Australian Government: Token mapping

About nChain

nChain is a global tech company offering software, IP licensing, consulting services and providing blockchain solutions and products. Founded in 2015, nChain advances the potential of blockchain technology through ongoing research and development of patentable inventions and by offering commercial solutions. With one of the largest portfolios of IP and research related to blockchain, we are uniquely positioned to support the Australian Government and the Treasury in its interaction with the ecosystem.

Q1) What do you think the role of Government should be in the regulation of the crypto ecosystem?

1. nChain agrees with the Consultation paper's roles set out in paragraph 11 (providing governing structures for rules, standards, and measures) and supports efforts to improve and refine those structures. nChain strongly supports Government's role in protecting property rights as a foundation for trust, stability and competitive ecosystems that generate trade, innovation, and growth.

   To fulfil these roles in the 'crypto ecosystem' we suggest it is critical for Government – including state and federal police, treasuries, courts, agencies, regulatory bodies, etc. – to understand and consider the following.

1.1. **Terms like 'crypto' risk confusing legal concepts and frameworks**

   We suggest the term 'crypto' has negative connotations both in and outside of the ecosystem that implies the speculative aspects and may create confusion, hesitancy, or resistance to enforce laws. Such connotations also

risk ignoring the public utility of the blockchain as a breakthrough technology for powering new, diverse, and secure applications. We suggest distinguishing between 'crypto' as tools for speculation or confusion and the blockchain as a public utility for immutable recordkeeping.

1.2. Misuse of 'decentralization'

We suggest 'decentralisation' has been misinterpreted in ways that confuse and undermine accountability and state sovereignty. It is a mistake to think that as blockchain-based systems are decentralised, they can operate outside of the law.

The purpose of Baran's 'decentralised' communication network in 1964 was to deliver a more resilient and reliable communications network with no single point of failure. Baran's diagram of 'centralized', 'decentralized' and 'mesh' networks was used to improve understanding of service "survivability" (see Baran, P. (1964). On Distributed Communications Networks. IEEE Transactions on Communications, 12(1), 1–9. https://doi.org/10.1109/TCOM.1964.1088883).

However, referring to a computer network as 'decentralized' does not make it politically or legally decentralized. Any individual, company or other legal entity that offers an immutable indexing service (as a node or transaction processor) or buys an immutable recording (on the blockchain) is a 'centralised' legal entity, embedded in a jurisdiction and subject to court orders.

It is therefore important to see the flaw in suggesting that blockchain technology does not need legal enforcement or can become an enforcement system itself as some have argued (see Bonnet, S., & Teuteberg, F. (2022). Impact of Blockchain and distributed ledger technology for the management, protection, enforcement, and monetization of intellectual property: A systematic literature review. Information Systems and E-Business Management. https://doi.org/10.1007/s10257-022-00579-y).

To summarise, Bitcoin is made up of multiple “centralized” legal entities (people, organisations such as transaction processors, etc.) that can now connect and trade with each other directly in a peer-to-peer way. Some refer to such peer-to-peer interactions as happening at the “edge” (of the network) or in a “decentralized” fashion. Exchanging peer-to-peer provides them with improved privacy, security, and efficiency compared to conducting all communications through an insecure communications channel that could leak information to unintended and unfriendly parties. After exchanging as peers, they can immutably record any details they desire associated with their exchange (whether agreements, files, etc.) or a compressed message digest of such records (using a hashing algorithm) in a single, public immutable database to prove their authenticity in the future should this be required by law enforcement. Parties transacting this way can improve and maintain privacy by using pseudonyms linked to identity, encryption, and other techniques and simplify law enforcement by using ‘country attributes’ as desired or required. These capabilities enhance system robustness, but they do not change the social commercial or legal relationships between entities.

For further reading we suggest, Papers Associated with Bitcoin and Related Topics in Law: Part I, Craig Wright, 2023 https://craigwright.net/blog/bitcoin-blockchain-tech/papers-associated-with-bitcoin-and-related-topics-in-law-part-i/.

1.3. Blockchain is a database; not a ‘new’ way of owning assets

The blockchain offers a public immutable ledger you can write to for the cost of micropayments. You can write to it to store public or private information. These features do not affect existing principles of law concerning ‘owning’ assets. Blockchain does not decentralise ownership, as ownership is not defined by the ledger.

1.4. Governments can already make orders to recover digital assets without private keys

‘Not your keys, not your coins’ is a term that is typically associated with the ‘crypto ecosystem’. However, it runs contrary to the laws of property and exchange and impedes general adoption. The mere possession of a key does not prove your ownership of a house, in the same way a ‘crypto’ (cryptographic) key does not prove your ownership of the digital asset. You own a digital asset when you have obtained it validly. If an individual can prove ownership of a digital asset within a court, then there should be mechanisms for recovering that asset.

Code is not law; law is law. Blockchain-based systems and the entities that facilitate them do not operate outside of the law. Government’s role involves enforcing both physical and digital property.

Key and asset recovery across the ‘crypto ecosystem’ is already possible and Government has an important role in facilitating such recoveries where required by law. This includes, for example, assets recoverable under court order by the police for proceeds of crime. Prior efforts across so called ‘crypto’ networks include:

a. The High Court of England and Wales’ 2023 order to ‘DeFi’ Oasis.app to, “take all necessary steps” to recover assets (see Statement Regarding The Transactions From The Oasis Multisig on 21st Feb 2023, https://blog.oasis.app/statement-regarding-the-transactions-from-the-oasis-multisig-on-21st-feb-2023/).

b. The clear articulation of this point by the Department of Justice’s manual for asset forfeiture: “Prosecutors should consult ..(OIA) regarding seizure of cryptocurrency from foreign service providers, such as institutional exchanges, even in cases where a wallet company does not itself have access to or control of the private key…” (see U.S. Department of Justice Criminal Division, Asset Forfeiture Policy Manual 2023, https://www.justice.gov/criminal-afmls/file/839521/download).

c. The Justice Department’s 2022 seizure of the world’s largest and longest running darknet market, Hydra Market (see DoJ, Justice

Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace, https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace).

d. Efforts by authorities spanning 17 countries in 2013 to shut down digital currency service Liberty Reserve for money laundering and operating an unlicensed financial services company (see DoJ, Charges Against Liberty Reserve, One Of World's Largest Digital Currency Companies, And Seven Of Its Principals And Employees For Allegedly Running A $6 Billion Money Laundering Scheme https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-liberty-reserve-one-world-s-largest).

Large public facing custodians of digital assets (exchanges and wallets) are increasingly appreciating government compliance and enabling court mandated asset recoveries. However, illicit activity also operates at the base token or blockchain layer. As discussed in 1.2, Government can address this with court orders to node operators that directs them to comply with ownership and proceeds of crime requirements. Software already exists for court enforcement at the blockchain layer for asset freezing and recovery (see Coingeek, 2022, Blacklist Manager: An innovation software solution to help retrieve stolen or lost digital assets https://coingeek.com/blacklist-manager-an-innovation-software-solution-to-help-retrieve-stolen-or-lost-digital-assets/).

1.5. Enforcing existing laws and regulatory frameworks

In a recent interview, SEC Chair Gary Gensler implied the SEC had all the tools it requires to address 'crypto', stating:

> "Everything other than bitcoin…you can find a website, you can find a group of entrepreneurs, they might set up their legal entities in a tax haven offshore, they might have a foundation, they might lawyer it up to try to arbitrage and make it hard jurisdictionally or so forth… They might drop their tokens overseas at first and

> contend or pretend that it's going to take six months before they come back to the U.S.… But at the core…these tokens are securities because there's a group in the middle and the public is anticipating profits based on that group" (see NYMagazine, 2023, Can Gary Gensler Survive Crypto Winter? D.C.'s top financial cop on Bankman-Fried blowback, https://nymag.com/intelligencer/2023/02/gary-gensler-on-meeting-with-sbf-and-his-crypto-crackdown.html).

We suggest enforcing existing protections and frameworks that have been built over many decades of experiences around risks to investors and consumers, including:

a. Providing financial services without an Australian Financial Services License (AFSL);

b. Securities, wire, and other frauds;

c. Money laundering;

d. Misleading and deceptive conduct;

e. Breaches of sophisticated investor laws; and

f. Breaches of design and distribution obligations.

The Consultation paper mentions the most common reason for consumers buying crypto assets was 'as a gamble to make or lose money' and highlights consumer losses as an issue. However, many schemes have been allowed to continue operations despite clearly breaching securities, misleading and deceptive conduct, and other laws. FTX's collapse reinforces the importance of legal actions involving securities fraud, wire fraud, and money laundering (see SEC, 2023, SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX, https://www.sec.gov/litigation/litreleases/2023/lr25616.htm).

We also suggest continued coordinated international action against anonymous systems. For example, the UN's Office on Drugs and Crime,

warns anonymous crypto-currencies have made fighting criminals involved in global child sexual exploitation networks harder by adding a new layer of secrecy that favours criminals (ABC, Crypto-currency makes child slavery trade harder to break: UN, 2019). Untraceable 'privacy coins' such as Monero may continue to pose problems for law enforcement and empower ransomware gangs, money launderers, and the sale of guns and drugs (Financial Times, Monero emerges as crypto of choice for cybercriminals, 2021).

1.6. **Improve privacy and security standards**

Privacy presents a key driver for the adoption of digital assets. Bitcoin introduces a pseudonymous Privacy Model (see chapter 10, Wright (Pseudonym: Nakamoto, S), Bitcoin: A Peer-to-Peer Electronic Cash System (August 21, 2008) https://ssrn.com/abstract=3440802) that allows certificate authorities and new kinds of Public Key Infrastructure systems that can be combined with 'country attributes' to deliver improved privacy, security, and compliance across public and private sectors and within and between jurisdictions. For more information, see PKI in our response to Question 2 below.

However, people continue to conflate user privacy and pseudonymity with legitimate concerns over complete anonymity and illicit activity. The balance between privacy and security is an ongoing concern and governments desiring thriving economies have a role to play in ensuring value exchange can occur in ways that preserve user privacy whilst maintaining a safe marketplace.

