Contents

Bitcoin Babe PTY LTD www.bitcoin-babe.com **ACN:** 613 688 707
DCE: DCE100575454-001 PO Box 4228 Penrith Plaza NSW 2750 enquiries@bitcoin-babe.com

1: Introduction

1.1: Foreword

In the past, government engagement has started – and stopped – at the line of an industry group within the cryptocurrency community. For the best chance of rectifying past decisions and advancing the future of the cryptocurrency space in Australia, industry engagement must come from more sources - not just the "select few" privileged enough to afford membership in industry groups.

In my experience (as made evident by my interactions with AUSTRAC and the ATO), government entities have approached a significant portion of their regulations and regimes with resources and decisions influenced by orderbook exchanges. This is primarily because “orderbook exchanges” comprised the substantial share of this industry group’s DCE membership base.

The cryptocurrency industry has since progressed and now encompasses a broader range of DCE subtypes more than just "orderbook exchanges." Subsets include OTC desks, peer-to-peer traders, Bitcoin ATMs, and brokers. As Australia's largest peer-to-peer trader, I have never been contacted by any government agency, ombudsman service, or not-for-profit organisation seeking to better understand the industry and how our requirements differ from those of an orderbook exchange or any other type of DCE business.

As such, it should be noted that my perspective on these issues and concerns may not necessarily reflect the DCE economy as a whole, but rather the peer-to-peer industry in particular.

1.2: Executive Summary

Following on from the Day 3 discussions at the Senate Committee enquiry into Australia as a Technology and Financial Centre on the 8th of September, the Committee requested an outline of the issues faced by Bitcoin Babe PTY LTD as a cryptocurrency business in Australia, and the impacts on myself as the owner of this business.

This paper has been prepared as requested, and seeks to detail the issues as well as proposed options/recommendations which could benefit the cryptocurrency industry which faces the same difficulties and will address the following topics:

- DCEs should be licenced and regulated, and the same should those who offer cryptocurrency "financial advice" services. There are AFSL criteria which may be readily replicated from current service and financial adviser regulations. Policymakers and ASIC should determine whether this comes within the jurisdiction of an AFSL or a newly established licencing category.
- In order to establish an effective regulatory framework for the cryptocurrency economy, ASIC and key industry participants need to organise working groups to guarantee that all problems and concerns are conveyed properly and succinctly with input by those with industry expertise.

Bitcoin Babe PTY LTD www.bitcoin-babe.com **ACN:** 613 688 707
DCE: DCE100575454-001 PO Box 4228 Penrith Plaza NSW 2750 enquiries@bitcoin-babe.com

- In its present form, the AUSTRAC registration procedure is inadequate and useless. Because regulations are not actively enforced on each DCE and are instead evaluated on a "case by case" basis, this creates gaps or "blind spots" for incompetent DCEs to slip into.
- There is presently no independent dispute resolution for DCEs or cryptocurrency-based services. AFCA should take a more active role through the creation of a department dedicated to cryptocurrency complaints and dispute settlement. If AFCA refuses to take on this role, resources and advice should be given to a suitable sector organisation (e.g., Blockchain Australia, Fintech Australia) to help them create a cryptocurrency-specific impartial dispute resolution body comparable to AFCA.
- The process of onboarding, managing, and offboarding a DCE from a financial institution is non-existent; banks and DCEs are not having an open conversation about cryptocurrency, exchange services, and consumer safeguards. Despite the fact that banks and financial organisations have been requested to engage with the industry on numerous occasions, they have to date repeatedly turn down this offer. This must be changed.
- Alternative payment methods which are labelled as "cryptocurrency friendly" come with a plethora of limitations and requirements, not to mention the fact that they are unreasonably costly. Larger organisations that have the resources available to meet these requirements and costs adopt these methods which in turn impacts smaller/independent firms and limiting the formation of new DCEs do not have the same resources at hand. This mindset will result in an oligopoly amongst bigger providers, similar to the present banking scenario of the "big four".
- Despite repeated warnings placed in as many places as possible across my own services, consumers continue to fall victim to scammers. Despite the efforts of industry consumer protection organisations (such as the ACCC, DCEs, Cyber.gov, and others) to educate consumers, according to recent ACCC statistics, it is apparent that the message is not getting through. Even if we can all sympathise with individuals who have been duped, a more systematic approach to consumer education on the dangers and responsibilities associated with cryptocurrency purchases is required.

