Response to Australian Treasury Token Mapping Consultation

Submission on behalf of Brave New Coin Ltd.

March 2023

Introduction

Brave New Coin (BNC) creates proprietary and bespoke institutional grade indices that align to the most liquid areas of the cryptocurrency market. BNC has established an independent, unique and trusted reputation that is strongly aligned to global financial standards.

Since its launch in 2014, BNC has been a leading provider of aggregated pricing data for crypto assets. BNC's core indexing methodology has been independently audited against key IOSCO principles.

BNC now connects to over 250 individual exchanges, for the purposes of aggregating and calculating spot prices and reference rates for around 1,600 individual cryptocurrencies and digital assets (and their respective fiat and crypto pairs). In addition, BNC's pricing engine monitors and, to the extent possible, verifies exchange-traded volumes for calculating the aggregated rates, as well as measuring free-float supply and tracking market cap.

Using a combination of these volume-and market-weighted calculations, along with a series of documented and semi-automated data capture and quality processes, BNC has developed a core pricing engine that can generate spot prices, market reference rates, high-frequency price feeds, single asset indices and weighted basket or composite indices.

In the absence of formal standards around digital asset identifiers and classifications, BNC has also developed the **General Taxonomy for Cryptographic Assets** (a reference database and classification system for crypto assets and crypto tokens), which allows market participants to construct asset allocations within their portfolios, assess the potential risk profiles of individual cryptocurrencies and tokens, and track their holdings (including corporate actions such as hard forks). References to this Taxonomy are included in the responses below.

Responses to the Consultation Questions

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

BNC Response: Overall, we would advocate for a light touch approach to crypto regulation (beyond existing investor education and consumer protection). Specifically, we would like to see more certainty regarding regulatory treatment of the crypto ecosystem, without stifling innovation or introducing regulatory arbitrage. In particular, this approach should provide clarity to industry and market participants on regulatory oversight (where appropriate), avoid overlapping or conflicting rules and regulations), and minimise arbitrary and overly-broad restrictions (especially in the definition and application of "financial product" and "financial service").

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

BNC Response - There are several ways in which consumer protections and investor safeguards can be implemented, and largely within existing frameworks (e.g., legislation, regulation, industry codes of conduct, adoption of best practice frameworks, adherence to technical standards):

Disclosure:
Businesses and exchanges should be compelled to offer simple and explicit information about their goods, services, and potential hazards when investing in crypto assets. This can assist consumers and investors in making knowledgeable choices and informed decisions about whether to invest in crypto assets and how to minimise or mitigate the risks.

Insurance:
Insurance coverage can shield consumers and investors from financial losses brought on by theft or fraud. To protect their clients, businesses and exchanges should be mandated to maintain sufficient insurance coverage.

Regulation:
In addition to ensuring that businesses conduct themselves fairly and ethically, regulatory oversight can assist in establishing standards for security, accountability, and transparency. This can support market integrity and safeguard investors and consumers from dishonest or dubious business activities. Additionally, regulators could have the authority to demand that businesses submit to routine audits, as well as that they have enough capital and insurance to cover losses in the case of a breach or insolvency.

Security:
Robust security methods can aid in preventing theft and hacking, such as multi-factor authentication, cold storage, and encryption. Best practices for security and risk management should be mandated for businesses and centralised exchanges.

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

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?

BNC response: One approach as regards industry best practice might be to have a formal separation between project coding, and coding audits. Publication of detailed audits may have a negative effect (e.g., highlight how to take advantage of a code exploit), but high-level findings should be made available via appropriate channels, with subsequent remediation and resolution.

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?

BNC response: As regards token listings specifically: one solution may be to require exchanges to publish and maintain formal listing rules and criteria, and release regular reports and/or require continuous disclosure on tokens listed for trading, such as trading volumes, liquidity and market depth, and perhaps publishing decisions on why a token was declined a listing.

As regards consumer protection against potential crypto-related scams: as with all forms of financial, ID and data scams (theft, fraud, hacks, cyber-security breaches) that are prevalent across all sectors of business, banking, financial services, utilities, government services and personal data, there needs to be greater emphasis on consumer education, including better financial literacy, and taking more individual responsibility for managing personal and financial data. Many so-called crypto scams exploit vulnerabilities in the existing conduct of e-commerce, utilities, banking and personal financial services - in large part, these issues could be addressed by implementing self-sovereign digital ID, so that consumers get to determine what personal data is shared with whom, for what purpose and for how long.