Issues raised in the Consultation paper and elsewhere provide an important opportunity for Australia to address root cause privacy and security concerns, such as via the introduction of an internet digital bill of rights (see DeSantis 2023 https://www.flgov.com/2023/02/15/governor-ron-desantis-introduces-groundbreaking-legislation-to-protect-the-digital-rights-and-privacy-of-all-floridians/).

1.7. **Explore CBDC and improved compliance operational standards**

CBDC could address risks associated with stablecoins and help enforce financial product frameworks that threaten financial stability via programmatic enforcement.

After the introduction of peer-to-peer micropayments with Bitcoin in 2009, demand for stable, trusted, micropayment-capable fiat tokens and a lack of CBDCs to meet such demand, resulted in private sector stablecoins with market risks that have already harmed participants. For example, in 2022, the Terra stable coin lost over 90% of its value in a short period. Some have speculated that a large player caused this collapse to profit from it (WSJ, Crash of TerraUSD Shakes Crypto, 2022). Another popular stablecoin Tether, suggests the possibility of a similar crash, having first assured the market they were fully backed by USD before lowering this to 74% and then 2.9% in 2021 (Financial Times, Tether says its reserves are backed by cash to the tune of… 2.9%, 2021).

Some stablecoins and today's shadow banking system more broadly, provide little insight into the mismatch in maturity dates of assets and liabilities and the potential for a crisis. CBDC could provide an infrastructural backbone for a new era of improved governance across Australia's regulatory frameworks.

For example, the Treasury could use a CBDC or eAUD to:

a. whitelist licensed service providers, networks, or tokens;

b. implement alert keys and new direct communications to market providers and consumers (for notices, breaches, etc);

c. implement private, immutable, and automatic reporting and audits across the financial licensing, custody, and other Australian regulatory frameworks; and

d. facilitate broader innovations for Australians as we suggest in responses to later questions.

Q2) What are your views on potential safeguards for consumers and investors?

2. We suggest Australia already has well-formed investor safeguards applicable to tokens that are financial products and a well-formed consumer framework applicable to non-financial arrangements through the ACCC. If consumer safeguards are expanded for consumers, we suggest they should not overlap with existing investor protections because this would likely create confusion and conflicts.

   The introduction of the blockchain (public immutable ledger) – as expanded upon below – presents the potential for new operational or technical means of achieving safeguards for both consumers and investors. We suggest this is a significant economic, social, and geopolitical opportunity for Australia.

2.1. **Education**

Education of consumers, investors, law enforcement and service providers will continue to be a critical area, particularly in the following areas.

a. **Innovative services** – education of government and industry about operational improvements (see below) can reduce or even eliminate errors, attack vectors and frauds, thereby facilitating faster, cheaper, and more secure services for Australians.

b. **Recourse** – Informing aggrieved consumers and investors of existing safeguards and protections under Australian law can help them seek recourse and more swiftly than new regulations.

   Government can also help highlight the benefits and risks associated with the ecosystem. New education standards could also be required of licensed providers. And plain English materials using concrete examples can help simplify and explain relevant concepts. For example, holding digital assets in your digital wallet on a device can be likened to holding physical cash in your physical wallet – so consider this when making decisions about amounts and protections.

2.2. **Enforce existing safeguards – including cases where people lack private keys**

Courts and law enforcement can and already have compel developers to move assets, with or without private keys. For example:

a. In 2023, the United States Department of Justice took steps to educate law enforcement concerning seizures without private keys, stating: “Prosecutors should consult the Office of International Affairs (OIA) regarding seizure of cryptocurrency from foreign service providers, such as institutional exchanges, even in cases where a wallet company does not itself have access to or control of the private key. Seizures from foreign-located service providers will require use of a mutual legal assistance (MLA) treaty request or other similar authority” (see U.S. Department of Justice Criminal Division, Asset Forfeiture Policy Manual 2023, https://www.justice.gov/criminal-afmls/file/839521/download).

b. In 2023, the High Court of England and Wales ordered self-described ‘crypto’ and ‘DeFi’ Oasis.app to “take all necessary steps” (in this case, deploying some code) to retrieve and seize assets associated with a $140 million exploit of the Wormhole bridge (see Statement Regarding The Transactions From The Oasis Multisig on 21st Feb 2023, https://blog.oasis.app/statement-regarding-the-transactions-from-the-oasis-multisig-on-21st-feb-2023/).

c. Liberty Reserve – in 2013, authorities spanning 17 countries coordinated to shut down the digital currency service Liberty Reserve for money laundering and operating an unlicensed financial services company.

2.3. **New operational safeguards made possible thanks to the blockchain**

The introduction of the Bitcoin whitepaper in 2008, followed by the various wire, securities and other frauds associated with today’s so called ‘crypto ecosystem’, resembles the evolution of the internet and associated frauds

and unsustainable business models that collapsed in the dot-com bubble. Both the internet and Bitcoin introduced game-changing technological breakthroughs that bad actors sought to exploit.

In 2009, an Australian citizen introduced the world's first public immutable ledger network delivering micropayments with a Turing complete scripting language (Wright, Turing Complete Bitcoin Script White Paper, 2018). This breakthrough introduced a new era of innovative capabilities (not previously possible on the internet) for safeguarding consumers, investors, and other entities including government agencies (such as treasuries and tax authorities), including the following:

a. **Direct electronic exchanges** – new choice in payment options for trade. In addition to physical cash and intermediated (financial) products, people and agents may trade and pay with secure digital cash. This is a fantastic development for humanity because competition and choice have historically freed people and markets from monopolies and oligopolies, unlocking new opportunities and promoting economically thriving societies.

b. **More secure communication and oversight via a new Public Key Infrastructure (PKI)** – Australians who use today's internet applications (including search, email, banking, publishing, etc), whether individuals or military operators, can gain improved privacy, security, and real-time compliance. Service governance can advance from annual or batched checks to instant revocations of (invalid KYC, AML, CFT, or other) certificates with "9000 certificate issuances, revocations, or updates per second at a cost of less than 0.005 USD per event" (A Blockchain-Based PKI Management Framework, 2021). For example, Australians could enjoy:

    (i) **Improved AML and 'country attributes'** – today's approach to AML faces cost and effectiveness problems and has been fundamentally challenged on a cost benefit basis, prompting the question: is the existing cost

effectiveness of existing AML and compliance obligations sustainable? (See Ronald 2018, Anti-money laundering: The world's least effective policy experiment?). A new PKI infrastructure on a public blockchain could include 'country attributes' to flag various jurisdictional operations in an immutable, yet private and secure way, reducing the AML cost burden on industry whist simultaneously improving compliance and privacy.

(ii) **Improved sanctions and blacklists** – IPv6 and a novel blockchain based PKI identity system, as explored by the ESTI's Industry Specification Group (IPG) IPv6 Enhanced Innovation (IPE) could decrease costs and improve compliance (see https://www.etsi.org/technologies/ipv6-enhanced-innovations-ipe).

c. **Improved network resilience** – a single attack on today's legacy digital systems can compromise the logs and data integrity of significant economic systems running on top. For e.g.:

(i) In 2011 an attack on DigiNotar compromised the Dutch Government, Google, their users and digital records (see 2012 IT News, DigiNotar hack details revealed by Dutch Govt, Final report released)

(ii) In 2018, the TSB outage left 1.9 million without access to payments (BBC, TSB customers hit by online banking outage, 1 April 2020).

(iii) In 2018, Visa suffered their first outage in over 7 years because of a failure in their authorisation service which had an estimated economic impact on retailers approximately £105m (Based on debit card spend of £530billion a year in the UK).

By contrast, Bitcoin has had 100% uptime for over a decade and remained resistant to attack. Systems that understand and

intelligently utilise the blockchain as a public utility can gain improved availability and resilience safeguards for consumers and investors compared to legacy networks.

d. **New asset recovery systems** – Recover lost and hacked funds without relying on third parties via backups. When a wallet (including a split-key exchange wallet) is lost or stolen, a second device holding a backup can automatically transfer the funds to a safe address. For example:

   (i) Split key systems can transform and prevent exchange and custodial hacks.

   (ii) Proofs-of-reserves can combat liquidity mismatches and crises.

   (iii) Asset rehypothecation and smart securitisation systems can become more secure, compliant, and efficient.

   Also see in our response to Question 7.

e. **Improved security** – immutable logs and identity systems can reduce welfare fraud, money laundering, and shadow banking crime.

f. **Improved court enforcement** – where courts issue freezing orders, specified funds cannot be spent, allowing recovery from illicit activity.

Q3) Scams can be difficult for some consumers to identify.

Q3) a) Are there solutions (e.g., disclosure, code auditing or other requirements) that could be applied

to safeguard consumers that choose to use crypto assets?

3. nChain strongly supports government and private efforts to help consumers and economies identify and resist scams. Australia can change incentives to commit civil and criminal wrongs by adjusting penalties, rewards, and methods, including innovative approaches and increased enforcement action, particularly under the existing financial products frameworks.

   Solutions to safeguard consumers choosing to use digital assets could include the following.

3.1. **Disclosures** – are already required in financial and consumer frameworks in the form of Australia's securities laws, financial licensing requirements, misleading and deceptive conduct provisions, etc. Additional disclosures may further educate the public.

3.2. **Code insertions –** laws could require developers to insert or make available for use, code to facilitate court orders, allowing improved international coordination. Such code already exists. For example, see the Bitcoin Association's Blacklist Manager (Coingeek, 2022, Blacklist Manager: An innovation software solution to help retrieve stolen or lost digital assets https://coingeek.com/blacklist-manager-an-innovation-software-solution-to-help-retrieve-stolen-or-lost-digital-assets/).

   Some states have drafted bills to require this – for example, Illinois, USA, requiring blockchain nodes to include code to respond to court orders to move assets and funds without private keys (see FINANCIAL REGULATION (205 ILCS 730/) Blockchain Technology Act. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4030&ChapterID=20).

3.3. **Code audits** – can be introduced. However, consumers or other parties failing to check if a service has an AFSL may be unlikely to check if an appropriate audit has been done without some kind of alert key or notification service (which could also be introduced).

3.4. **Trust framework** – verified list (whitelists) of approved service providers that meet a minimum consumer standard can be updated and monitored with increasing immutability, specificity, privacy, and efficiency enabled by the blockchain.

