Token Mapping Consultation Response
February 2023

Company
Greythorn Asset Management

Sector/Industry
Cryptocurrency & Web3 Investment Services

GREYTHORN
ASSET MANAGEMENT

A. Background

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

As the crypto ecosystem continues to evolve, the government must find a balance between protecting consumers and fostering innovation, all the while allowing for a two-way conversation to occur between regulators and developers to create a flexible and dynamic approach towards allowing a new subset of asset classes and systems to be developed over the next few decades.

In our view, the role of the government is not to wholly govern the blockchain ecosystem but to encourage positive utilisation of the technology, spur innovation and collaborate with developers, users, consumers and financial product designers to establish the groundwork for a dynamic regulatory environment which allows the space to be “future-proof” instead of implementing harsh reactive regulatory controls and protection only when black-swan events such as when the downfall of LUNA, UST, FTX, Celsius and Voyager occur.

This idea resonates with the original founding ideals which Satoshi Nakamoto had established well in advance with the creation of Bitcoin. The P2P Bitcoin ideology came from the regulatory oversight of products within the centralised financial systems created behind closed doors. It is lobbied by well-established entities and individuals with financial incentives to extract as much value from unsuspecting consumers and investors.

While blockchain technology and cryptocurrencies have tremendous potential for decentralised finance and other applications, they also come with risks like hacking, volatility, and fraud. Blockchain technology brings forth a financially inclusive, decentralised and open system whereby anyone can trust a centralised entity and verify transactions and statements within a distributed public system that allows for the free flow of information and financial opportunities for all. Therefore, the government must establish policies and regulations that mitigate these risks without stifling innovation.

One possible step the government could take is to provide clear guidelines for the use and regulation of cryptocurrencies and blockchain technology. The government could take this one step further and establish an open communication network between inter-regulatory bodies, developers and financial participants who would allow for amicable consensus of the foundation for the web3 industry, setting dynamic standards for crypto exchanges, ensuring transparency in token offerings, and clarifying tax laws that relate to cryptocurrencies, especially those that are within the “intermediate token system” classification outlined by the Token Mapping paper.

Another critical aspect is educating the public on cryptocurrencies and the associated risks. The government could collaborate with universities, community groups, and other stakeholders to offer education on cryptocurrencies and their risks. Ultimately, a well-informed public can make better decisions about participating in the crypto ecosystem, while the government can protect consumers and promote innovation in the space.

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

Safeguards for consumers and investors are essential to ensure that the benefits of cryptocurrencies are not offset by their risks. Some potential safeguards could be implemented:

- *Disclosure requirements:*
  Crypto companies should disclose information about the risks associated with their products and services and any potential conflicts of interest. This information should be easily accessible to the public and presented clearly and concisely.

- *Code auditing:*
  Third-party firms should audit smart contracts and blockchain protocols to identify vulnerabilities or bugs that hackers could exploit. This could help prevent catastrophic incidents like the DAO hack, which resulted in the loss of millions of dollars worth of Ether. The government would be interested in collaborating with current 3rd party attestation/blockchain entities involved heavily within the crypto industry to vet potentially harmful code, technology implementation and projects (namely Chainanalysis, Rugdoc, Prismatik).

- *Consumer protection laws:*
  Existing consumer protection laws should be extended to cover the use of cryptocurrencies, ensuring that consumers have legal recourse in case of fraud, misrepresentation, or other wrongdoing.

  The token Mapping exercise assists within this scope to understand what assets within the crypto space allow, as this would cut many “scams” outright within any regulatory reach. However, being decentralised, it will not only be the government’s responsibility to protect consumers but also for both consumers and developers to educate and provide education within the potential edge-use cases of blockchain technology.

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?**
- **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?**

➔ **a)** Several solutions could be implemented to safeguard consumers using crypto assets. One potential solution is the implementation of disclosure requirements, as mentioned above. Additionally, exchanges and other crypto service providers could be required to maintain specific minimum cybersecurity and data protection standards.

Another potential solution is establishing a regulatory framework for crypto assets that ensures the safety and stability of the underlying infrastructure. This could include setting up a system of independent auditors to oversee the operation of exchanges and other service providers.

➔ **b)** To prevent consumers from being exposed to scams involving crypto assets, regulatory levers such as licensing, registration and certification could be implemented to prevent consumers from being exposed to scams involving crypto assets. This would help ensure that only legitimate exchanges and service providers can operate in the space, specifically on fiat on/off ramps.