Bitcoin Babe PTY LTD www.bitcoin-babe.com **ACN:** 613 688 707
DCE: DCE100575454-001 PO Box 4228 Penrith Plaza NSW 2750 enquiries@bitcoin-babe.com

2: Regulation and ASIC involvement

> *Licensing and regulation should apply not only to DCEs, but also to those who provide cryptocurrency "financial advisory" services. Numerous AFSL requirements can be easily copied from existing provisions governing services and financial advisors. Whether this falls under the purview of an AFSL or a newly created licencing category should be a matter for policymakers/ASIC to decide.*
>
> *ASIC and relevant industry members should form working groups to ensure that all issues and concerns are communicated clearly and concisely in order to create an efficient regulatory system for the cryptocurrency economy.*

2.1: Custodial Requirements

2.1.1: Issue: DCE Subtypes

There are several types of DCEs (for example, peer-to-peer traders, crypto atm services, and so on) that do not take custody of customer cryptocurrency or funds.

2.1.2: Solution: DCE Subtypes

These types of services require recognition and leniency where custodial requirements are concerned, which should be clearly defined in any application or dealings with ASIC or other interested industry bodies.

2.1.3: Issue: Defined custodianship attributes

Custodianship requires specified characteristics, such as the duration of a DCE's custody over a customer's funds or cryptocurrency, in order to be considered a custodial agreement.

> *A customer engages a DCE to purchase cryptocurrency for the purpose of exchanging it for goods or services. A prepayment is made to the DCE with the intent of executing an order within 48 hours, thereby limiting potential loss in an unstable market. As the DCE has no intention of acting as a custodian, the registration requirements should be different than for a DCE that takes custodianship of a customer's funds/cryptocurrency for a "long term" period.*

2.1.4: Solution: Defined custodianship attributes

Provide a clearly defined time period during which a DCE may retain a customer's funds for the purpose of later executing an order. If the funds held are not used within a specified time period, they should be returned to the customer. Where funds are not returned, a penalty may be assessed (as the DCE is taking on a custodianship role without proper permission).

Where funds cannot be returned (e.g., a mistaken payment that is unclaimed), provisions should be made for their allocation to a trust, which has its own set of requirements and does not fall under a custodianship arrangement.

Bitcoin Babe PTY LTD www.bitcoin-babe.com **ACN:** 613 688 707
DCE: DCE100575454-001 PO Box 4228 Penrith Plaza NSW 2750 enquiries@bitcoin-babe.com

2.2: Duty of Disclosure

2.2.1: Issue: DCE's and Cryptocurrency/Token issuers conflict

Numerous exchanges have benefited financially from listing specific cryptocurrencies or tokens through the use of undisclosed agreements with issuers. Currently, there is no requirement to disclose the existence of such an agreement, which may lead to consumers making poor investment decisions based on a "trusted service" listing a trading pair.

2.2.2: Solution: DCE's and Cryptocurrency/Token issuers conflict

Where a DCE has been compensated financially to list a particular trading pair with a cryptocurrency/token, the pair must be distinguished from others in some way that alerts consumers to its "paid" status (similar to a "sponsored post" on social media or the disclosure of advertisements).

2.3: Independent dispute resolution

2.3.1: Issue: No formal independent dispute resolution service for DCE's

There is currently no delegated independent body capable of resolving disputes – AFCA lacks the dedicated resources devoted to cryptocurrency complaints (For further information, see section 4.1.1). Not only will the establishment of an independent body be beneficial to consumers, but membership in the independent body should be mandatory.

2.3.2: Solution: No formal independent dispute resolution service for DCE's

Make a recommendation to AFCA to establish a department specialising in cryptocurrency complaints/dispute resolution services or provide funding for the establishment of such a department.

Alternatively, if AFCA declines to assume this responsibility, resources and guidance should be provided to a trusted relevant industry body (i.e., Blockchain Australia, Fintech Australia) who have the expertise to establish a cryptocurrency-specific independent dispute resolution body similar to AFCA.

Regardless of the path chosen, a working group should be formed to ensure consultation with all business types and levels in order to ensure that all DCE subtype requirements are considered, and industry needs a whole are met.

2.4: Competency Tests

2.4.1: Issue: No test of competency for key DCE personnel.

There is no "competency check" to ensure that the person(s) in charge of a service actually understand what they are doing and are aware of their responsibilities. Additionally, there is no maintenance programme in place to ensure that these competency checks are conducted on an ongoing basis.

2.4.2: Solution: No test of competency for key DCE personnel.

A "competency check" on key personnel involved in the DCE, including their background (criminal, financial, etc.), relevant education/industry experience, and so on. ASIC should conduct repeat checks on a routine basis. Additionally, procedures should be developed in the event that an existing licensee fails one of these checks.

2.5: Financial impact

2.5.1: Issue: Negative financial bearing on small and start-up businesses

Due to the high financial costs associated with AFSL registration in its current form, it can be a roadblock for small and start-up cryptocurrency businesses. There are no exemptions or waivers from the application or maintenance of AFSL requirements associated with the provision of a cryptocurrency service.

