We provide a Safe, Easy, and Secure insurance protection for user's digital assets in the blockchain NFT space.

TOKEN MAPPING CONSULTATION, AUSTRALIAN GOVERNMENT, THE TREASURY. REQUEST FOR FEEDBACK AND COMMENTS

Introduction

The crypto ecosystem has been a subject of great interest in recent years, with the rise of cryptocurrencies and blockchain technology. The role of government in the regulation of this ecosystem is important, as it affects the functioning, safety, and stability of the crypto market. Supporting government intervention, crucial safeguards for consumers and investors also play a crucial role in the growth of the crypto market. Criminal activity including scams in the crypto market continues to rise as do the challenges faced by consumers in identifying them is also a significant concern.

This introduction sets out the questions that will be discussed in detail, including the role of the government, consumer protections, scam prevention, definition of crypto assets and networks, taxonomy, intermediated crypto assets, identification of intermediated token systems, financial products, public crypto networks, investment restrictions, marketing and promotion, smart contract development, smart contract applications and consumer outcomes. The purpose of this discussion is to understand the key challenges and opportunities in the crypto ecosystem and the role of government and other stakeholders in promoting a safe and secure environment for consumers and investors.

The Role of Government in the Regulation of the Crypto Ecosystem

The crypto ecosystem has grown rapidly in recent years and has become a significant part of the financial landscape. To ensure the stability, security and reliability of this system, the role of government in regulation is critical. The government can play a role in creating a framework that provides clarity and stability, while still allowing innovation and growth to continue.

In terms of regulation, the government should aim to establish a clear and comprehensive legal framework that defines the rights and obligations of all parties involved. This includes rules around the use of crypto assets, their creation, distribution, and trade, as well as the obligations of exchanges and other intermediaries.

The government should also work to establish a regulatory regime that is flexible enough to adapt to changes in the crypto ecosystem, but strong enough to protect consumers and investors. Areas of interest and develop include:

1. Regulatory oversight: Governments have a responsibility to protect their citizens from fraudulent or illegal activities. NFTs operate within decentralised ecosystems, which makes it difficult for governments to monitor and regulate these activities. Governments may be concerned about the lack of oversight and the potential for abuse within these systems. Currently, there is little to no regulation around the use and trading of NFTs. This lack of regulation may leave governments concerned about the potential for fraudulent or illegal activities such as money laundering, tax evasion, and other financial crimes. NFTs can be used to transfer value across borders without going through traditional financial channels. This can make it difficult for governments to track money laundering and tax evasion activities.
2. Investor protection: NFTs are often sold as investment opportunities. Governments may be concerned that these investments are not properly regulated or that investors are not adequately informed about the risks involved.
3. Intellectual property rights: NFTs are often used to represent digital art, music, or other creative works. Governments may be concerned about the implications of these assets for intellectual property rights and the potential for piracy or infringement.
4. Taxation: NFTs continue to gain popularity and value, governments may be concerned about their ability to tax transactions involving them. It can be challenging for governments to track and tax digital assets effectively, which could lead to significant revenue losses.

5. Consumer protection: Governments may worry about the potential for consumers to be taken advantage of in the unregulated market for NFTs. Investors may not fully understand the risks involved or the true value of these assets, which could lead to financial losses.
6. Environmental concerns: Some NFTs are built on blockchain technology, which requires a significant amount of energy to operate. As governments continue to focus on environmental issues, they may be concerned about the carbon footprint of these digital assets.

Currently, there is no consensus among governments regarding the regulation of digital assets. Some countries have taken a proactive approach and have established legal frameworks to regulate the use of digital assets, while others have taken a wait-and-see approach.

Intermediated crypto assets, also known as "wrapped" real-world assets, have gained increasing popularity as a new form of investment and value exchange. However, the regulatory frameworks surrounding these assets are diverse and vary from country to country, with some nations imposing restrictions on their issuance on certain public crypto networks. This raises the crucial question of determining the suitability of a particular public crypto network for hosting wrapped real-world assets in Australia.

When considering the suitability of a public crypto network, several factors must be considered. The first is evaluating the network's security and reliability, which involves examining the underlying technology, such as the consensus mechanism used for validating transactions, and ensuring that sufficient measures are in place to prevent hacking or fraud.