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.

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?

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

BNC response: Whilst understanding that this concept has been adopted to achieve consensus on a high-level framework, it does not appear to be entirely satisfactory.

First, "use" and "control" are not entirely interchangeable in the way they are being used here (and may even be mutually exclusive?): for example, telco customers may have "exclusive use" of their personal mobile phone number, and with mandatory portability, customers can take this number to any network provider - but "exclusive control" (network access and inter-connectivity) still vests with the current network operator to which the number is connected.

Second, does "public data" in this context mean "data in the public domain", "data that is publicly available" (but still subject to copyright or other over-arching rights), or "data that users choose to make public" (even though it may be otherwise personal and/or exclusive")?

Third, by this definition, it would seem that not only mobile phone numbers, but also personal e-mail addresses, website domain names, IP addresses, Twitter handles etc. could be considered a "crypto token" (using the terminology in the Consultation document). Surely this is not the intended consequence?

Finally, in terms of "future proofing" the legislation - extending the telco and internet analogies used above, who within the telco industry could have anticipated VoIP? The initial response in the USA (regulatory, commercial, licensing) was to treat VoIP as a "phone service" (largely because it was a medium for carrying "voice" data over existing network infrastructure?). Incumbent telcos saw a threat to their existing voice business (even though they also controlled much of the internet infrastructure and on-line connectivity). Eventually, VoIP was classified as an "information service" - what was relevant was the purpose (to convey information) and the content (the data itself), and not necessarily the medium of carriage or transmission. Similarly, defining a "crypto token" as a "unit of digital information that can be 'exclusively used or controlled' by a person – despite that person not controlling the host hardware where that token is recorded" risks over-simplification. Rather, any proposed regulatory framework for "crypto tokens" should be sure to reference the underlying nature of the "data" (rights, purpose, form, etc.) that the "token" may represent, and not the technology that created it or the "network" to which it is connected.

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

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

BNC response: When we published our "General Taxonomy for Cryptographic Assets" in 2018 (see https://bravenewcoin.com/insights/brave-new-coin-launches-a-global-classification-standard-for-crypto-assets and https://bravenewcoin.com/enterprise-solutions/taxonomy) it was in response to two main observations:

1) A clear lack of formal standards for unique identifiers and consistent reference data for crypto tokens and assets
2) An obvious need to differentiate between different types and categories of crypto tokens and assets ("not all cryptos are the same")

There are parallels in traditional financial services: namely, the use of standardised entity, issuer, issue and instrument identifiers as well as standardised reference data and corporate actions; and where asset subclasses are used to distinguish between different types of equities, fixed income securities and derivatives (preference shares, non-voting shares; senior, secured, subordinated and unsecured debt; options, swaps, futures). These categories may have regulatory intent (e.g., wholesale vs retail products), they can aid risk assessment (credit ratings, capital adequacy, counterparty exposure) or they have evolved for contractual and structuring purposes (e.g., ISDA standard agreements).

A bespoke Taxonomy or Classification Framework for the crypto ecosystem can help to distinguish between the technical, economic and functional attributes of different categories of crypto tokens and crypto networks (separate to their treatment as "financial products" or "financial services"). It can assist in assessing inherent risks (design, technology, security, commercial) of individual protocols and networks, and when applied in the context of financial products, it can aid investment diversification, portfolio construction and performance attribution.

If designed effectively, a bespoke Taxonomy can expand and develop as technology evolves, without having to rewrite existing legislation. It supports the use and adoption of standards (similar to Securities Identifiers and Reference Data in traditional financial markets). It can also support comparative law analysis when reviewing cross-border regulation and passporting regimes.

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

BNC response: Unless structured properly, a bespoke Taxonomy with regulatory application may fail to keep up with technology and innovation. It may risk pigeonholing and even inhibiting new protocols and networks before they have had time to be assessed and evaluated (thereby stifling innovation), unless the Taxonomy is capable of adapting. It raises the risk of embedding inconsistencies within and across different regulatory models.

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.