2.5.2: Solution: Negative financial bearing on small and start-up businesses

Provide concessional AFSL registration rates to small businesses based on criteria such as turnover/revenue, employee count, services provided, and so on.

Furthermore, small businesses should be provided with incentives and funding to encourage and reduce the cost of membership in industry bodies (to promote inclusivity in industry discussion and to stay current on policy changes, among other things), as well as the costs of dispute resolution if an independent body is engaged.

2.6: Financial advice

2.6.1: Issue: Current licensing does not allow for cryptocurrency advisory

Services and entities that provide cryptocurrency-based investment advice are not required to register with ASIC in a financial advisor-type role.

2.6.2: Solution: Current licensing does not allow for cryptocurrency advisory

Include cryptocurrency advice as a separate registration category for financial advisors and ensure that those currently providing cryptocurrency advice are licenced in accordance with AFSL requirements or as recommended by relevant industry voices.

Bitcoin Babe PTY LTD www.bitcoin-babe.com **ACN:** 613 688 707
DCE: DCE100575454-001 PO Box 4228 Penrith Plaza NSW 2750 enquiries@bitcoin-babe.com

3. AUSTRAC involvement

> *The current AUSTRAC registration process is insufficient and meaningless in its current capacity. Because requirements are not actively enforced upon each DCE and rather assessed on a "case by case" basis, this subsequently leaves openings or "blind spots" for inadequate DCE's to fall into.*

3.1: Registration, Review, and Renewal process

3.1.1: Issue: The registration process is weak

At the time of my registration (April 2018), the AUSTRAC registration process included the following steps:

1. Application form
2. Production of a DCE compliance manual in line with AUSTRAC published guidelines
3. Procurement of a Police background check
4. Registration renewal every three years.

Even though a compliance manual and a police background check were requested, neither was checked at the initial application submission stage and my registration was approved regardless.

3.1.2: Solution: The registration process is weak

Strengthen the registration process by ensuring AUSTRAC are conducting diligent reviews of applications prior to their approval. This should include confirming the existence of the documentation referenced in points 2 and 3 (section 3.1.1), prior to the registration being approved.

3.1.3: Issue: The review process is weak

DCEs are required to complete an annual "questionnaire" via the "AUSTRAC online" portal. This questionnaire is used to notify AUSTRAC of any reviews or changes to your business structure, practises, personnel, AML/CTF programme, and so on, as well as to provide feedback on AUSTRAC's service.

AUSTRAC will review/assess/audit DCEs on a case-by-case basis at their discretion.

Throughout 2018 and 2019, I requested AUSTRAC for specific guidance relating to reporting requirements as a peer-to-peer trader. My concerns were that because of the structure of my business, some AUSTRAC requirements may not be adequately met in comparison to other services. I received no response from AUSTRAC regarding my queries.

In 2020, my compliance manual was requested for review, accompanied by threats of business closure or jail time if I failed to provide "sufficient" documentation. As a small business owner, this was extremely distressing and concerning, as not only had AUSTRAC never engaged with my business, but also with the structure of peer-to-peer trading (it was my understanding that AUSTRAC involved only "Blockchain Australia" registered orderbook style DCEs at the time of policy engagement).

It was only after writing to my Member of Parliament that I was able to meet with AUSTRAC officials to discuss their intentions – which were to learn more about the peer-to-peer space through my AML/CTF processes and to use the review process as a learning opportunity for both of us.

3.1.4: Solution: The review process is weak

AUSTRAC's approach to engaging DCE subtypes with which it is unfamiliar needs to be drastically overhauled – threats of business closure are excessive and unnecessary. Due diligence should be exercised, and AUSTRAC's requirements should be revised/adapted to ensure that all DCE subtypes are covered in order to ensure that requirements and responsibilities are clear and concise.

AUSTRAC delegates should follow up with DCEs following the submission of a yearly review in which a significant change has occurred or where feedback requiring attention has been left.

This should also be used as an opportunity to request copies of the documentation referenced in points 2 and 3 (section 2.1.1), to confirm its existence, if it has not been done so already.

3.1.5: Issue: The renewal process is weak

The renewal process consists of filling out an application form that is similar to the one that was provided at the time of initial registration. There is no requirement for supporting documentation for this review. Notification of a successful renewal is issued via email.

I submitted my renewal application three months prior to my expiration date. Despite multiple attempts to contact me regarding the status of my renewal, I did not receive a phone call until the week before my registration expired, at which point an AUSTRAC delegate informed me that there had been a delay and that I could continue operating my business past the expiry date if they did not notify me of my renewal by that point (however, if my renewal was refused, I would need to cease trading immediately). I did not receive an approval notice for renewal until the day of my registration expiry.