Additionally, penalties for non-compliance could be increased to deter bad actors from operating in space. The government could also establish a regulatory sandbox, allowing new and innovative crypto projects to operate under relaxed regulatory conditions while still ensuring consumer protection.

In conclusion, the government has an important role to play in the regulation of the crypto ecosystem. By implementing policies and safeguards that protect consumers and investors while still fostering innovation, the government can help ensure that the benefits of cryptocurrencies and blockchain technology are realised while minimising the risks to the overall ecosystem.

B. Token Mapping: Terminology & Concepts

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 tokens and crypto networks for the purposes of future legislation?**
- **b) What are the benefits and disadvantages of adopting this approach to define crypto tokens and crypto networks?**

- **a)** The concept of 'exclusive use or control' of public data can define crypto tokens and crypto networks in legislation by clarifying that these tokens and networks have a unique quality that distinguishes them from other data records. This concept can be used to differentiate crypto tokens and crypto networks from other types of digital assets and to provide a clear definition that can guide regulatory oversight and ensure consumer protection.

- **b)** The benefits of adopting this approach to define crypto tokens and networks include greater clarity for regulators and consumers and more effective regulation and consumer protection. However, there may also be disadvantages, such as potential difficulties in applying the concept in practice and the possibility of unintended consequences resulting from overly broad or narrow definitions. Additionally, the definition may need to be updated regularly to keep pace with rapidly evolving technologies in the crypto space.

Q5) This paper sets out some reasons 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?**
- **b) What are your views on creation of a standalone regulatory framework that relies on a bespoke taxonomy?**
- **c) In the absence of a custom 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?**

- **a)** Additional supporting reasons for the value of a bespoke taxonomy include providing clarity and consistency in the regulatory treatment of different types of crypto assets, facilitating the development of industry standards and best practices, and enabling effective risk management and supervision by regulators. Alternative views may suggest that existing regulatory frameworks can adequately address the risks associated with crypto assets without needing a separate taxonomy.

- **b)** Creating a standalone regulatory framework that relies on a custom taxonomy can be beneficial if it provides clear and comprehensive guidance on the regulatory treatment of different types of crypto assets, reduces regulatory uncertainty, and promotes innovation and growth in the crypto industry.

  However, it should be designed in a flexible and adaptable way to the rapidly evolving nature of the crypto market. Especially as noted in the paper, a bespoke taxonomy may cripple the innovation in the space as much of the breadth of possible functions within the web3 token classification is theoretically non-exhaustive.

- **c)** In the absence of a bespoke taxonomy, regulatory certainty for individuals and businesses using crypto networks and assets in a non-financial manner can be provided by applying existing regulatory frameworks, such as data protection laws, consumer protection laws, and anti-money laundering regulations. Regulators can also provide guidance and education to promote awareness and understanding of the risks and opportunities of using crypto assets.

Furthermore, we would argue that the absence of a bespoke taxonomy allows inter-regulatory entities to collaborate with developers and users within the ecosystem to establish open communication and discussion on regulatory certainties that could be implemented. Taking examples of decentralised protocols such as Uniswap, Blur, and many others, regulatory bodies could provide non-financial clarity (clear public messaging of issues and systems) to provide clarity on the correct language, structure and structure and framework of a token ecosystem.

C. Intermediated Token Systems

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?**

➔ **a)** Reforms may be necessary to ensure that a wrapped real-world asset gets the same regulatory treatment as the asset backing it. This is because the current regulatory framework for cryptocurrencies and traditional assets is not designed to address the unique characteristics of wrapped assets. Specifically, there may be concerns around the accuracy and verifiability of the underlying asset, as well as issues related to custody and control. One potential reform could be to create a new regulatory framework specifically for wrapped assets that takes into account their unique features.

➔ **b)** Reforms may also be necessary to ensure that issuers of wrapped real-world assets can meet their obligations to redeem the relevant crypto tokens for the underlying good, product, or asset. This is because the redemption process may be subject to various risks and uncertainties, including counterparty risk and market volatility. One potential reform could be to require issuers to provide regular updates on the underlying asset and to maintain adequate reserves to meet redemption obligations. Additionally, issuers may need to implement robust risk management practices to ensure that they are able to fulfil their obligations even in adverse market conditions.

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

- **a)** Yes, crypto asset service providers should be required to ensure their users can access information that allows them to identify arrangements underpinning crypto tokens. This can be achieved through disclosure requirements that mandate providers to provide clear and concise information about the underlying assets or arrangements that support the tokens. Providers could also use blockchain technology (Proof of Reserves, transaction IDs) to create transparent and immutable records of the underlying assets or arrangements, which users can access and verify by a third party.