Scalability is another crucial aspect to consider. This includes evaluating the network's ability to handle a high volume of transactions and whether it has the capacity to accommodate the growing demand for crypto assets.

The governance structure of the network is another critical factor to consider. This involves evaluating the decision-making role of stakeholders, dispute resolution processes, and the accountability of network participants.

Finally, the regulatory environment for crypto assets in Australia must be considered. This involves assessing the regulatory framework for crypto assets, such as licensing requirements and disclosure obligations, and ensuring that the network complies with these regulations.

While intermediated crypto assets offer consumers new investment opportunities, they also pose potential risks. These assets are often complex and may not be transparent, leaving consumers vulnerable to fraud and mismanagement. As a result, it may be necessary to impose restrictions or frictions on investment in these assets to mitigate these risks. For instance, intermediaries may be required to provide clear and concise information to consumers about the underlying arrangements, including any risks involved, and obtain a license from ASIC with strict disclosure and reporting requirements.

Limiting the amount of investment in these assets could also help reduce the risks associated with them while still allowing consumers to access new investment opportunities. However, it is essential to ensure that these limits do not restrict access to these assets excessively, as this could have negative consequences for consumers and the economy.

Potential Steps

7.

a. Existing regulation needs to be reformed to ensure it is relevant for wrapped real-world assets. Relevant laws should ensure digital assets are subject to the same regulatory requirements as the underlying asset they represent in a manner such that the digital asset is able to accurately reflect the intrinsic value and characteristics of the real world asset, to thereby foster trust in the purchasing party.

Stablecoin assets should be treated by the law in the same manner that the underlying currency is when held in financial institutions. A reasonable level of collateralization is necessary to ensure the crypto asset can be redeemed 1:1 for its underlying asset always and not be vulnerable to supply-demand fluctuations. Legal frameworks that apply to transfer of cash, such as KYC and AML, should apply in the same manner. The stablecoin itself must be strictly a product that uses crypto networks and smart contracts to automate existing business protocols without the need for a trusted third party: an asset that provides instrumental value in the settlement of payments but does not promise future returns derived from the efforts of others.

Intermediated crypto assets that represent real world assets such as real estate, luxury goods, memberships, etc. only need moderate regulation that ensures the holder of the digital asset can easily confirm the asset represents its physical counterpart. This can be achieved through establishment of standards to link the physical asset to the digital representation with NFC chips.

Crypto assets that represent securities, such as bonds, debts, and debentures, should be subject to the same regulations that govern the securities markets.

b. To ensure issuers of wrapped real-world assets can meet their obligations to redeem the relevant crypto tokens, certain reforms are necessary according to the type of asset.

For stablecoin assets, legal frameworks need to exist to ensure that the asset is adequately collateralized so that the underlying currency is able to meet demand for redemptions without significant fluctuations in value. Asset issuers should be obligated to model out redemption scenarios and undergo stress testing to ensure that the digital asset does not fluctuate by more than a particular benchmarked percentage rate as dictated by regulation. Collateral liquidity needs be regularly audited by independent third parties and quarterly reports issued to provide full transparency and assure market participants that their assets are secure.

c. For intermediated crypto assets that represent real world assets, a clear link needs to be established between the digital and the physical asset that can be proven without reasonable doubt. There is yet to be a failsafe method to prove this link as existing digital assets simply represent claims for the physical, but early technological primitives are emerging that link the physical asset programmatically to the digital through the usage of NFC chips. Government regulation should require all high value assets to be linked and audited to mitigate risk of fraud.

For crypto assets that represent securities, a suitable redemption mechanism would ensure that no other claim can be made on the digital token once the asset holder chooses to redeem it. This can be ensured through programmatically restricting redemption to legal entities, which are registered on the blockchain as the legal holders of the security.

8.

d. Crypto asset service providers must be required to provide their users with access to all non-sensitive information that enables them to identify arrangements underpinning crypto tokens.

For custodial services, such as centralized exchanges, this must be disclosed as Proof of Reserves. Exchange reserve balances need to be transparently disclosed so that users have confidence whilst interacting with their products and services. Third-party auditors such as Chainlink and Hacken can verify balances are equivalent to customer deposits. This ensures that during periods of stress, the exchange does not become insolvent as FTX did in November 2022.

