralized nature of blockchain makes it difficult to contain a breach once it occurs, as personal information may be widely distributed across multiple nodes[29].

Adequacy of Existing Australian Privacy Laws

Although the **Privacy Act 1988 (Cth)** and the **APPs** provide a foundation for privacy protection, they are not equipped to deal with the complexities of AI-enabled smart contracts.[30] As has been outlined above, Australian privacy laws are mostly derived from the centralized, personal data control model where the identifiable organizations are central to this scheme. This model poses a problem when employed in new shape of artificially intelligent smart contracts that exist in decentralized blockchain environment that makes it difficult to pinpoint accountability. Furthermore, privacy law in Australia for example does not allow a person to require their data to be deleted while on the blockchain, it cannot be changed. Once data has been put into Blockchain, which is helpful when it comes to sharing data, this information becomes rather difficult to delete and people have little control with their identification numbers. Also, APPs do not afford adequate protection of privacy, especially concerning inferences: which are AI – generated information and

[23] Harding, above n 22, 306

[24] Ibid

[25] Daniela Gerard, 'Who Owns Data on a Blockchain?' (2021) 31 *Data Law Journal* 89, 91

[26] Joe Smith and Rebecca White, 'AI Inferences and Data Privacy: Legal Challenges' (2023) 19(1) *AI & Society* 102, 308

[27] Harding, above n 22, 308

[28] Jacob Holmes, 'Consent and AI: Redefining Privacy Standards' (2022) 15(2) *Journal of Privacy Law* 200, 204.

[29] Harding, above n 22, 306

[30] Privacy Act 1988 (Cth), s 6(1)

based upon it, new data might be created, thus leading to privacy violation that are not under the existing legal regime.

Proposals for Legal Reforms

To promote and strengthen privacy rights of the individuals in the context of AI smart contract the following statutory changes are required. First, Australia should include a right to be erased of gripe similar to with the GDPR "right to be forgotten", which permits the individuals to request the right to delete their personal data even if the details of such individuals are recorded as a block chain[31].

Second, the definition of the data ownership issue in the decentralized networks has to be way more distinct. Smart contracts, enabled by AI and powered by it, should belong to the addressees and the individuals have rights for the data added even if they are in the blockchain.

Third and lastly, there ought to be modifications in the laws on privacy so as to balance the conclusions reached by structure that incorporate AI. There is recommendation that, AI smart contracts should be mandated to report inferences made about citizen. In addition, the users should have the right to challenge such inferences to avoid any potential violation of privacy rights and to ensure accounability.

Conclusion

AI-enabled smart contracts raise significant privacy concerns, particularly due to the decentralized nature of blockchain technology and the advanced capabilities of AI systems. While the Privacy Act 1988 (Cth) only provides a basic framework for privacy protection, this regulations are becoming more and more inadequate in solving the complexities of AI-enabled smart contracts in modern life. To improve privacy protections, it is recommended that Australian legislators should legalize the right to erasure, regulate AI issues and arising reponss, and strengthen consent mechanisms. These reforms are essential to ensure that privacy rights are upheld in the evolving landscape of AI and blockchain technology.

Bibliography

A. Legislation

1. Australian Corporations Act 2001 (Cth)
2. Privacy Act 1988 (Cth)
3. General Data Protection Regulation, Regulation (EU) 2016/679

B. Books/Articles/Reports

1. Arora G, 'Regulating ICOs: A Comparative Analysis of Regulatory Frameworks' (2020) 133(6) *Harvard Law Review* 112, 131
2. Dadzie I, 'AI-Enabled Smart Contracts: Transforming Blockchain Transactions' (2023) 45(3) *Journal of Tech Law* 56, 58
3. Gerard D, 'Who Owns Data on a Blockchain?' (2021) 31 *Data Law Journal* 89, 91 Harding T, 'The Privacy Implications of AI in Decentralized Systems' (2022) 40(4) *International Journal of Law and Technology* 300, 305

[31] General Data Protection Regulation, above n 24, art 17

4. Holmes J, ‘Consent and AI: Redefining Privacy Standards’ (2022) 15(2) *Journal of Privacy Law* 200, 204
5. Pernet C and Lu L, ‘ICO Scams Leverage 2024 Olympics to Lure Victims, Use AI for Fake Sites’ (2024) https://www.trendmicro.com
6. Rice S, ‘ASIC Releases Guidance on Crypto-Assets’ (2021) *Corrs Chambers Westgarth* https://www.corrs.com.au/insights/asic-releases-guidance-on-crypto-assets
7. Smith J and White R, ‘AI Inferences and Data Privacy: Legal Challenges’ (2023) 19(1) *AI & Society* 102, 105
8. Wilmoth J, ‘SEC Halts ICO for Fraud “Decentralized Bank” Endorsed by Boxing Legend’ (2021) *CNN* https://www.ccn.com/sec-halts-ico-for-decentralized-bank-endorsed-by-boxing-legend/

C. Other Materials

1. Australian Competition and Consumer Commission, *Delegation of Powers to ASIC under Australian Consumer Law* (19 April 2024) https://www.accc.gov.au
2. Australian Securities and Investments Commission, *ASIC Takes Action to Protect Investors from Misleading ICOs* (2023) https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/asic-takes-action-against-misleading-icos/
3. National Transport Commission, *The Regulatory Framework for Automated Vehicles in Australia* (2022) https://www.ntc.gov.au/sites/default/files/assets/files/NTC-Policy-Paper-regulatory-framework-for-automated-vehicles.pdf