- **b)** Besides providing information about underlying assets, crypto asset service providers could take other initiatives to promote good consumer outcomes. For example, they could implement robust security measures to protect user funds (Custodial Solutions - MPC, Multi-Sig Wallets, 2FA and others) and personal information, provide clear and concise information about fees and charges, offer dispute resolution mechanisms, and provide education and resources to help users make informed decisions about investing in crypto assets.

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?**

- a) Whether or not a specific kind of intermediated crypto asset should be defined as a financial product depends on various factors, such as the asset's characteristics, risks, and potential benefits. Some intermediated crypto assets may have similar features to traditional financial products, such as securities or derivatives, and may pose similar risks to investors. In such cases where clear and exact similarities could be drawn between traditional products to the corresponding cryptocurrency equivalent are evident, it may be appropriate to define them as financial products.

  Nonetheless, in our view, any regulatory definition of an intermediary asset as a financial product should be openly reviewed and workshopped between developers, users and inter-regulatory bodies to ensure that decentralised equivalent products that are offered in a much more constructively clear and verifiable manner are not gated to only the privileged few and stifled by reactionary regulative actions imposed due to edge-case events such as Luna and FTX.

  Thus, we would argue that no set kind of *truly* decentralised intermediated crypto assets exist. Such a categorisation should be focused on centralised offerings that would have lasting damage within the ecosystem.

- b) Similarly, some crypto asset services, such as custodial services or investment advice, may have features resembling traditional financial products or services with similar risks and benefits. Defining such services as financial products may provide

regulatory oversight and consumer protections. However, defining a crypto asset service as a financial product should be based on a thorough analysis of its characteristics and potential risks and benefits.

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?

Assessing the suitability of a specific public crypto network to host wrapped real-world assets requires considering several factors. These include:

- *Technical capacity and security:*
  The public crypto network should have the technical capacity and security features required to handle the volume and complexity of the transactions in wrapping real-world assets. This includes speed, scalability, and resistance to hacks and attacks.

- *Governance and compliance:*
  The public crypto network should have robust governance and compliance mechanisms to ensure that the rules and standards governing the wrapping and trading of real-world assets are followed. This includes mechanisms for dispute resolution, regulatory compliance, and risk management.

- *Market demand and liquidity:*
  The public crypto network should have sufficient market demand and liquidity to support trading wrapped real-world assets. This includes factors such as the size and diversity of the network's user base, the availability of market-making and liquidity-provision services, and the ability of users to convert wrapped assets into other crypto or fiat currencies easily.

- *Legal and regulatory considerations:*
  The public crypto network should operate within a legal and regulatory framework that provides clarity and certainty regarding the treatment of wrapped real-world assets. This includes factors such as the network's jurisdiction, applicable laws and regulations, and the level of regulatory oversight and supervision.

In assessing the suitability of a public crypto network to host wrapped real-world assets, regulators may also consider factors such as the track record and reputation of the network, the quality of its technical and legal infrastructure, and its ability to innovate and adapt to changing market conditions. An example of a good public crypto network would be one that closely resembles a more decentralised network, with Node counts and validator numbers as two main metrics in choosing suitable public crypto networks to host wrapped RWAs.

Ultimately, the goal is to ensure that intermediated crypto assets are issued and traded in a safe, transparent, and efficient manner that protects the interests of investors and promotes market integrity.

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?

Yes, there should be limits, restrictions or frictions on the investment by consumers in relation to any arrangements not covered already by the financial services framework. This is because such investments can be risky, and consumers may not fully understand the nature of the underlying arrangements. Without appropriate safeguards, consumers could be exposed to fraud, misrepresentation, or other forms of misconduct.

Therefore, ensuring that intermediated crypto assets are subject to appropriate regulatory oversight and that investors are provided with adequate information to make informed investment decisions is important. This could include measures such as disclosure requirements, investor suitability assessments, and limits on the size or type of investments that consumers can make in intermediated crypto assets.

D. Public Token Systems

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?

A regulatory framework to address the marketing and promotion of products within the crypto ecosystem may be suitable for Australia to ensure consumer protection and promote market integrity. Such a framework could be implemented by requiring issuers and promoters of crypto products to comply with certain disclosure requirements, such as providing clear and accurate information about the risks associated with the product, its features and functionality, and the underlying technology.