3.1.6: Solution: The renewal process is weak

Once the recheck of requirements 1-3 (section 2.1.1) has been completed, the renewal application should be approved.

Additionally, if delays are anticipated, AUSTRAC should inform the DCE of the anticipated wait time and reassure them that they can continue conducting business during this period. This information should be made publicly available on the AUSTRAC website or via AUSTRAC online.

3.2: Competency test

3.2.1: Issue: No test of competency for key DCE personnel.

There is no requirement for training or a test of comprehension/knowledge regarding the regulatory responsibilities of a DCE – anyone can sign up with no prior experience or understanding of the requirements relating to a DCE's KYC/AML/CTF obligations.

3.2.2: Solution: No test of competency for key DCE personnel.

Establish a competency check as part of the registration process to ensure that registered key personnel possess a thorough understanding of the KYC/AML/CTF requirements and obligations. This can be demonstrated through a mandatory questionnaire requirement by AUSTRAC/ASIC and supported with educational credentials or work/industry experience as part of DCE registration. Where this cannot be verified, certified training can be used to bring key personnel up to a sufficient level. This can be accomplished through an industry-consultant/designed training programme administered by a reputable third party.

3.3: DCE verification

3.3.1: Issue: No way to verify the legitimacy of a DCE registration

Anybody can claim to be "AUSTRAC registered" by providing a fictitious registration number. At the moment, the only way to validate a registration is for the DCE to provide a screenshot of their AUSTRAC portal. Given the ease with which such screenshots can be altered – and the fact that they contain scant information about the registration – this is insufficient for verifying their legitimacy.

Additionally, there is a risk of financial institutions abusing a public register, in that if a "complete" database is made available, they could systematically debank/ban all DCE's on the list from using their service.

Similarly, with ABN/ACN hijacking becoming more prevalent through scam techniques, a public DCE register would expose DCEs to impersonation, potentially resulting in additional consumer loss.

> *ABN/ACN Hijacking: The act of a scammer locating a legitimate business's registration information and then creating a website using those details to promote some sort of fraudulent scheme, which appears legitimate due to the "real" business credentials.*

3.3.2: Solution: No way to verify the legitimacy of a DCE registration

To prevent impersonation of a DCE through use of the DCE registration number, some form of two-factor authentication would be required to prevent this abuse, without the need of exposing a public register. Examples of this could include:

1. DCE# + URL search – By requiring the DCE's registration number and registered website URL, consumers/interested parties will be able to verify the legitimacy of not only the registration, but also the website on which they are engaging. For example:

   > *My customer may search for my registration number (12345) and my website address (www.bitcoin-babe.com) and receive a confirmation of registration; however, if they search for my registration number (12345) and an impersonator's website address (www.bitcoin-babe2.com), they will receive a negative result*

2. DCE# + Registration Date – By requiring something less well-known to the public – such as the date of the DCE's registration with AUSTRAC – the DCE can control who can and cannot verify their registration.

3. Implementing a random-key generation & verification service via AUSTRAC – Where a DCE can login to AUSTRAC and generate a random single-use alphanumeric key, which they can send to a customer, who would be able to enter the same key on an AUSTRAC verification portal to confirm/validate registration
4. Developing a system of digitally signed verification tokens - a larger scale project but could be used across the board to verify other registration types such as ABN, ACN, AFSL, Remittance Registration etc.

3.3: Financial Advisors

3.3.1: Issue: Future cryptocurrency financial advisors encountering illegal activity

Registration with AUSTRAC is at present not required for entities that provide crypto-based financial advice. This should be a requirement, given the risk posed by an unscrupulous individual seeking advice on how to "evade tax" using cryptocurrency.

3.3.2: Solution: Future cryptocurrency financial advisors encountering illegal activity

Financial advisors should be required to register with AUSTRAC (in a full or conditional capacity) in order to submit "Suspicious Matter Reports" (SMRs) if they come across such instances of behaviour.

Bitcoin Babe PTY LTD www.bitcoin-babe.com **ACN:** 613 688 707
DCE: DCE100575454-001 PO Box 4228 Penrith Plaza NSW 2750 enquiries@bitcoin-babe.com

4. AFCA involvement

> *In my experience, mediators and ombudsmen handling cases have demonstrated a lack of knowledge and comprehension regarding cryptocurrency and cryptocurrency-related businesses. This results in not only frustration for all parties involved, but also a sense of "lack of justice" on the part of the DCE due to the perception that the case was not properly handled. This has been exacerbated by the fact that mediators or ombudsmen will commonly recuse themselves from cases due to their lack of understanding of the issue.*
>
> *Additionally, AFCA states on their own website that "complex cases" can take up to 16 weeks (4 months) to resolve. At the time of writing, I have two unresolved cases with AFCA – both lodged in the first week of February 2021. This would put the duration of these disputes at six to seven months.*

4.1 Industry involvement

4.1.1: Issue: No independent dispute resolution for DCEs or Cryptocurrency based services.