3.5. **Improved public certification and licensing systems** – improved PKI systems (see our response to Question 2) could be utilised to introduce improved and importantly, immutable:

a. **Whitelists** – providing a public list of approved projects, functions, operators, with associated 'approved' marks or badges.

b. **Blacklists** – providing a public list of banned operators, networks, IPs, etc.

c. **Operations via hierarchical key systems** – that do not compromise privacy or require excessive overhead or delays. For example, a licensing authority can issue a child key foreach authorised entity, allowing operators to operate with privacy, in a provably licensed way, whilst also benefiting from new security advantages (see nChain 2022, The Metanet, Technical summary: A Blockchain-based Internet) including:

(i) **Improved recovery over lost funds without a third party via backups** – when a wallet is lost or stolen, a second device holding a backup can automatically transfer the funds to a safe address. Where courts issue freezing orders, specified funds cannot be spent, allowing recovery from illicit activity.

(ii) **Improved account reconciliation and automated audit services** – triple entry accounting and automatic real-time financial reporting and audits can streamline and reduce compliance burdens whilst simultaneously improving financial and cash-based exchanges transacted on the public blockchain.

(iii) **Improved law enforcement, legal and dispute resolution services** — notarisation, arbitration, and court integration services including freezing orders, thawing orders, etc.

Q3) b) What policy or regulatory levers could be used to ensure crypto token exchanges do not offer scam tokens or more broadly, prevent consumers from being exposed to scams involving crypto assets?

3.6. **All policy or regulatory levers that impact economic incentives can reduce scams**.

Criminal groups act as profit seeking enterprises. To minimize online criminal threats associated with 'crypto assets', Government can focus on minimising the economic returns from cybercrime across the board for Australian society (see Wright, Craig S, Criminal Specialization as a Corollary of Rational Choice (May 28, 2010) https://ssrn.com/abstract=3461064).

The economic rationality of criminals is likely to have significant impacts on state and non-state actors (individuals, organisations, militaries, etc) over the coming decades as systems designers begin to understand and implement new infrastructure solutions – particularly those using Bitcoin (BSV) and IPv6 – to significantly increase the cost of attacks and thereby achieve improved privacy, security, availability and cost-efficiency for the benefit of their consumers, citizens, and shareholders.

3.7. **Enforce existing laws and frameworks**

As stated in our response to Question 1, Australia's existing financial products framework covers a wide of tools for enforcement against securities fraud, misleading and deceptive conduct, wire fraud, etc. "that apply to crypto assets in Australia". We suggest Australia could be more proactive in enforcement. Enforcement could also target advertising networks that have assisted consumer scams.

Governments that do not enforce the law, undermine deterrence and signal to criminals that those who breach the law will go unpunished. The result is a lowering in the perceived cost of breaching the law, an increase in the net appeal of scams, and an eventual increase in losses for scammed consumers and investors. This pattern seems repeatedly observable in today's financial environment, spanning the dot-com bubble, the sub-prime bubble, and most recently the 'crypto' bubble.

Enforcing the law has historically been an effective tool for combatting various scams in the securities space. In some cases, enforcement has waned whilst various schemes scale and multiply until an eventual landmark or high-profile case followed by higher and more consistent standards of enforcement action against large and small offenders. Today's case against FTX and the criminal charges against FTX co-founder Sam Bankman-Fried – for securities fraud, wire fraud, multiple conspiracy counts related to wire fraud, illegal campaign contributions, money laundering, operating an unlicensed money transmitting business, and bank fraud – in time might be seen as one such example (2023 CNBC FTX founder Sam Bankman-Fried hit with four new criminal charges, https://www.cnbc.com/2023/02/23/ftx-founder-sam-bankman-fried-hit-with-new-criminal-charges.html).

3.8. **Consider new oversight and compliance capabilities**

Please also see our response to Q3.a. For example, a clearer trust framework or whitelisting policy for communicating AFSL license requirements for service providers, their listing KYC, AML and other practices, reserve transparency standards, as well as whether they implement innovative protections such as split-key systems and proofs-of-reserves for liquidity transparency. Blacklists could also help people identify scam tokens, exchanges, etc.

3.9. **Use the blockchain's immutable audit trail to increase the cost of crime and for those aggrieved, the ease of recourse**

Utilising the blockchain's immutable audit trail can disincentivise crime by increasing its costs because offenders must risk submitting immutable evidence of their crimes that can be used against them. Requiring processes that utilise the blockchain's immutable audit trail (see PKI and the blockchain concepts above) can make scams harder and simultaneously, make compliance and recourse easier.

3.10. **Improve educational content and access to information**

a. Immutably public scoring and reporting – government authorities could poll licensed and unlicensed exchanges publicly using the blockchain's immutable audit trail to facilitate improved public transparency in market reporting. This could allow markets to compete more honestly and effectively and assist efforts to deliver a fairer and more level playing field.

b. Lookup services and blacklists – provide a free and open lookup service that allows people to search quickly and easily to see if a listing, coin or person is associated with existing scams, bad actors, parties under investigation, etc.

c. Education campaigns that address common myths – for example:

(i) The myth that 'crypto' is new, different, or somehow exempt from existing securities, misleading and deceptive conduct, and other laws.

(ii) The myth that public token systems lack enforceability. The reality is court orders can require miners to reassign property (for example, by updating UXTO sets) or risk bankruptcy and criminal actions for non-compliance.

Q4) The concept of ‘exclusive use or control’ of public data is a key distinguishing feature between crypto tokens/crypto networks and other data records.

Q4) a) How do you think the concepts could be used in a general definition of crypto token and crypto network for the purposes of future legislation?

4. We suggest not relying on the concept – ‘exclusive use or control’ of public data as a key distinguishing feature to distinguish between crypto tokens/crypto networks and other data records – as a general definition for crypto tokens and crypto networks for the purposes of future legislation because:

4.1. **Australia does not seem to require new laws for ‘cryptocurrency’ or digital tokens because of the common law, existing regulations and existing enforcement actions**

Consider the following:

a. Australia’s common law and existing frameworks have successfully resolved electronic contract disputes for almost seventy years.

‘Crypto’ does not introduce anything fundamentally new concerning principles and their application. Law has been resolving electronic contracting disputes for almost seventy years (see the well-studied case, *Entores v Miles Far East Corp* (1955] 2 QB 327) where Lord Denning dealt with issues of contracting through electronic communications by telex. Also see Craig Wright, 2020, Cryptocurrency and the Law of the Horse https://craigwright.net/blog/law-regulation/cryptocurrency-and-the-law-of-the-horse/.

b. Australia has existing legislation that already deals with securities and misleading and deceptive conduct (‘crypto’).

In paragraph 146, the Consultation paper acknowledges existing statutes allow Australians to seek justice across a wide variety of circumstances including securities frauds, misleading and deceptive conduct, etc. – all of which have developed case law and legal standards that have evolved over thousands of years, including almost seventy years of electronic contracting by wire telegraph and the internet.

c. High profile enforcement actions

(i) Liberty Reserve – in 2013, authorities spanning 17 countries coordinated to shut down the anonymous digital currency service Liberty Reserve for money laundering and operating an unlicensed financial services company (see BBC 2013, Liberty Reserve digital money service forced offline, https://www.bbc.com/news/technology-22680297).

(ii) The High Court of England and Wales has not insisted on new 'crypto' regulations to clarify the law so that they can deliver justice. Instead, concerning the recent Wormhole hack, they simply issued a court order to self-proclaimed 'crypto' and 'DeFi' Oasis.app to retrieving asset (see Statement Regarding The Transactions From The Oasis Multisig on 21st Feb 2023, https://cryptopotato.com/wormhole-bridge-exploit-140m-worth-stolen-assets-recovered/).

(iii) This subject of developer duties to access and return lost and stolen assets will be re-addressed in an upcoming case at the U.K. Court of Appeal concerning Tulip Trading Ltd v Bitcoin Association, Van der Laan, Schnelli, etc. and the recovery of £3+ billion worth of Bitcoin (see ONTIER, Court of Appeal Allows Trial To Determine Bitcoin Developer Fiduciary Duties, 2023

https://www.ontier.digital/post/court-of-appeal-allows-trial-to-determine-bitcoin-developer-fiduciary-duties).

4.2. **'Crypto' does not appear to confer 'exclusive use or control' of public data in all cases**

Consider for example:

a. People holding Bitcoin cannot exclude miners from responding to Court orders that compel them to update their UTXO set to reassign coins because 'crypto' does not operate outside the law.

b. Many webmasters also enjoy 'exclusive use or control' over the 'public data' they make available on their websites – though like the Bitcoin example above, this does not make them immune to enforcement actions directed at themselves personally, indirectly through ISPs, etc.

c. Defining a 'crypto token' by what it 'can be' suggests vagueness and a lack of clarity which begs concrete, case-by-case attention.

d. The citations raised to support the concept of 'exclusively used or controlled' include a UK paper which is still in the consultation phase (see Law Commission (UK), 'Digital Assets: Consultation paper', 2022 https://www.lawcom.gov.uk/project/digital-assets/) and recent and voluntary US legislation that some 21 USA states have adopted (see Article 12, pg. 229 of 'Uniform Commercial Code Amendments 2022 https://www.uniformlaws.org/viewdocument/final-act-164?CommunityKey=1457c422-ddb7-40b0-8c76-39a1991651ac&tab=librarydocuments) suggesting they are not yet well tested by courts and possibly contain hidden or secondary risks or consequences adverse to ensuring that markets are fair, efficient, and competitive.

e. The Consultation paper risks breaching its own requirement, in footnote 40, of being “overly simple” (inadvertently capturing systems used for everyday purposes).

4.3. **Lack of a clear policy goal**

The Consultation paper does not appear to make a compelling case in answering the important questions: what is the goal? And what is the benefit of having more ‘general’ definitions when Australia already has legal definitions that allow regulatory authorities and judges to apply the law on a case-by-case basis?

This can be contrasted with the UK which has expressed at least the intension to become “a world-leader in fintech, unlock growth and boost innovation” (see HM Treasury, Future financial services regulatory regime for crypto assets Consultation and call for evidence, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1133404/TR_Privacy_edits_Future_financial_services_regulatory_regime_for_cryptoassets_vP.pdf).

4) b) What are the benefits and disadvantages of adopting this approach to define crypto tokens and crypto networks?