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?**

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?**

BNC response: In principle, there should be no need to introduce reforms in this area - the wrapped asset (or perhaps the term "tokenized asset" is more appropriate in this context?) should be treated no differently to the underlying asset itself - it should be a case of "substance" over "form" (similar to dematerialised shares vs paper share certificates?).

However, there are three main areas in the actual operation of tokenized assets that may warrant further consideration:

1. Evidence that the underlying or real world assets actually exist, and are redeemable on demand - by the use of independent audits, collateral management systems and continuous asset valuations
2. In the case of certain goods (e.g., cars. artworks, luxury goods, collectibles) appropriate certificates of authentication, provenance, independent valuations and disclosures on past auction bidding and saleroom results)
3. Where financial products such as security tokens are concerned, technical standards and protocols to ensure tokens can only be transferred between qualifying holders/wallets.

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

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?**

BNC response: In principle, yes - users should be able to access relevant information as it relates to their use of a protocol or network. In the case of non-financial products and services, this can be achieved by the use of Technical White Papers, publications of Standard Terms and Conditions for network use, results of any independent smart contract audits, disclosures as to what technology may have been used to deploy a network or issue a token, and a clear statement of the rights and obligations that may attach to a token.

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

BNC response: Service providers could: adopt industry standards and best practices relevant to the sector or domain in which their services (and underlying networks and protocols) are designed to operate; apply for membership of recognized industry bodies and professional associations; obtain appropriate certifications and accreditation; and where relevant, participate in recognised external dispute resolution schemes. These suggestions are not intended to be exhaustive, nor should the absence of one or more of them deem the service provider, network or protocol to be disinterested in consumer outcomes.

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.

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

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

BNC response: Overall, we welcome this opportunity to bring regulatory clarity and market certainty to the definition of certain crypto assets and crypto services, both within the existing provisions of the functional perimeter, and especially with regard to non-financial products. In particular, the lack of an explicit definition of "utility token" has been seen as an obstacle to market development and innovation. This has been the cause of some frustration, since it can raise the presumption that a crypto asset is by default a financial product, financial service or security (and should be regulated as such) *unless it can be proved otherwise*.

In reality, and from a practical and objective perspective, there are other suitable and non-security definitions that can be applied to crypto assets that should not render them as financial products or services. However, this demands that the categorisation of crypto assets is approached holistically - using a combination of technical, functional, economic, financial, contractual and regulatory definitions.

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?

BNC response: We would refer to suggestions we have made elsewhere in our responses e.g., the use of independent smart contract audits, regular asset audits, collateral management tools, and protocols for asset transfers.

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?

BNC response: We don't believe there is any need for such restrictions beyond those imposed by the financial services framework. Again, this does raise the need for a specific definition for "utility" tokens, non-financial network tokens, and tokens that resemble software licences or subscription agreements.

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?

BNC response: We are not convinced of the need for specific regulation for the marketing and promotion of crypto products that do not constitute financial products or financial services. Surely non-financial products and services are already covered by existing laws with respect to the sale of goods and services? Isn't the principle to remain technologically agnostic with respect to regulation?

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

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

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

BNC response: Unless Treasury is planning to mandate or approve the use of certain smart contracts (or smart contract applications) over others, the solution will largely come from a combination of: independent smart contract audits (even where open source software has been used); making data available that shows how often a piece of open source code has been deployed; adopting appropriate software standards such as ISO specifications; and tracking the number and/or impact of known exploits or hacks. Ultimately, the choice of smart contract (or application) has to be based on whether or not it is fit for the express or intended purpose it was designed to be used for.

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).

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

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

BNC response: Smart contract lending and conventional pawnbroker lending are two different approaches to lending that involve different levels of risk. Despite the fact that both structures are viable lending models, they have different approaches to risk management and counterparty risk. The following are the main risk variations we have identified between these two types of transactions:

Counterparty Risk:
In traditional pawnbroker lending, the borrower offers collateral in the form of a tangible asset, such as jewellery or other valuable goods, which the pawnbroker keeps as security for the loan. The pawnbroker may sell the collateral to recoup their losses if the borrower defaults on the loan. In smart contract lending, the security is often kept in the form of a blockchain-based cryptocurrency or token. The requirement for a

central authority is removed, but the danger of counterparty default is increased since the value of the collateral can fluctuate and be exposed to sharp price changes.