There are no dedicated representatives, processes, or other mechanisms in place for the resolution of disputes involving a DCE or other services utilizing Cryptocurrency at this time. Further to the issues described in section 2.3.1, there is nothing in place to handle complaints such as:

1. Consumers v DCE
2. Business v DCE
3. Superfund v DCE
4. Trust v DCE
5. DCE v DCE
6. DCE v financial institutions

4.1.2: Solution: No independent dispute resolution for DCEs or Cryptocurrency based services.

As per the recommendations made in section 2.3.2, make a recommendation to AFCA to establish a department specialising in cryptocurrency complaints/dispute resolution services, or provide funding for the establishment of such a department.

Alternatively, if AFCA declines to assume this responsibility, resources and guidance should be provided to a relevant industry body (i.e., Blockchain Australia, Fintech Australia) to establish a cryptocurrency-specific independent dispute resolution body similar to AFCA.

Regardless of the path chosen, a working group should be formed to ensure consultation with all business types and levels in order to ensure that all possibilities and scenarios are considered.

Bitcoin Babe PTY LTD www.bitcoin-babe.com **ACN:** 613 688 707
DCE: DCE100575454-001 PO Box 4228 Penrith Plaza NSW 2750 enquiries@bitcoin-babe.com

5. Debanking and Industry involvement

> *Banks and DCEs are not having an open discussion about cryptocurrency, exchange services, and consumer protections; the process of onboarding, managing, and de-boarding a DCE from a banking institution is non-existent. While engagement from banks and financial institutions is frequently requested and openly appreciated, banks and financial institutions consistently reject this invitation.*

5.1: Debanking and mistreatment

5.1.1: Issue: Excessive use of power when debanking DCEs and its key personnel

The process of "de-banking" a DCE has become excessively aggressive and hostile. If a bank makes the "commercial decision" not to deal with a DCE, that is their right – however, purposely de-banking the personal accounts of those directly (or indirectly) associated with that DCE (i.e., directors, employees, stakeholders, customers, etc.) in a way that restricts their personal access to day-to-day products (personal transaction accounts, credit cards, loans, mortgages, insurance, superannuation etc.) is unwarranted and unnecessary.

5.1.2: Solution: Excessive use of power when debanking DCEs and its key personnel

Engage relevant industry bodies to amend relevant legislation and the banking code to include sections on "reasonable action" when declining to engage with or terminating a relationship with a DCE and their related parties. This could include requirements such as:

1. Provisions relating to the continuing banking relationship of personal financial accounts, lines of credit, and the honouring of insurance policies, among others (i.e.: it would be unreasonable for a bank to force someone to refinance their mortgage with another institution if they debanked a DCE business account).
2. Where a bank declines to provide services to a DCE or an individual, the bank should provide sufficient justification, evidence, and clearly articulate the reason of closure to the DCE or individual to ensure the decision was not made in an anti-competitive manner, or an easily rectifiable cause.
3. Timeframes for how long a DCE or individual has to make alternative banking arrangements should be clearly defined to avoid abrupt closures that can result in financial loss. Current legislation only states that "reasonable time" should be allowed, leaving the "time frame" up to the bank's discretion and interpretation, or to the AFCA in the event of a dispute.
4. Notify the DCE or individual of their disclosure of their commercial decision to other third-party entities (such as business sub-groups, other banking partners, monitoring programmes, etc.) and provide sufficient justification and evidence to the DCE or individual regarding how they arrived at this decision to ensure it was not made in an anti-competitive manner.
5. A bank should compensate a DCE or individual if it is determined that they did not act reasonably in accordance with the requirements.

5.1.3: Issue: Excessive use of power when freezing accounts relating to DCEs

Given a DCE's high liquidity, freezing a transaction account can have a significant negative impact on the DCE (i.e.: access to liquidity to purchase more cryptocurrency and maintain business revenue is ceased, unable to verify customer transactions and reconcile accounts for accounting purposes etc.). Additionally, banks can do this indefinitely and without explanation.