4.4. **Disadvantages**

The Consultation paper proposes problematic definitions which may be superfluous or worse, undermine Australia’s competitiveness and credibility by:

a. **Signalling confusion**

As explained in our response to 4.a, Australia already has a wide variety and historically proven legal mechanisms and protections – whether peer-to-peer or intermediated, civil or criminal.

The presence of buzzwords – such as ‘crypto’, ‘DeFi’, ‘DAO’ and ‘smart contracts’ – do not evade well established legal concepts for identifying parties and liability. For example, a DAO, without alternative structuring, would simply default a partnership with no liability protection. Aggrieved parties can sue one or more of the DAO’s developers who are jointly liable.

With respect to ‘smart contracts’, the legal sphere already has a mature body of law concerning Electronic Data Interchange (EDI).

In paragraph 180, the Consultation paper identifies a concrete perceived difficulty, stating, “An interest in a DAO through holding a voting token (commonly known as a ‘governance token’) may be difficult to classify under existing financial services laws. They are not ‘equity’ in any traditional sense, and they do not necessarily entitle holders to legal ‘ownership’ of the DAO controlled funds. However, DAOs can generate revenue for their token holders and many DAOs control ‘treasuries’ of crypto token valued in the hundreds of millions or billions of dollars.”

Various jurisdictions classify a security using the Howey test which states something is a security if “there is the investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others.” If someone pays for a DAO token (which implies the efforts of others) because, as the paragraph says, “many DAOs control ‘treasuries’ of crypto tokens valued in the hundreds of millions or billions of dollars”, then this strongly suggests the expectations of profit, so it is a security. However, since the paragraph also says, ‘not necessarily’, such decisions and distinctions historically are made through disputes and by courts on a case-by-case basis.

a. **Creating cost, waste and legal uncertainty through contradictory definitions or assumptions**

The Consultation paper proposes a variety of 'crypto' definitions ('crypto asset', 'crypto token', etc), which rest upon a vague and circular definition for 'crypto' being 'an umbrella term for crypto networks' – itself defined as essentially "all computing platforms globally" since computers hold at least some digital files.

We suggest the Treasury reconsider the potential for errors and assumptions of the proposed definitions. For example:

(i) Paragraph 167: "A smart contract is not a 'contract' in a legal or plain English sense". This prompts the obvious question: what then, is the point of such a definition?

(ii) Paragraph 29: citing Luke Dashjr, "A **public crypto network** aims to provide certain information security guarantees". Do they? Which specific concrete informational guarantees?

This seems at odds with the express wording of the Bitcoin whitepaper which does not mention any 'guarantee' or 'guarantees' and instead, expressly mentions the contrary: "Messages are broadcast on a best effort basis" (See Wright (Pseudonym: Nakamoto, S), Bitcoin: A Peer-to-Peer Electronic Cash System (August 21, 2008) https://ssrn.com/abstract=3440802).

(iii) Paragraph 30: citing V Buterin, "A public crypto network… If there are no restrictions on the computers that are allowed to join the network, it creates an open information processing system that cannot discriminate between users or use cases" reveals another error.

Firstly, if this were true, nodes (transaction processors) would be unable to reject blocks from other nodes they perceive as bad actors. The past decade of transaction processor behaviour and the Bitcoin whitepaper – which includes key terms for Bitcoin's unilateral contract –

demonstrates the contrary: “Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash” (see Wright (Pseudonym: Nakamoto, S), Bitcoin: A Peer-to-Peer Electronic Cash System 2008).

Secondly, Bitcoin can discriminate between use cases and developed to include insights from common carriers and associated laws. Bitcoin’s double hash was implemented to allow “us to have immutable data storage that can be filtered with the hash being validated and a subsequent prune of illicit material being allowed in certain jurisdictions…[so that]… we can selectively deliver content.” (see 2019, Coingeek, Dr. Craig Wright on the double hash puzzle https://coingeek.com/dr-craig-wright-on-the-double-hash-puzzle/ and https://craigwright.net/blog/bitcoin-blockchain-tech/the-puzzle-of-the-double-hash/)

4.5. **Benefits**

a. **Jurisdictional diversity**

Passing such definitions would produce outcomes that may distinguish Australia’s attractiveness for foreign and economic investment. This may not, though could be, favourable for Australia, but would provide insights for other Jurisdictions seeking to learn from Australia’s actions in the space.

4.6. **Other approaches**

a. **Re-consider approaches**

If Australians who lost out to scams, misrepresentation, and other schemes, aren’t aware of their existing legal protections, will more

regulations truly help and represent a steward's use of Australian taxpayer resources?

b. **Don't be fooled by 'crypto': Enforce the law**

Like 'crypto', the rise of the Internet as a commercial tool created a level of uncertainty surrounding the law of offer and acceptance (see Wright, Craig S, Electronic Contracting, New Wine in Old Bottles, 2006, https://ssrn.com/abstract=2957057). Don't be fooled. Deter criminals by enforcing existing, long proven and well-established legal concepts and protections, particularly fraud – securities, wire, misleading and deceptive conduct, etc. In the end, 'crypto' networks are simply groups of people (developers, promoters, investors, etc) with machines running code that are embedded in, and subject to, the laws of Jurisdictions.

c. **Consider issuing clarifications on how existing legal concepts apply and suggest existing means of recourse for harmed consumers and investors**

Since law is applied on a case-by-case basis, instead of proceeding with broad definitions that ignore this aspect of Australia's legal system and may cause inconsistencies, regulators and Judges may issue clarifications and orders applying existing laws to 'crypto'.

Q5) This paper sets out some reasons for why a bespoke 'crypto asset' taxonomy may have minimal regulatory value.

Q5) a) What are additional supporting reasons or alternative views on the value of a bespoke taxonomy?

5. **Supporting view: Global interoperability**

Developing a taxonomy could support interoperability by providing organisations with taxonomy terms they could choose to use when designing and developing their domains and systems. Organisations and governments could achieve even greater interoperability, efficiency, and compliance cost savings by expressly coding the domain into a broadly supported and accessible ontology that provides quick and easy integration options. Converting what was previously implicit knowledge in human brains and taxonomical terms in books and files, into explicit interoperable data structures in computing systems unlocks opportunities for more automated, scalable, and real-time systems.

For example, the Financial Industry Business Ontology (FIBO) (see https://spec.edmcouncil.org/fibo/) has allowed financial organisations and regulators to operate with improved efficiency and reduced the cost of data preparation and transformation costs between previous inconsistent and less-interoperable taxonomies, definitions, and systems.

5.1. Alternative view: Lack of compelling need

Does Australia have compelling policy reasons requiring a ‘Crypto Assets’ taxonomy? The Consultation paper does not appear to provide compelling reasons why a ‘crypto assets’ taxonomy is required and seems to present inconsistencies that undermine the case for exhaustive token mapping. For example:

a. The Consultation paper:

   (i) Implies, at paragraph 32, that most activities are already covered by existing AFSL requirements though its use of the words “exchanges, lending and borrowing services) who are typical intermediaries”;

   (ii) Lists, at paragraph 146, existing Australian crypto asset regulations including: regulators, acts and protections that aggrieved ‘crypto’ participants and speculators have the option of deploying today; and

(iii) Does not appear to clearly articulate why ‘crypto’ is not dealt with by existing regulatory bodies and failing that, the common law.

(iv) Does not seem to provide clear measures for assessing the value of the exercise.

b. To the extent that grievances are a major issue, it may be more cost-effective to, instead of seeking yet more regulations, educate Australians with, for example, some high-profile enforcement actions against ‘crypto’ bad actors. For example, would scams decrease if DAO developers learned cautionary tales of the risks of doing business through Partnerships? Would large advertising or other networks be more careful with compliance if they were found to be associated with aiding and abetting misleading and deceptive conduct?

c. If Australia does proceed with such a taxonomy, then:

(i) What good is the foundational philosophy of having a functional approach to defining financial products and services?

Since Australia’s financial services framework uses an abstract or principled definition – more vague than overseas Jurisdictions with their exhaustive lists; but more adaptable; and delivering ever greater clarity through case-by-case applications and supplementary definitions – would an express taxonomy not imply Australia had moved towards civil Jurisdictions?

(ii) Why stop at tokens? Why not map the full range of OTC potentialities?

Q5) b) What are your views on the creation of a standalone regulatory framework that relies on a bespoke taxonomy?

5.2. We suggest that creating a standalone regulatory framework that relies on a bespoke taxonomy seems, for reasons outlined above (see our response to Question 5.a, unlikely to be fruitful because such a framework:

a. Does not appear to be required because of existing laws and regulations and likely superior benefits achieved from a higher level, functional or principles-based approach;

b. Developing such a taxonomy in a way that is enduring and not unnecessarily complex seems unlikely since this would be equivalent to classifying all over the counter (OTC) transactions which legal systems have been unable to achieve despite decades or even hundreds of years of experience;

c. A bespoke taxonomy and framework could adversely affect the costs and benefits of Australian innovation if, as the existing paper suggests, definitions are not based upon well-established legal principles and or lack objective criteria for which the entire proposition can be measured and justified; and

d. Such a framework may not address compliance concerns arising from a lack of enforcement.

Q5) c) In the absence of a bespoke taxonomy, what are your views on how to provide regulatory certainty to individuals and businesses using crypto networks and crypto assets in a non-financial manner?

5.3. To the extent that regulatory certainty for individuals and businesses exists, we suggest it be provided using the functional or principled approach of classifying ‘financial products’ and ‘financial services’ and proceed by resolutions on a case-by-case basis. Crypto assets and networks that are

non-financial can be treated as such and proceed through existing consumer protections.

Australia's existing frameworks and approach to certainty have been built and refined over decades. A key strength of the common law and this framework is its ability to adapt principles to facts on a case-by-case basis instead of trying to exhaustively specify everything that could happen in a complex and changing world.

5.4. **Do not be fooled by 'crypto': Enforce the law**

ASIC has clarified that Bitcoin is not a financial product (see ASIC, Senate inquiry into digital currency, Submission by the Australian Securities and Investments Commission, 2014 https://www.aph.gov.au/DocumentStore.ashx?id=4b6d105f-3e0a-4d52-aaab-1f35842ed5f1&subId=302297). However, a surprising number of 'crypto' exchanges, issuers, etc. would appear to require an AFSL to operate in Australia and service Australian clients. International collaboration could assist related enforcement actions.