Liquidity Risk:
In smart contract lending, the collateral is often kept in a decentralised liquidity pool, which is administered by a smart contract. Due to the ease with which borrowers can enter the pool and withdraw their collateral upon loan repayment, this enhances both liquidity and flexibility. Pawnbroker financing, in contrast, requires tangible collateral that could be more challenging to liquidate quickly.

Operational:
Given that smart contract lending uses blockchain technology and smart contract programming, it has a higher level of technical sophistication. This could create new dangers like the potential of coding errors, exploits of known vulnerabilities, hacking, or technological issues. On the other hand, traditional pawnbroker lending is a more established and understood business model with fewer operational risks or technical difficulties.

Transparency:
The loan terms and the collateralization procedure can be easily examined and tracked because smart contracts are transparent and immutable. Combined with the use of smart contract oracles to source current market prices and valuations, this lowers the possibility of fraud or collateral mispricing, and guarantees an honest and open loan process. Conversely, traditional pawnbroker lending is based on relationships and trust, which can be more challenging to prove and follow, especially the risk associated with ownership and provenance of pledged goods.

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

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

BNC response: Crypto asset exchanges and automated market makers (AMMs) are both ways to trade crypto assets, but they take different approaches to risk management, order execution, and liquidity provision. The following are the main risk differences between using an AMM and a crypto asset exchange:

Liquidity Risk:
AMMs rely on liquidity pools to facilitate trades, which are maintained by other users who deposit their crypto assets into the pool. The liquidity of an AMM depends on the size of the pool and the volume of trading activity. If there is a sudden surge in trading activity, the liquidity pool may not be able to keep up, which can result in slippage and higher transaction fees. Crypto asset exchanges, on the other hand, typically have centralised order books that provide greater liquidity and more efficient pricing.

Counterparty Risk:
With an AMM, trades are executed automatically and anonymously, without the need for a counterparty. This can reduce the risk of counterparty default, as there is no one on the other side of the trade to default on their obligations. In contrast, when using a crypto asset exchange, traders may be exposed to counterparty risk if the exchange is hacked or experiences liquidity problems. (On Counterparty risk, we

note that ASIC has signalled plans to regulate crypto exchanges, and to regulate custody, which would address these issues.)

Price Risk:
AMMs use a mathematical formula to determine the price of a crypto asset, based on the ratio of the two assets in the liquidity pool. This can result in price slippage, especially for large trades, as the price may shift significantly based on the size of the order. Crypto asset exchanges, on the other hand, typically provide more stable pricing, as they match buyers and sellers based on their order book.

Smart Contract Risk:
AMMs rely on smart contracts to execute trades and manage the liquidity pool. There is a risk that these smart contracts may contain bugs or vulnerabilities that could be exploited by attackers, resulting in the loss of funds. Crypto asset exchanges also face similar risks, such as the risk of hacking or insider trading.

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

BNC response: The available data comparing consumer outcomes in trading on conventional crypto asset exchanges with user outcomes in trading on automated market makers (AMMs) is limited, and direct comparisons are difficult. One research study indicates that AMMs often have higher transaction fees and lower liquidity than centralised exchanges, which can lead to higher costs for traders. In contrast, another study shows that traders on AMMs, specifically Uniswap and SushiSwap, generally earn higher returns than those on centralised exchanges. However, the same study highlights that trader performance varies widely, with some earning substantial profits and others incurring significant losses. The data presents a mixed picture regarding consumer outcomes in trading on conventional exchanges versus user outcomes in trading on AMMs, as while some studies suggest that AMMs may offer higher returns, others note potential drawbacks such as higher fees, lower liquidity, and greater volatility.

Moreover, a research paper published in the Journal of Financial Economics in 2021 analysed the price impact of trading on AMMs versus centralised exchanges. The study found that the price impact of trading on AMMs was lower than that on centralised exchanges, indicating that users were able to trade more efficiently on AMMs." Links to research references mentioned here::

Dune Analytics report on DEXs and CEXs trading volumes and fees in 2021:
https://dune.xyz/dashboard/duneanalytics/Dex-Wars-2021

Delphi Digital report on AMMs versus centralised exchanges returns:
https://www.delphidigital.io/reports/automated-market-makers-a-retail-traders-dream

Price impact and liquidity provision on automated market makers:
https://www.sciencedirect.com/science/article/pii/S0304405X2100113X