A great example of currently ongoing regulatory changes are being done in Dubai, whereby the government has set up a regulatory framework and entity to oversee the innovation within the web3 space in Dubai. One suggestion could be to implement a similar framework for Australia, allowing not only just a regulatory sandbox (such as the CDBC project) but also encapsulating a collaborative inter-regulatory exercise between the Treasury, ASIC and also web3 developers which would create a more synergistic and technologically expansive approach towards regulating the web3 industry.

To conclude, regulatory oversight could be strengthened through the use of dynamic regulatory sandboxing of potential projects, potentially creating frameworks inspired by the regulatory building blocks presented by the Dubai government and its underlying Blockchain Council licensing requirements and enforcement measures for projects. It is important to balance consumer protection with innovation and avoid imposing overly burdensome

requirements that stifle innovation and growth in the sector. Any regulatory framework should also be flexible enough to adapt to the evolving nature of the crypto ecosystem.

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?**

➔ **a)** Regulatory and policy levers that can encourage the development of smart contracts that comply with existing regulatory frameworks include:

- *Education and outreach:* Educating developers on the regulatory requirements and implications of their smart contracts can increase compliance and reduce the risk of unintended legal violations.
- *Collaboration with regulators:* Regulators can engage with developers to understand the technology and provide guidance on how to design smart contracts that comply with existing regulations.
- *Incentives:* Providing incentives for compliance, such as tax breaks or funding opportunities, can encourage developers to create smart contracts that comply with existing regulatory frameworks.

➔ **b)** Regulatory and policy levers that can ensure smart contract applications comply with existing regulatory frameworks include:

- *Regulatory oversight:*
  Regulators can monitor smart contract applications for compliance with existing regulations and take enforcement action against non-compliant applications.

- *Mandatory compliance requirements:*
  Regulators can require smart contract applications to comply with specific regulations or standards, such as data protection or anti-money laundering regulations.

- *Self-regulation:*
  The development community can establish self-regulatory standards and best practices that promote compliance with existing regulations.

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 analogous services provided through smart contract applications?**

➔ **a)** The key risk differences between smart contracts and conventional pawn-broker lending include transparency, enforceability, and dispute resolution issues. Smart contracts are typically self-executing and enforceable through code, which can reduce the risk of fraud and counterparty risk. However, smart contracts may not be transparent to all users and may be subject to programming errors or hacks.

Conventional pawn-broker lending, on the other hand, is typically more grounded in traditional brick-and-mortar businesses, allowing for a perceived notion of “safety” for consumers as you would be engaging your loan with a business. Nonetheless, we would argue that the risk here is that a consumer would not see the process of how the APY for a loan would be structured and offered to them, potentially allowing the brokers to potential APY gauging and malpractices, which would be detrimental to the consumer but very beneficial to the loan originator.

Such a risk is mitigated in a smart-contract system, whereby users, consumers and developers could verify and confirm the source of truth and calculation of a particular borrowing rate based on a set number of factors such as the TVL, risk metric of a given asset and its availability within the lending protocol. This brings transparency and reduces the “information risk” that the consumer bears, further distributing it and allowing the market to price an efficient borrowing/lending rate for both the consumer and lending protocol asset provider.

Essentially the key difference in both instances would be the transparency of how each different iteration of loan origination could provide the best outcome for the borrower and lender.

➔ **b)** There is limited quantifiable data available on consumer outcomes in conventional pawn-broker lending compared with user outcomes for analogous services provided through smart contract applications. However, some studies suggest that using smart contracts for collateralised lending may offer benefits such as lower costs, faster processing times, certain flexibility and greater accessibility.

Lower costs for consumers are felt via the lower borrowing APY observed in various web3 lending asset pools, with rates as low as 0.77% (wBTC), 2% - 4% for stablecoins (USDC, USDT) and as high as 15.47% (BAL) on AAVE. In comparison, pawnbroker lending typically would provide lending capital with a requirement of at

least 18% APY on principal.

Furthermore, within pawn-broking operations, collaterals are typically self-evaluated by pawnbrokers and could be detrimental to the market value of a consumer's asset. This means that, on average, the typical pawnbroker would value a USD 10,000 asset and offer a loan of up to 60%-80% of the notional amount. Depending on which protocol a consumer utilises, DeFi alternatives allow for greater flexibility in collateral and its assets.

Faster processing times are dependent on what the consumer requires the funds for. Both pawnbroker and DEFI lending platforms do not require the lengthy process of KYC/AML for the funds that are being borrowed. However, with the speed of how transactions are confirmed, if a user generates a transaction to collateralise and borrow funds from Maker, funds typically would get released near instantaneously due to the deterministic outcomes that smart contracts provide, whilst pawn-broker lending may be subject to further internal reviews (or lack thereof) before the release of funds.