At a broader contracting level, non-financial peer-to-peer transactions are already well-established concepts at law and individuals and businesses are already protected. Australia passed through a similar phase of confusion during the early internet (see Wright, Craig S, Electronic Contracting, New Wine in Old Bottles, 2006, https://ssrn.com/abstract=2957057).

5.5. **Reconsider assumptions and existing advice**

We suggest reconsidering existing advice provided to Australians in light of information contained in this submission, particularly our response to Question 9.

Individuals and businesses seeking to use misunderstood or unproven digital networks – particularly with constantly changing protocols, damaging and unnecessary constraints, or acknowledged security flaws – may recall the lessons of history. In particular, "buyer beware" and Matthew 7:24-27, "a

wise man… built his house on the rock… the floods came… winds blew and beat on that house; and it did not fall, for it was founded on the rock… a foolish man… built his house on the sand… the rain descended, the floods came, and great was its fall."

5.6. **Other considerations**

a. **Education** – including improved training or requirements for Australian licensees, license providers, regulatory bodies, educational systems, law colleges, etc. who engage with consumers and investors.

b. **Broader policies** – inflation, financial repression and other policies may be disincentivising productivity and savings and promoting an environment that encourages consumers and investors to seek out speculative schemes.

c. **Aiding and abetting** – Advertising, Big Tech or other networks may be aiding and abetting speculation.

d. **Special interests** – Draftsmen, lobbyists and other special interests may be pursuing new regulation to combat 'crypto' at expense of the Australian taxpayer for personal and not broader Australian interests.

Q6) Some intermediated crypto assets are 'backed' by existing items, goods, or assets. These crypto assets can be broadly described as 'wrapped' real world assets.

Q6) a) Are reforms necessary to ensure a wrapped real-world asset gets the same regulatory treatment as that of the asset backing it? Why? What reforms are needed?

Q6) b) Are reforms necessary to ensure issuers of wrapped real-world assets can meet their obligations

to redeem the relevant crypto tokens for the underlying good, product, or asset?

6. We suggest there are well established protocols concerning wrapped real-world assets including existing securities and commodity frameworks. For example, Australian banks have issued tokens redeemable for Australian dollars and face existing liquidity, reserve, audit, and other requirements.

6.1. Although the mere existence of so called 'crypto' or digital tokens does not fundamentally alter principles but merely their application (see Craig Wright, 2020, Cryptocurrency and the Law of the Horse https://craigwright.net/blog/law-regulation/cryptocurrency-and-the-law-of-the-horse/) the introduction of a public immutable ledger capable of micropayments with a Turing complete scripting language can offer new capabilities that improve operations, efficiency, and compliance. In particular:

a. **Proofs-of-reserves to combat liquidity mismatches** – also see our response to Question 7b. Benefits associated with public token networks can be strengthened with improved regulatory oversight that combines the blockchain as a public utility with private overlay networks that allow licensees to demonstrate reserves, security, and compliance in real-time either publicly or privately. Such systems present a significant opportunity for real-time systems including debt securitisation networks and the Internet of Things (IoT).

b. **Asset rehypothecation** – can similarly be improved though the public utility of the blockchain and overlay networks because of available improvements for audit trail, access control, and management cost.

c. **Leverage** – the immutability of the public blockchain combined with private overlay networks allows for improvements for services providing and managing leverage as well as for governments

seeking to provide improved oversight without compromising privacy.

6.2. Operators that seek to evade the law will continue to be a challenge. For example, if FTX had complied with securities and other requirements it would have been less likely to fail as it did. However, as suggested above, new capabilities that improve the transparency, cost, and speed of compliance can improve markets globally.

Q7) It can be difficult to identify the arrangements that constitute an intermediated token system.

Q7) a) Should crypto asset service providers be required to ensure their users are able to access information that allows them to identify arrangements underpinning crypto tokens? How might this be achieved?

7. The Consultation paper acknowledges that, “It can be difficult to identify the arrangements that constitute an intermediated token system.” Complexity is a major reason Australia has implemented the existing, case-by-case friendly approach to securities, allowing regulators and courts to apply and adapted to changing times, technologies, and schemes.

7.1. The Consultation paper uses the word “crypto asset service provider” but this is not a legal term under existing frameworks and therefore seems a less grounded way of dealing with well-establish concepts in law for classifying various contractual relationships. Existing legal concepts may be more helpful for classifying and addressing ‘crypto’.

7.2. Australia has well-formed diligence, disclosure and other requirements for existing financial services firms and regulatory bodies (ASIC, AUSTRAC, ATO, etc.) to enforce them. Where issuers, providers, promoters, and other parties fail to comply, including failures to disclose and provide “access to information that allows them to identify arrangements”, we suggest:

a. Enforcement – for example, for failing to comply with disclosure requirements and distribution requirements. If offenders are operating outside of Australia, this may require international actions and collaboration.

b. Address potential internal conflicts – to the extent that governance is compromised by internal conflicts such as regulatory capture, corruption, or incompetence – which seems at least possible based upon the 2017-2019 he Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry – Australia's continued prosperity requires that such concerns be identified and addressed.

Q7) b) What are some other initiatives that crypto asset service providers could take to promote good consumer outcomes?

7.3. Operational initiatives enabled by the introduction of a micropayment delivering public immutable blockchain with a Turing complete scripting language (Wright, Turing Complete Bitcoin Script White Paper, 2018) include:

a. **Improved Public Key Infrastructure (PKI) for significantly improved security, KYC and/AML)** – from annual checks to instant revocation of (invalid KYC, AML, etc) certificates with "9000 certificate issuances, revocations, or updates per second at a cost of less than 0.005 USD per event" (A Blockchain-Based PKI Management Framework, 2021). This has wide and significant implications for certificate authorities and anyone who uses their services (such as email, banking, etc.) and could address significant vulnerabilities in today's internet as demonstrated by attacks such as DigiNotar.

b. **Cheaper payments (micropayments)** – the ability to price below legacy electronic payment cost floors such as card network fees and bank transfers. 10x cheaper than cards. Costs will decrease

further as volumes scale. Sub-20¢ payments will power new industries (see **Error! Reference source not found.**).

c. **More accessible payments** – the ability to provide the unbanked, and those in remote areas, instant, global and efficient cash. People without phones or bank accounts can enter the economy with less friction (smart cards).

d. **Faster settlement** – near instant global payments.

e. **Improved cross-border payments** – from days to milliseconds; 9-5pm to 24/7.

f. **More resilient and available payments and service** – "Anywhere, anytime". 100% uptime. Trade during outages thanks to offline payments.

g. **New payment types**

(i) **Multi-party** – pay all parties on events. Unlocks real-time taxation.

(ii) **Peer-to-peer** – like handing someone cash. Avoids relying on fragile, distant servers.

(iii) **Offline** – instead of "cash or lose the sale" merchants can accept offline payments with reasonable credit risk via a simple client and broadcasting on reconnection. Thresholds (lower values only) can reduce risk further.

(iv) **Programmable** – innovation and competition opportunities, increased policy scope and effectiveness, improved latency, and fraud protections.

h. **Safer payment options**

(i) **The ability to recover lost funds without a third party via backups** – when a wallet is lost or stolen, a second

device holding a backup can automatically transfer the funds to a safe address.

(ii) **Anti-crime payments** – immutable logs and identity systems can reduce welfare fraud, money laundering, and shadow banking crime. Where courts issue freezing orders, specified funds cannot be spent, allowing recovery from illicit activity.

i. **Improved privacy** – for example, via the AML/CFT compliant New Privacy Model (Nakamoto, 2008).

j. **Immutable traceability and attributes** – unalterable evidence trails. Recommended or required use of the blockchain as an immutable timestamp and audit service incorporating defined 'country attributes', or other attributes associated for regulated products, services, agreements, or other information could significantly improve national and international compliance and dispute resolution.

k. **Real-time insights** – atomic (singular) data fields can be priced and transacted across a wide variety of domains such as: location (from merchant to country), source (KYC), product, etc. allowing new kinds of real-time services, transparency (for example, audits concerning products or tokens from minting to last payment), improved liquidity and asset programs, etc.) without compromising privacy.

l. **Improved Fiscal Policy** – allowing innovative governments and Treasuries to deploy:

(i) **Frictionless real-time taxation and rebates** – from burdening payors with tracking, reporting, and paying tax and rebates, to automatic multi-party payments.

(ii) **Fiscal transfers** – bypass indirect transmission to achieve objectives more directly whilst reducing cost and risk.

m. **New business models and industries** – for example:

(i) **Transaction Processing**: delivers micropayments, jobs, price improvements and sustainable energy.

(ii) **Interoperable services**: Digital Passports will remove friction, save time, cost, and privacy across all industries.

(iii) **Micropayment industries**: a new economic era. The internet after ads. See https://nchain.com/creating-the-internet-of-value-through-bitcoin-data-interchange-and-iot-technology/.

(iv) **Direct models**: micropayment fees. Pay-per: byte, watt, CPU-cycle, etc.

(v) **Indirect models** – providers cover costs for other benefits (new customers, data, interactions, etc.).

n. **Enhanced services for existing banking systems** – improve bank efficiency, settlements, issuances (credit, bonds), etc.

o. **Improved compliance** – automated audits, real-time compliance, triple-entry accounting, real-time reporting etc will free labour to pursue new growth.

p. **Improved accountability** – staff, committees, etc. can issue, hash, timestamp (to the blockchain) and distribute (publicly or privately): orders, reports, legislation, reserves, etc. For example:

(i) **Proofs-of-reserves to combat liquidity mismatches** – we have seen exchanges listing more tokens for networks (such as Bitcoin) than exists in the total supply, indicating that some exchanges are lying about their actual positions. Requiring authorised exchanges to tag

addresses could provide a real-time proof of reserves for networks, allowing law enforcement and the public to assess the risks of trading more easily with a particular service. Such approaches will provide improved transparency and decrease the chances of prior breaches such as at Mt. Gox.

(ii) **Split key systems** – (also see multi-party payments) can prevent exchange hacks from comprising everyone's funds. Where hacks do happen and exchange providers lose their keys, hackers will be unable to steal funds because they lack the client's key. Clients can then recover funds after a pre-determined time. Exchanges and custody arrangements can become significantly more secure and reliable, decreasing counterparty risk, scams and fraud across economies.