> *As of writing, I have two accounts that have been frozen since January 2021 and one account that has been frozen since June 2021, freezing $100,000 that I have been unable to verify the balance of and use to replenish my trading stock, resulting in lost assets and revenue.*

5.1.4: Solution: Excessive use of power when freezing accounts relating to DCEs

Engage relevant industry organisations to amend relevant legislation and the banking code to include sections on "reasonable action" when freezing an account. This could include requirements such as:

1. Provide adequate justifications for freezing an account or transaction and provide this justification to the DCE with an opportunity for rectification.
2. Timeframes clearly defined for how long a bank may reasonably freeze an account/funds in order to conduct reasonable procedures.
3. Where the freeze concerns a specific transaction, place a hold on the transaction(s) in question while allowing the DCE to continue operating. This should be conditional on the DCE's ability to demonstrate that adequate safeguards have been implemented to ensure that a repeated issue does not occur again – such as suspending the customer who initiated the suspicious transaction. Additionally, the bank should provide an opportunity for rectification to the DCE.
4. A bank should compensate a DCE financially if it is determined that the bank did not act reasonably in accordance with the requirements. Additionally, given the potential tax implications, "opportunity cost" should be recognised as a reasonable claim of financial loss.

> *Opportunity cost: The loss incurred when trading stock (cryptocurrency) is unable to be replenished by a DCE. Hypothetically, I sell 1 bitcoin for $1000. The funds are credited to my account, and I send the bitcoin to the customer. Shortly thereafter, the bank places a hold on my account pending the outcome of an investigation. I am unable to repurchase the 1 bitcoin in order to replenish my stock. The bank investigation takes three months, after which they release my $1000. The price of Bitcoin has increased to $10,000 during this time, which means I would need an additional $9,000 to repurchase my bitcoin – this $9,000 is referred to as the "opportunity cost" and is not recognised as compensable loss by banks or AFCA. Despite this, our current tax laws state that selling bitcoin to a customer – which was not repurchased in the form of trading stock – is considered a disposal and thus triggers a capital gains event. If I had purchased that Bitcoin a week prior to the sale for $700, I would owe tax on the $300 "capital gain." Additionally, the $9,000 "opportunity cost" cannot be written off as a loss.*

5.1.5: Issue: Historical review of previous mistreatment

While changes to relevant legislation to prohibit unjustified debanking would be welcomed by DCEs and future entrants to the economy, this does not consider the historical mistreatment of existing DCEs and personnel who have encountered hostile forms of debanking in the absence of prior recourse or reconciliation.

This would result in the disappearance of the vast majority of well trusted legacy businesses with established customer bases within the cryptocurrency community, leaving consumers vulnerable to less vetted services or "bad actors".

5.1.6: Solution: Historical review of previous mistreatment

Following legislative and licencing updates, financial institutions should be strongly encouraged to re-visit and review previous actions taken against DCEs or their personnel and give serious consideration to whether or not the decisions can be overturned.

Furthermore, recommendation should be given to the ACCC to launch a more stringent investigation into the claims of anti-competitive behaviour historically displayed by banks against DCEs.

5.2: Industry involvement

5.2.1: Issue: No encouragement to cease debanking from AUSTRAC

AUSTRAC does not provide sufficient encouragement for banks to form working groups with their DCE customers to discuss potential AML/CTF/Fraud risks, transactions, and so on, due to tipping off laws and other factors.

5.2.2: Solution: No encouragement to cease debanking from AUSTRAC

Engage relevant authorities to permit the disclosure and sharing of valuable information between banks and DCE customers without fear of being penalised for tipping off, violating privacy provisions, or anything else.

5.2.3: Issue: No encouragement to cease debanking from ATO

The ATO relies on DCEs to collect customer information and transaction history on a yearly basis in order to meet tax prefill requirements. It should be noted that by debanking DCEs, services are compelled to seek alternative or cash-based payment methods, which can result in easier concealment of transactions – which facilitates tax evasion, money laundering, and similar activities.

5.2.4: Solution: No encouragement to cease debanking from ATO

Include the ATO in working groups and engagements to emphasise the benefits of having "easily followed money" (via a DCE with a registered bank account) in order to combat tax evasion and fraud, and ultimately inhibit money laundering.

Bitcoin Babe PTY LTD www.bitcoin-babe.com **ACN:** 613 688 707
DCE: DCE100575454-001 PO Box 4228 Penrith Plaza NSW 2750 enquiries@bitcoin-babe.com

6. Barriers to entry and Encouragement of DCE payment relationships

> *Alternative payment methods labelled "cryptocurrency friendly" come with a slew of restrictions and conditions, in addition to being prohibitively expensive. This places larger entities that can "afford" to continue doing business ahead and destroying smaller/independent businesses as well as preventing the establishment of new DCEs. This mentality will result in an oligopoly between larger services, emulating the current "big four" banking situation.*

6.1: Barriers to Entry

6.1.1: Issue: Banks require a “capital contribution” to open an account

This is when a bank requests that a DCE deposit a specified amount (i.e.: BNK – aka Goldfields Money – have in the past requested $500,000) into a "holding account" in order to enable the business's transaction accounts to operate. Not only is this capital requirement unreasonable for the majority of businesses (as it is unaffordable and unattainable), but it also not feasible to the operating model of all DCE subtypes such as peer-to-peer trading.