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

➔ **a)** One key difference in risk between using an AMM and using the services of a crypto asset exchange is that AMMs are decentralised and operate based on predetermined rules set in code. In contrast, crypto-asset exchanges are centralised and typically operated by a single entity.

AMMs do not require the custody of assets as tokens are held by each user within their web3 wallet. In contrast, custody is surrendered to the centralised entity within a crypto asset exchange. This means there may be less transparency and accountability in a centralised exchange, whilst potential vulnerabilities to code exploits or other technical issues may plague AMMs, especially newly launched projects.

The key differences between the risk of using an AMM and Central Exchange would encompass the following issues:

1. Custodial Risk:
As mentioned previously, due to the nature of AMMs and self-custodied assets, the risk of losing assets via phishing attacks is prevalent within DeFi, whereby attackers attain users' private keys through phishing methods such as malicious fake links, Trojan malware, and prevalent phishing code available within Discord, Telegram, and Twitter channels.

When users transact within centralised exchanges, the self-custodial risks associated with phishing scams to attain private keys dramatically decrease, as exchanges would be expected to have security systems (MPC solutions, hot/cold wallet segregation, etc.) to prevent third-party exploits. Nonetheless, centralised exchanges inherently carry risk, as multiple instances over the past ten years have indicated that funds within a centralised (non-regulated) entity would be at risk due to conflicts of interest (exchange owners running away with customer funds or the most recent case - FTX commingling of user funds with Alameda Research) and are still subject to specific phishing tactics that may let third-party exploits occur for users of centralised exchanges.

Some users may not have the required operational security to safeguard their assets, which may lead to external exploits if they are not educated in proper crypto custodial management. However, in both instances, there is a crucial difference in trust. In using AMMs, users would trust that their operational security would be sufficient to safeguard their assets while using centralised exchanges would require the user to trust the centralised exchange.

2. Platform Risk:
The Risk of potential vulnerabilities to code exploits or other technical issues, especially within the protocol level in an AMM (i.e. ‘migrator’ code in Pancakeswap AMM forks). This is especially true with newer platforms/dApps that come into the market, and users may risk losing their assets if projects do not have the best intentions (e.g. the abuse of the ‘migrator’ code from Pancakeswap on various AMM forks which allows teams to syphon funds from AMM Liquidity Pools within the dApp) or simply had a bug/exploit that was not discovered by the team/external audits such as reentrancy attacks, router exploits, flash loan attacks, price oracle attacks that allow black-hat actors to drain assets out of AMMs and DEFI dApps.

Due to the inherent simplicity of just offering a marketplace, centralised exchanges would not have these attacks/exploits that would have occurred due to bugs/vulnerabilities; however, users would be exposed to platform risks such as price manipulation, stop hunts, wash trading and various potentially dubious activities that have had been occurring in centralised exchanges in the past.

3. Token Risk:
In an AMM, tokens are traded directly between liquidity pools, typically comprising various tokens. Users, thus, would have to confirm the token contract of each asset intended for trading. On the other hand, users would generally rely on the responsibility of exchanges to list non-exploitive assets that are “safe” - essentially trusting the exchange's ability to list quality projects within the marketplace.

Additionally, AMMs may have limited liquidity for specific tokens, which can result in slippage when making trades. On the other hand, centralised exchanges typically offer more liquidity for a broader range of tokens.

Ultimately, the critical differences in risk between using an AMM and using the services of a crypto asset exchange lie in the placement of users’ trust, be it with

themselves on their operational security or with a centralised exchange, its legitimacy and regulation.

➔ **b)** Various studies have been published concerning AMM trading efficiency in relation to trading fees, Market Making performance (impermanent losses/gain) and liquidity. Several notable papers are:

1. BIS paper: Trading in the DeFi Era - automated market-maker
2. SNB paper: On The Quality Of Cryptocurrency Markets

Quantifiable data on consumer outcomes in trading on conventional crypto asset exchanges compared with user outcomes in trading on AMMs. For example, a study by DappRadar found that the average user on decentralised exchanges (which include many AMMs) traded smaller amounts than users on centralised exchanges but made more frequent trades. Additionally, the same study found that users on decentralised exchanges experienced higher gas fees (i.e. transaction fees paid to miners) and longer wait times for transactions to be processed.

GREYTHORN
ASSET MANAGEMENT