(iii) **Asset rehypothecation** – the blockchain and overlay structures can improve and expand the reach and operation of asset rehypothecation and securitisation agreements, particularly as tokenisation, IoT networks and digital twins advance (see nChain, 2022, Creating the Internet of Value through Bitcoin Data Interchange and IoT Technology, https://nchain.com/creating-the-internet-of-value-through-bitcoin-data-interchange-and-iot-technology/). The public nature of the blockchain, when coupled with the New Privacy Model and the intelligent use of encryption, will allow for simultaneously improved compliance and improved privacy.

7.4. Businesses can also promote good consumer outcomes through less innovative yet important means including easy-to-understand education materials, best practice security measures, disclosures of important duties, risks and requirements, dispute resolution systems, and so forth.

Q8) In addition to the functional perimeter, the *Corporations Act* lists specific products that are financial products. The inclusion of specific financial products is intended to both: (i) provide guidance on the functional perimeter; (ii) add products that do not fall within the general financial functions.

Q8) a) Are there any kinds of intermediated crypto assets that ought to be specifically defined as financial products? Why?

Q8) b) Are there any kinds of crypto asset services that ought to be specifically defined as financial products? Why?

8. There are kinds of 'intermediated crypto assets' or 'crypto asset services' that ought to be specifically defined as financial products. However, instead of defining blanket and potentially counter-productive definitions now (that might adversely affect Australia's interests), it seems more prudent for such definitions to arrive as they have under the existing framework for prior financial products – that is, on a case-by-case basis (see https://asic.gov.au/regulatory-resources/regulatory-index/financial-services/financial-products/).

Q9) Some regulatory frameworks in other jurisdictions have placed restrictions on the issuance of intermediated crypto assets to specific public crypto networks. What (if any) are appropriate measures for assessing the suitability of a specific public crypto network to host wrapped real world assets?

9. nChain supports a principled-based approach for assessing and managing risks associated with suitability of so-called public crypto networks.

9.1. ASIC Report 705 proposed criteria from their earlier consultation (CP 343) to assist organisations in assessing 'crypto-asset' suitability for underlying assets (see point 15 on page 8 of 2021, Response to submissions on CP 343 Crypto-assets as underlying assets for ETPs and other investment products https://download.asic.gov.au/media/p3tnevtt/rep705-published-29-october-2021.pdf), including: institutional support, service provider availability, mature spot markets, transparent pricing, etc. Shareholder feedback raised concerns this was 'too restrictive'.

In ASIC's view at that time, "the only crypto-assets that are likely to satisfy these factors at this point in time are bitcoin (BTC) and ether (ETH)". We suggest neither are suitable for the reasons below. We also propose that readers who have an open mind, can suspend any bias arising from today's spot prices and who investigate Bitcoin's original concept and present incarnation may discover valuable insights.

9.2. We suggest the following are appropriate measures for assessing the suitability of specific public crypto networks to host digital assets.

a. **Scale** – can the network scale to meet demand?

Some networks face scale limitations because of:

(i) protocol limitations – such as Ethereum (see Cointelegraph, Ethereum network congestion temporarily shuts down crypto gaming casino https://cointelegraph.com/news/ethereum-network-congestion-shuts-down-crypto-gaming-casino); or

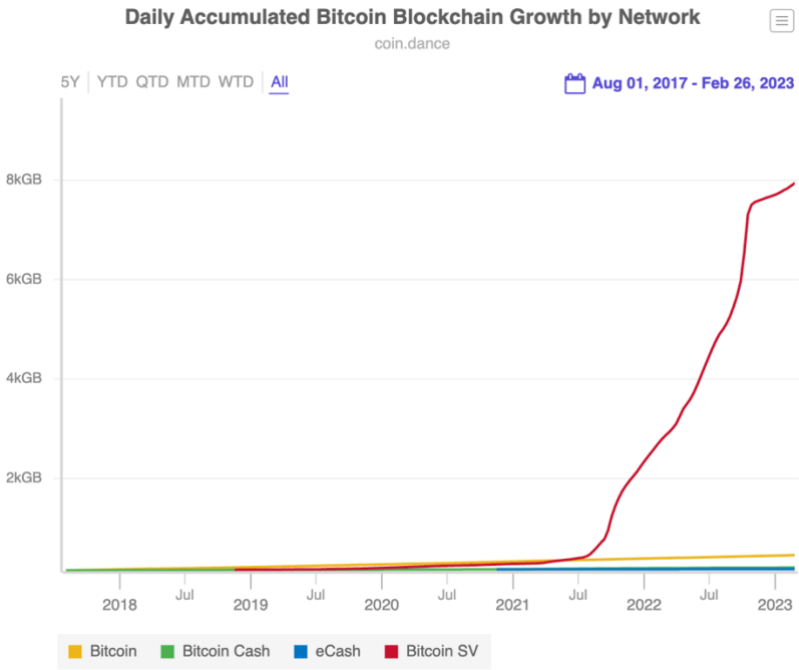
(ii) self-imposed limitations – such as BTC developers' decision to fork away from the original Bitcoin protocol and implement a limited block strategy of 1MB and later 4MB block caps.

Other networks have unbounded protocols that allow infrastructure to scale to serve billions or even trillions of users. The most notable example is Bitcoin with its unbounded block strategy as

originally demonstrated by the lack of a block cap at the network's launch and Satoshi's express confirmation to Mike Hearn by email.

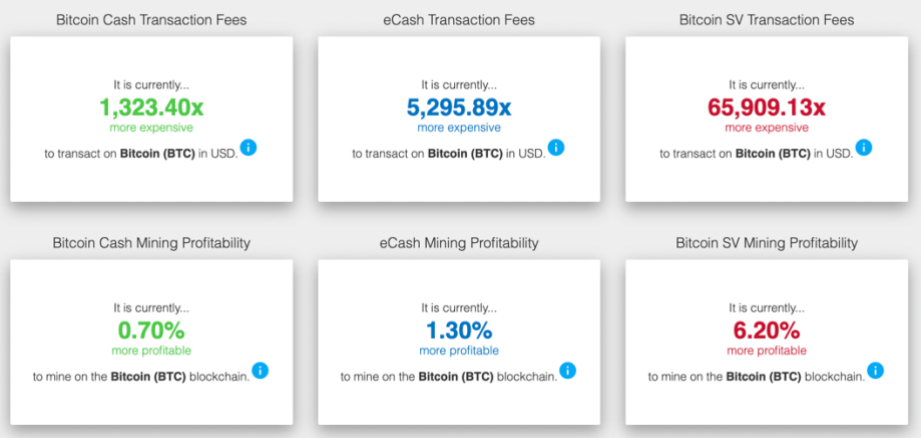
"*The existing Visa credit card network processes about 15 million Internet purchases per day worldwide. Bitcoin can already scale much larger than that with existing hardware for a fraction of the cost. It never really hits a scale ceiling*." – Satoshi Nakamoto email to Mike Hearn, 2013, https://bitcointalk.org/index.php?topic=149668.msg1596879#msg1596879)

The internet did not scale to billions overnight because doing so requires investment in infrastructure. However, like the internet, Bitcoin (BSV) is demonstrating scale with, as of the time of writing, 4GB blocks and 18,606,42 peak Transactions Per Second (TPS) on main-net (see https://bitcoinscaling.io/stats) and the largest daily cumulative growth of comparable networks (see https://coin.dance/blocks/growth).



b. **Cost** (price efficiency) – does the network facilitate and have an incentive system game-theoretically designed to promote innovation and achieve the cheapest micropayments possible?

Some public networks, such as Bitcoin (BSV) is orders of magnitude more cost efficient than others (See https://coin.dance/#fees).



c. **Security** – is the network secure? How secure? How easy is it to audit?

Some public networks are fundamentally insecure. For example, Vitalik Buterin recently admitted to critical security vulnerabilities plaguing Ethereum on The Network State Podcast, stating, “layer twos that exist on Ethereum today, they basically all have what I call training wheels, like, some kind of back door that lets developers come in and like say, stop and change the protocol” (The Network State Podcast, Vitalik on Starting New Countries and Improving Yourself | The Network State Podcast with Balaji #1, https://www.youtube.com/watch?v=1xhPqZZYJSE&t=41m). By contrast, other networks such as Bitcoin (BSV) offer a variety of compelling layer 1 and layer 2 tokenisation solutions that have yet to be breached.

A major benefit of public token systems is the source code they utilise can often be easily accessed for security audits by independent third parties. Government can promote such validations which can also fit within a whitelisting framework.

d. **Resilience and network uptime** – how resilient is the network to attacks? How long has it been operating?

For example, Bitcoin (BSV), which uses the most resilient digital network architecture, a ‘small world’ mandala network, has experienced 100% uptime for over a decade (see D J Watts 1, S H Strogatz, Collective dynamics of 'small-world' networks).

By contrast, Solana, which uses the fragile and legacy mesh architecture common to today’s internet, continues to be plagued by outages, going offline over 7 times in 12 months (see Cointelegraph, Reliably unreliable: Solana price dives after latest network outage https://cointelegraph.com/news/reliably-unreliable-solana-price-dives-after-latest-network-outage).

e. **Compliance** – what are the circumstances of the public token network’s launch and operation? Does the network demonstrate respect for law and sovereignty? Are nodes and validators ‘public facing’ and thus more easily addressable by laws and courts?

Concerning the initial token distribution, the transparency of the launch procedure, the nature of protocol rules (changing or stable), or the lifespan of the network, etc. are important. Public token networks not operating on a compliant and established legal basis carry legal risks capable of negatively impact any users of that network. For example, SEC Chair Gary Gensler’s recent comments – “Everything other than bitcoin” – suggest Ethereum is a security (see NYMagazine, 2023, Can Gary Gensler Survive Crypto Winter? D.C.’s top financial cop on Bankman-Fried blowback.https://nymag.com/intelligencer/2023/02/gary-gensler-on-meeting-with-sbf-and-his-crypto-crackdown.html).

For ongoing operations, honest governments can require that nodes and validators be ‘public facing’, as is the case with public utilities so that people can more easily identify them to deliver court mandates such as for asset recovery. Permitting ‘anonymous’ node operators would contravene a long history of public safety operations associated with energy, transportation, and other industries and utilities.