For on-chain custodial services, such as wBTC, the terms of the arrangement are evident through examination of smart contracts and custodian balances on the blockchain. When a user wishes to interact with wBTC, the underlying asset, BTC, is held in a custodial wallet 1:1 to create wBTC, and then redeemed when the wBTC is returned. Proof of Assets are publicly verifiable through viewing on-chain balances of custodian addresses.

When dealing with sensitive information, such as personal holder details for securities tokens, this data can be provided discreetly with the usage of zero-knowledge proofs, which is a method of providing proof the required information exists without disclosing the information itself. This is a critical aspect of maintaining privacy of sensitive information on otherwise open blockchains.

e. One of the most important initiatives that crypto asset service providers can undertake is education of how assets are secured to foster consumer trust. Once relevant regulations are in place to ensure that consumer assets are backed adequately, consumers need to be informed exactly how these assets are backed and how the redemption process occurs to convert back to the underlying asset. Further, consumers need education on how intrinsic value of a crypto asset is determined and how the instrumental value is applied, if relevant.

9.

a. Intermediated crypto assets that represent existing financial products, such as stablecoins or bonds, should be defined as financial products since they promise redemptions 1:1 for the underlying asset.

Intermediated crypto assets that do not represent existing financial products, such as memberships, event tickets, or collectibles, should not be defined as financial products since these assets simply represent digital claims on the physical counterpart.

Token mapping regarding how assets are categorized is critical to ensure regulation does not stifle business activity.

b. Intermediated crypto asset services that promise future returns need to be defined as financial products because they resemble traditional financial services. Some examples include payment services, custodial services, asset exchange services, and leveraged trading services. Regulation of these services is important to ensure that consumers are protected against misrepresentation of services or fraudulent activity.

10. For a crypto network to be deemed suitable for hosting intermediated crypto assets, the network needs to be as a minimum sufficiently decentralized to prevent collusion amongst validators and secure enough to mitigate risk of exploitation at the base layer and manipulation of asset value. Scalability is important but this can be addressed through layer 2 solutions that use optimistic or zero-knowledge rollups to provide users with affordable and fast transactions without compromising the security of the base layer.

11. Decentralization can be quantified by using the Nakamoto Coefficient, a measurement of the minimum number of nodes a malicious actor would have to control to disrupt the blockchain's network. It is also important to ensure that nodes are not able to collude through off-chain coordination.

Security of a blockchain can be determined by its network effects. Blockchains with higher market caps have higher levels of security than those with lower as more participants means that there is greater distribution of assets and therefore a lower chance of a malicious participant being able to take advantage of the underlying consensus algorithm that secures the network.

12. Limits, restrictions, or frictions on the investment by consumers should not be imposed on intermediated crypto assets in relation to any arrangements not covered already by the financial services framework because the crypto assets are simply digital versions of the underlying assets. Imposing further restrictions would not only hinder further development of business activity and innovation in Australia but also would encourage market participants to migrate to crypto friendly jurisdictions.

Safeguards for Government, Consumers, and Investors

One solution to improve transparency in the cryptocurrency ecosystem is code auditing, which evaluates the code used to create a cryptocurrency to ensure it is secure and free from vulnerabilities. This gives consumers and investors a greater level of assurance that their funds are safe and secure.

Insurance protection can play a significant role in protecting consumers and investors from potential financial losses. By reducing risk and increasing transparency, insurance protection helps to mitigate the financial impact of events such as theft, hacking, or fraud. It also encourages investment and boosts confidence in digital tokenised assets, contributing to the growth and development of the digital asset ecosystem.

Conclusion

In conclusion, insurance protection is a crucial aspect in safeguarding the investments of consumers and investors in the fast-growing digital asset ecosystem in Australia. The Australian government should take a proactive approach in addressing the challenges posed by digital tokenised assets by establishing a clear regulatory framework that ensures transparency, security, and stability, while still fostering innovation and growth. The implementation of licensing requirements, consumer education, and code auditing can prevent fraudulent activities and protect consumers and investors.

Moreover, the government must assess the suitability of public crypto networks and enforce necessary reforms for intermediated crypto assets, ensuring equitable treatment and protection for investors. The balancing act between regulation and access should prioritize consumer and investor protection while supporting the economic growth of the country. By considering insurance protection as part of their investment strategy, consumers and investors can have peace of mind knowing their assets are protected from potential losses.