> *As a peer-to-peer trader, I require my "capital" (trading stock) to be held in cryptocurrency in order to escrow the amount requested by the customer. As a result, it would be impossible for me to hold a large amount of “fiat capital”. This type of capital requirement would be more advantageous for an exchange service that holds funds "in trust" for their customers, which can then be kept in that "holding account."*

6.1.2: Issue: Services charging excessing fees

This is the case when payment processing services choose to charge a higher premium to DCEs in order to cover their management costs. There is currently only one service in Australia that allows for DCE onboarding.

As of March, of this year, Monoova (a payment processing service that I was denied access to due to my alleged operation of an "adult entertainment service") was charging DCEs a $2,500 monthly "starting fee" for one of their accounts. Additional fees apply if your transaction threshold is exceeded or if a fraud case is opened.

Furthermore, Monoova are not covered by any government programmes (such as the $250,000 guarantee) and provide no recourse in the event of a compromised account. These fees are excessive for a small/medium-sized business, as it would cost at least $30,000 for a business to gain access to basic payment rails with no guarantees or safeguards.

6.2: Alternative ideas and recommendations

6.2.1: Solution: Limit bank liability

Clearly define and distinguish the responsibilities and liabilities of DCEs and banks – This is to alleviate any regulatory burden/pressure that banks may face as a result of banking a DCE, and to ensure that DCEs bear adequate regulatory responsibility for their actions.

6.2.2: Solution: Recognition of Banking as a utility as opposed to a service

With the possibility of a reintroduction of the Currency (restrictions on the use of cash) bill 2019 (ban on cash transactions exceeding $10,000) and the push to make Australia a "cashless economy" during the pandemic, the push to transform Australia into a "cashless economy" is gaining momentum. This would increase the average consumer's reliance on banking services. As the number of debanked entities and individuals increases, their ability to rely on such services will become increasingly difficult. As a result, consideration should be given to classifying banks as utilities and imposing stricter scrutiny and penalties in the event of a refusal to provide service.

6.2.3: Solution: RBA to provide transaction services to DCEs

Request the RBA to provide provisional banking services to DCEs for the purpose of providing access to payment rails (BSB/ACC, PayID/Osko, Bpay, SWIFT, etc.) via accounts for a DCE to only use for transactional purposes (i.e., to receive payment from and make payment to customers). Transaction monitoring could be provided in collaboration between RBA service providers and the DCE, based on agreed requirements that take into consideration DCE's AML/CTF program, including KYC conditions, which would be recognised by AUSTRAC. Custodial services provided by the RBA could be investigated at a further time.

6.2.4: Solution: Engagement of the Digital Finance CRC

Given that this organisation was founded to create new financial opportunities, they should be involved in developing projects/products/services that provide payment alternatives for businesses and consumers experiencing debanking (as this is not a "cryptocurrency industry"-specific issue), while still "communicating" with traditional financial payment rails. Additionally, the onboarding of such businesses and consumers may result in more accurate and complete data for regulatory research opportunities.

6.2.5: Solution: Lessen the barriers to payment rails

By facilitating access to payment rails (BSB/ACC issuing, PayID/Osko, Bpay, SWIFT, Credit/Debit card, etc.) for the purpose of processing payments, it can foster innovation in the payment processing space, allowing for increased competition, and resulting in lower pricing. This solution would work well in conjunction with solutions 6.2.1 and 6.2.4 in order to facilitate further progress.

Bitcoin Babe PTY LTD www.bitcoin-babe.com **ACN:** 613 688 707
DCE: DCE100575454-001 PO Box 4228 Penrith Plaza NSW 2750 enquiries@bitcoin-babe.com

7. Consumer education and Scam prevention

> *Consumers continue to fall prey to scams despite repeated warnings posted in as many locations as possible throughout my own services. However, according to recent ACCC data, despite the efforts being made by industry consumer protection bodies (such as the ACCC, DCEs, Cyber.gov, and so on) to educate consumers, it is clear that the message is not getting through. While we can all empathise with those who have been scammed, I believe a more disciplined approach to education regarding the risks and consumers' responsibilities when it comes to purchasing cryptocurrency is necessary.*

7.1: Resources

7.1.1: Issue: No resources for consumers, DCEs etc. regarding cryptocurrency scams

As a DCE, I lack a clear channel or procedure for reporting scams that I have encountered or discovered through my own due diligence when engaging with customers. Additionally, there is no procedure for me to follow when advising a customer who has been scammed (or is about to be scammed) on how to take appropriate measures regarding what to do if they have handed over sensitive information and how to be more cautious in the future. Given I am the first person a consumer comes into contact with when these events occur, this is the most opportunistic moment to provide educational resources and help.