Q10) Intermediated crypto assets involve crypto tokens linked to intangible property or other arrangements. Should there be limits, restrictions or frictions on the investment by consumers in relation to any arrangements not covered already by the financial services framework? Why?

10. As stated in our response to Question 1, the blockchain is just a database and hence is not a new means of owning assets. If desired or required, wallets can set limits, restrictions or other frictions on cash and financial products and services.

10.1. For those interested in de-risking linked assets, we suggest tokens linking to property can be improved through the blockchain because it can provide an immutable audit trail which is significantly harder to defraud compared to legacy approaches which often involve multiple, separate sets of records on separate systems.

10.2. Privacy of linked assets can also be improved whilst also being real-time compliant by using pseudonymous identifiers on the blockchain which may also include country attributes (see PKI above) and link to encrypted on-chain or off-chain information.

10.3. To the extent that limits, restrictions, or frictions on consumer investments are required at a framework level, we suggest they proceed to be brought under the existing framework on a case-by-case basis as with past failures of justice and supplementary definitions added to Australia's financial products and services framework (see https://asic.gov.au/regulatory-resources/regulatory-index/financial-services/financial-products/).

10.4. We suggest future consultations might yield more comprehensive answers to this question by providing examples they think clarify as "arrangements not covered already by the financial services framework".

Q11) Some jurisdictions have implemented regulatory frameworks that address the marketing

and promotion of products within the crypto ecosystem (including network tokens and public smart contracts). Would a similar solution be suitable for Australia? If so, how might this be implemented?

11. Australia has existing regulatory frameworks governing requirements for the marketing and promotion of financial and non-financial including existing sophisticated investor provisions and those covering advertising and misleading and deceptive conduct. Aggrieved parties can also seek remedies using the common law and through international courts. To the extent that Government perceives itself to be disempowered we suggest revisiting our response to Question 1 and considering the following.

11.1. Education

If Australians are not of aware of protections or unmotivated to pursue remedies, are there compelling reasons for more regulation? Investing in quality education that makes Australian's more responsible, capable, and productive can make Australians more resilient, less dependent, and less susceptible to scams and the agendas of adversarial state and non-state actors.

11.2. Enforcement

History demonstrates that where there are real and serious breaches of law, motivated parties eventually bring actions. For example, consider:

a. Liberty Reserve – in 2013, authorities spanning 17 countries coordinated to shut down the digital currency service Liberty Reserve for money laundering and operating an unlicensed financial services company.

b. Grokster – in 2005, peer-to-peer file sharing companies Grokster and Streamcast (maker of Morpheus) were held liable (secondary liability) for inducing copyright infringement via their users. See MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005).

c. FTX – in 2023 and 2023, the SEC commenced proceedings against FTX for breach of securities laws (see SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX, https://www.sec.gov/litigation/litreleases/2023/lr25616.htm) – demonstrating that what many think of as 'crypto' is not unique and in many cases, sits within existing securities frameworks.

Q12) Smart contracts are commonly developed as 'free open-source software'. They are often published and republished by entities other than their original authors.

Q12) a) What are the regulatory and policy levers available to encourage the development of smart contracts that comply with existing regulatory frameworks?

12. nChain supports the view that so called 'smart contracts' do not usurp any of the underlying legal principles of contract law nor their application to electronics – see Electronic Data Interchange (EDI) arrangements. The same level of promises, intermediaries and agents apply as they do to traditional finance. While new types of intermediaries exist – in particular, nodes or transaction processors – net functions seem the same.

12.1. Today's production and distribution of so-called 'smart contracts' is like the historical production and distribution of paper boilerplate contract templates by innovative lawyers seeking to provide faster, more standardised, transparent, and cost-effective services – and the subsequent evolution from paper to electronic contractual templates (EDI) and other communications standards. Contracts are legal products that range from 100% standardised to 100% customized and compete in the open market and courts to help people manage trade and risk. History demonstrates that, as we have seen with paper and electronic contracts, over time and by the invisible hand of the market (Smith, 1776), contracting parties encounter

disputes and identify the strengths and weaknesses of Jurisdictions, clauses, legal terms, contractual templates, providers, etc. The result is a virtuous circle of increasingly precise, efficient, and reliable:

a. Legal products – including contractual terms, clauses, templates, and mediums (from oral contracts to written; written to electronic; electronic to electronic, timestamped, and hashed on the blockchain); and

b. Dispute resolution processes – spanning Jurisdictions, courts and private arbitrations.

These advancements improve our lives by providing us with ever greater abilities to flourish, trade and manage risk.

Today, developers are designing, coding, and assembling digital contract products and making representations or promises about how they think they will perform in the legal marketplace. People then use and facilitate access to these products with implicit promises about their suitability. Such people may be promoters, issuers, transaction processors (nodes), etc. To the extent that these agents breach the law, they can be prosecuted, further advancing the cycle.

12.2. To encourage developments of contracts that comply with existing frameworks, we suggest:

a. Enforcement

Enforcement will allow courts and regulators to classify ‘smart contracts’, applications and arrangements into legal terms and consequences via rulings, orders and Judgements that provide the market with feedback that can stimulate innovative ideas for more compliant ‘smart contracting’ procedures.

Aggrieved public and private sectors can already bring actions against defendants using a wide array of options as the Consultation paper rightly acknowledges at paragraph 146.

Consumers or investors who have made losses in ‘DAOs’ (not operating as corporations or other protective structures) may sue any of the ‘DAOs’ developers, claiming they a legally speaking, a ‘partnership’ and thus joint and severally liable for other partners’ debts incurred under the partnership. This may improve the perceived accessibility of legal recourse to people using ‘DAO’ arrangements and prompt new ‘smart contract’ templates with more specific options for identifying parties, terms, choice of laws, choice of jurisdiction, procedures for dispute resolution, etc.

Entrepreneurs and businesses may discover the value in choosing digital contract templates that specify codes, tags, flags or other information to comply with state law.

If repeated instances of the same cases demonstrate a fundamental misunderstanding in the marketplace, the following regulatory frameworks and associated regulatory bodies, can issue, as they have in the past, clarifications through additional supplementary rulings and definitions:

(i) Financial services regulatory framework – which covers sophisticated investors, securities fraud, misleading and deceptive conduct etc. via the Corporations Act, Australian Securities and Investment Commission Act 2001 (ASIC Act), and National Consumer Credit Protection Act 2009 (NCCP Act).

(ii) Money laundering and terrorist financing framework – via AUSTRAC and the Anti Money Laundering and Counter Terrorism Financing (AML/CTF) Act. Digital currency exchanges must already register with AUSTRAC.

(iii) Taxation framework – ATO and Income Tax Act, Goods and Services Tax Act.

b. Education and Training

If Australia is to remain competitive in the increasingly digital and automated future, it is critical that government and industry understand what blockchain offers as a public utility (particularly for exchange, automation, AI, IoT, IPv6, etc) and consider how can it improve efficiency, privacy, compliance, and enforcement?

Many jobs require continuous learning and development. To the extent that Australian policy requires education, provide it. For example:

(i) The US Department of Justice manual provides advice on asset seizures, even “in cases where a wallet company does not itself have access to or control of the private key” (see U.S. Department of Justice Criminal Division, Asset Forfeiture Policy Manual 2023, https://www.justice.gov/criminal-afmls/file/839521/download).

(ii) Software exists for court enforcement procedures including asset freezing and recovery (see Coingeek, 2022, Blacklist Manager: An innovation software solution to help retrieve stolen or lost digital assets https://coingeek.com/blacklist-manager-an-innovation-software-solution-to-help-retrieve-stolen-or-lost-digital-assets/).

(iii) Counter psychological operations, buzzwords and myths designed to subvert and escape justice – ‘Smart contracts’, ‘crypto’, etc are subject to law. Enforcing existing laws will provide the market with feedback to adjust and develop more innovative and compliant solutions.

c. Improve the operational efficiency of enforcement action across whole of government

As we have explained in our response to Question 2 above (see 2.3. New operational safeguards made possible thanks to the blockchain), Australia has a significant opportunity to improve policy across the board when it comes to how it monitors, tracks, and enforces the law.

d. If the above fails, consider broader mandates

For example, the state of Illinois, USA recently drafted a mandate that any blockchain operating there includes smart contract code that would enable it to respond to court orders and move assets/funds without private keys (see FINANCIAL REGULATION (205 ILCS 730/) Blockchain Technology Act. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4030&ChapterID=20). However, this has not yet passed and may be unnecessary if Government uses existing frameworks as stated above.

Q12) b) What are the regulatory and policy levers available to ensure smart contract *applications* comply with existing regulatory frameworks?

12.3. Please see our response to Question 12.a as well as consider operational improvements, each of which can be tailored by any individual regulatory body or framework to suit their precise needs and specific applications (see Question 2 and 2.3. New operational safeguards made possible thanks to the blockchain).

For example, consider the question: what if Australia's government services (applications) were real-time, frictionless, more transparent, more accountable (using an immutable evidence trail), more private, more detailed (atomic), and significantly more cost efficient than they are today?

They can be. It's all possible today. nChain can assist Australia in providing its citizens, residents, and tourists with benefits including:

a. **Advanced Fiscal Policy**

(i) **Frictionless real-time taxation and rebates** – from burdening payors with tracking, reporting, and paying tax and rebates, to automatic multi-party payments.

(ii) **More efficient and direct fiscal transfers** – bypass indirect transmission to achieve objectives more directly whilst reducing cost and risk.

b. **Advanced Treasury Policy**

(i) **Automatic account reconciliation and audits** – including triple entry accounting and automatic real-time financial reporting and audits can streamline and reduce compliance burdens whilst simultaneously improving financial and cash-based exchanges transacted on the public blockchain.

(ii) **Improved law enforcement, legal and dispute resolution services** — notarisation, arbitration, and court integration services including freezing orders, thawing orders, etc. Such judicial integration services are critically important for the effective operation of a digital currency.

c. **New and improved payments**

(i) **Multi-party** – pay all parties on events. Unlocks real-time taxation.

(ii) **Peer-to-peer** – like handing someone cash. Avoids relying on fragile, distant servers.

(iii) **Offline** – instead of “cash or lose the sale” merchants can accept offline payments with reasonable credit risk via a simple client and broadcasting on reconnection. Thresholds (lower values only) can reduce risk further.

(iv) **Programmable** – innovation and competition opportunities, increased policy scope and effectiveness, improved latency, and fraud protections.

d. **New Public Key Infrastructure (PKI)**

PKI is a core technology powering 'secure' website, email, banking and other applications. Today's approach to PKI has key security vulnerabilities. The blockchain introduces a new, improved and more secure approach to PKI that could significantly improve the security, compliance and efficiency of Australian public and private operations. Security and compliance can advance from annual checks to instant revocations of (invalid KYC, AML, CFT, etc.) certificates. Existing capabilities can deliver "9000 certificate issuances, revocations, or updates per second at a cost of less than 0.005 USD per event" (A Blockchain-Based PKI Management Framework, 2021). A new PKI infrastructure can allow Australians to gain:

(i) **Improved exchange, trade, custody, and asset recovery systems –** for example, new asset recovery systems, new split-key systems that prevent hacks from compromising all data and funds (see above), etc.

(ii) **Improved AML** – today's approach to AML which has been fundamentally challenged on a cost benefit basis, prompting the question: is the existing cost effectiveness of existing AML and compliance obligations sustainable? (See Ronald 2018, Anti-money laundering: The world's least effective policy experiment?). A new PKI infrastructure on a public blockchain could reduce the AML cost burden on industry whist simultaneously improving compliance and privacy.

(iii) **Improved whitelists, sanctions and blacklists** – IPv6 and a novel blockchain based PKI identity system, as

explored by the ESTI's Industry Specification Group (IPG) IPv6 Enhanced Innovation (IPE) could decrease costs and improve compliance (see https://www.etsi.org/technologies/ipv6-enhanced-innovations-ipe).

Q13) Some smart contract applications assist users to connect to smart contracts that implement a pawn-broker style of collateralised lending (i.e. only recourse in the event of default is the collateral).

Q13) a) What are the key risk differences between smart-contract and conventional pawn-broker lending?

13. **Legal risks**

Lenders typically seek a profit. Therefore, conventional pawn-brokers often perform KYC so that they may seek recourse in the event their borrower's fail to pay or if loan sizes exceed value thresholds thereby requiring KYC by law. If parties who contract electronically (via smart contracts or automated exchanges) do not require KYC checks, they may face:

a. Compliance risks – developers or contracting parties who have breached laws may find themselves facing heavy fines, sanctions or even jail time for breaching the law because of law enforcement action using standard human intelligence, network monitoring techniques, etc.

b. Legal recourse risks – In the case of a breach or default, participants (borrowers or lenders) will find it more difficult to seek recourse because they do not know who they are dealing with. For this reason, many individuals and businesses insist on written contracts over the more difficult to demonstrate oral contracts.

13.2. **Documentation risks**

Parties often prefer to contract using written agreements because they make it easier to prove terms when disputes happen compared to oral agreements. If a pawn-broker finds their security is compromised by fraud, they may seek recourse and produce KYC information and a written contract to support their claim.

When contracting electronically (see Electronic Data Interchange (EDI)), prudent parties similarly ensure they have quality documentation, data storage and access control processes in place so that if a dispute arises, they can similarly prove their claims when seeking recourse.

As discussed above (see 2.3. New operational safeguards made possible thanks to the blockchain), the blockchain unlocks new capabilities for solving and automating away much of the cost, drudger and error associated with today's documentation and compliance procedures.

13.3. Collateral and liquidity risks

If the collateral in a 'smart-contract' scheme is a digital asset, it may be exposed to higher volatility compared to whatever a conventional pawn-broker takes as security.

Much of the trading on crypto exchanges is fake volume. Trading algorithms buy and sell from themselves to mimic real markets. What this has meant is that in the event of a large move, such as March 2020, the liquidity was not there. Exchanges had to shut down and reports are that entities like Tether had to shore up gamblers who were insolvent (see NASDAQ, The Crypto Market is Not Immune to Contagion Risk, https://www.nasdaq.com/articles/the-crypto-market-is-not-immune-to-contagion-risk).

13.4. Systemic risks

If one pawnbroker gets into financial trouble it does not affect all the other pawn brokers. This is not the case in the 'crypto' world as seen with the collapse of Terra, FTX, Genesis Trading and many others where one collapse meant big problems for associated entities.

The digital nature of often highly connected ‘crypto’ networks (compared to traditional pawn brokers) means that ‘smart contracting’ parties are exposed to, and feeding global systemic risks compared to the more physically negotiated in-person pawn-broker arrangements (see NASDAQ, The Crypto Market is Not Immune to Contagion Risk, https://www.nasdaq.com/articles/the-crypto-market-is-not-immune-to-contagion-risk).

The interoperability or ‘composability’ of smart contracts, meaning their ability to have dependencies that build upon one another, is similar to how existing derivative markets are often priced on differentials of differentials of other financial products.

Without requirements constraining such products to reference real-world assets, we find ourselves in a situation where contractors increase leverage and fragility in the global financial system. With blockchain markets now measured in the hundreds of billions or more, the risk is significant.

Many prominent investors, such as Warren Buffet, Charlie Munger, Ray Dalio, Nassim Taleb and many others have long warned of the perils of such practices and their increasing likelihood of creating cascading defaults even leading to sovereign debt crises.

Q13) b) Is there quantifiable data on the consumer outcomes in conventional pawn-broker lending compared with user outcomes for analogous services provided through smart contract applications?

13.5. Yes, quantifiable data does exist for consumer outcomes across both conventional pawn-broker lending and analogous digital contracts because such businesses have a profit motive to keep records and improve their operations. Whilst data exists, it is not necessarily freely accessible.

13.6. **Conventional pawn broking**

a. Industry data – providers such as IBIS world offer data associated with the pawn broking industry (see IBIS, Pawn Shops in Australia, 2022 https://www.ibisworld.com/au/industry/pawn-shops/5124/).

b. Consumer outcomes – contact and survey existing pawnbrokers directly.

Australian researchers have published on the topic and reported loan characteristics, default rates, etc, (see, The Pawnbroking Industry: Evidence from Victoria, by Nick Bienkowski and Kevin Davis, Department of Accounting and Finance, The University of Melbourne, 1997, https://kevindavis.com.au/secondpages/workinprogress/PAWNVICT.pdf).

Table 2: Loan Characteristics

Loan Size			
- Loans under $100	49%		
- Loans $100-$200	26%		
- Loans above $200	25%		
- Average Loan Size	$95		
Redemption Cost (after 1 mth.)	Cost ($)	Interest Rate[a] (monthly)	Interest Rate (annual)
- $20 Loan	23.82	19.1%	229%
- $100 Loan	115.27	15.3%	184%
- $500 Loan	565.00	13.0%	156%
- Average		16.6%	199%

[a] Note; all pawnbrokers charge a flat monthly interest rate with interest charged from the start of the month.

Table 3: Default Rates and Holding Period

Redemption		Non-Redemption	
- within 1 month	42%	- Loans under $100	29%
- within 3 months	40%	- Loans greater than $100	16%
- greater than 3 months	18%		
Average Loan Period			
- Agreed loan period	32 days		
- Holding period	60 days		
- Holding period for regulars	86 days		

13.7. **Analogous pawn-broking through electronic contracting or 'smart contracts'**

a. Exchanges – popular exchanges associated with analogous pawn broking or ‘staking’ schemes, such as Blockfi (https://blockfi.com/) and Celsius (https://celsius.network/) can be contacted for further information.

b. Developers and ‘DeFi’ securities issuers – information on loan terms, default rates, etc. can be obtained via the developers, issuers and reporters associated Ethereum tokens and protocols AAVE (https://aave.com/) and Compound (https://compound.finance/).

Q14) Some smart contract applications assist users to connect to automated market makers (AMM).

Q14) a) What are the key differences in risk between using an AMM and using the services of a crypto asset exchange

14. There are risks associated with both AMMs and crypto exchanges. In the case of crypto asset exchanges, a main source of risk is caused by the dependency of users on the crypto exchange as an entity. In the case of AMMs, there is a risk profile for each of the two main types of actors: end users (or ‘traders’) and ‘liquidity providers’ who contribute to the pool of available funds in an AMM in return for a share of the fees collected by the AMM.

14.1. Important solutions exist which can fundamentally eliminate some or all these risks and provide significant benefits to public and private sectors, including new asset recovery systems, split key systems, real-time proof of reserves, etc. as discussed above.

14.2. Key differences in existing risk between an AAM and using a crypto asset exchange – not using the innovative controls as suggested above – are summarised in the table below.

Risk	AMM	Exchange
Credit risk	Isolated to your counterparty (or counterparties) and the AMM.	Expanded to include the exchange operations.
Operational and counterparty risk	Limited to capabilities, your counterparty, and your chosen AMM. Using keys to transact (especially if not issuing new keys) may expose you to hacks and exploits.	Technical issues, downtime, preventing trades, policy (including fee) changes, suspending trading intentionally, misappropriation of funds (e.g., FTX, Quadriga CX).
Recourse risk	Faster (if you have collected KYC, terms and other key information associated with your deals).	Delays (MTGOX users still waiting after 10 years). Priorities (on bankruptcy, you may find yourself behind more senior creditors).
Compliance and fraud risk	If your AMM operates without KYC, you may end up holding blacklisted (forfeited) coins. Ability to swap volatile or illegal tokens.	If your Exchange doesn't manage KYC, you may end up holding blacklisted (forfeited) coins. Ability to swap volatile or illegal tokens.
Liquidity and market risk	Risk of exposure to higher price fluctuations or 'slippage'	
Direct loss risk	Liquidity providers may risk 'impermanent loss' of staked tokens due to market inefficiencies	

Q14) b) Is there quantifiable data on consumer outcomes in trading on conventional crypto asset exchanges compared with user outcomes in trading on AMMs?

14.3. Yes, it is likely that there is data on consumer outcomes in trading on both conventional exchanges and AMM. Conventional exchanges (though this may change with future models) have access to their users' data. And because many AMMs run on public networks, this may be easier to acquire compared to traditional OTC markets.

Contact

If you have any questions or would like to enquire about new innovations or operational capabilities, please contact nChain at contact@nchain.com or visit our website at https://www.nchain.com/.