7.1.2: Solution: No resources for consumers, DCEs etc. regarding cryptocurrency scams

Collaborate with the ACCC, Cyber.gov, and industry to create a cryptocurrency-specific “scam watch” website. This can serve as a "one-stop shop" for everyone to consult and obtain resources. This could provide materials and services such as:

1. Cryptocurrency information and risks – A basic “Frequently Asked Questions” section defining what cryptocurrencies are, how they work, and so on. This should be used to convey the message that not all cryptocurrencies are "bad" or "scams," but that, like any activity, they come with inherent risks (such as irreversible transactions, for example), and how to mitigate them.
2. Scam types – investment scams, employment scams, initial coin offerings, and phoney financial advisors, among others.
3. The ability to report a scam – such as a person, service, product, token/coin, or business – on your own behalf, on behalf of a third party (such as a friend or family member), on behalf of a business, or on behalf of a DCE.
4. Scam register – a searchable public database of user-submitted names, emails, social media handles, and recounts. Users can conduct a search of this register to determine whether the product/service/person/business with which they are dealing is legitimate. Naturally, submissions to this register would require approval, and there would be an appeals process should you find yourself incorrectly listed.
5. How to seek assistance – What to do if you have been scammed, how to avoid being scammed in the future, assisting people at risk (such as the elderly, disabled, or those suffering from mental health problems as a result of financial loss), and so on.

6. Statistics – visual representation of data gathered from reports.
7. News and alerts

7.2: Consumer responsibility

7.2.1: Issue: There is no conciseness between banks and DCEs regarding consumer responsibility

Given the inherent self-sovereignty of cryptocurrency and the lack of recourse available to consumers who "lose" their crypto, education regarding due diligence and the consumer's liability must be clearly defined. This is not being heard by financial institutions, and therefore, results in a number of “false fraud reports” which not only further tarnishes the images of DCEs but can also result in unnecessary financial loss. As an example:

> *A consumer purchases bitcoin for the purpose of investing it in a cloud mining scheme promoted by a person they recently met on Instagram. The cloud mining scheme does not exist; thus, the consumer has been scammed. The consumer notifies their bank of this financial loss. Due to the tumultuous relationship between DCEs and banks, this results in a fraud claim being filed against the consumer's transaction to the DCE for the exchange of the cryptocurrency. The DCE’s bank must comply with the return request, debiting the DCEs bank account and returning the funds to the consumer. Now, the DCE has not only lost the funds, but also the cryptocurrency taken (by the consumer).*

In any other industry, this type of "poor decision making" would be the consumer's responsibility – poor decision = loss. Due to the consumer's lack of knowledge (or the bank's nefarious motives), this onus is shifted to DCEs without explanation or justification. To explain this in another way:

> *A consumer makes a purchase of shoes from a retailer. The consumer lends the shoes to a friend on the condition that the friend will return them three days later. The friend fails to return the shoes and vanishes, resulting in the consumer losing their shoes. As a result, the consumer returns to the retailer with their receipt and requests that a refund be issued for the stolen shoes.*

Of course, in this case, the shoes were lost due to the consumer's poor judgement in not conducting due diligence and lending them to an irresponsible friend. The retailer is not obligated to compensate the consumer – this statement should also apply to cryptocurrency.

7.2.2: Solution: There is no conciseness between banks and DCEs regarding consumer responsibility

Request banks use their available platforms and services to educate their customers and implement systems or procedures to assist them during the prevention or recovery process. Examples of this could include:

1. When a bank customer sends money to a known/suspected DCE account, the bank should implement a more conservative warning system, informing the customer of the potential risks of cryptocurrency scams – a call, SMS, or email prior to the transaction being processed, with a reference to the “crypto scam watch” website (as mentioned in section

7.1.2), to confirm they understand the risks and their liabilities if the crypto is stolen. Once confirmation is received, then the transaction can be approved. This should be done tastefully, without insinuating that the DCE is a scam or using other such language.

2. If a bank customer purchases crypto and then attempts to lodge a fraud claim for the funds sent to the DCE, then the bank should deny this request, make appropriate security updates/changes, and provide the customer with resources on what to do next (i.e.: who to contact if they have shared personal information, reporting the scam, referencing the resources on the "crypto scam watch" website as mentioned in section 7.1.2 etc.).

7.3: Crypto influencers

7.3.1: Issue: Unlicensed social media "crypto influencers" giving illegal advice

The term "crypto influencer" refers to someone who provides what is essentially investment advice and promotes "call to action" events, in which they tell their audience where or what to invest their money or cryptocurrency into. They will often create communities through social media tools such as Facebook Groups, Discord Servers, or group chats on messaging apps such as Facebook Messenger, Telegram, WhatsApp, Signal etc. Further to this, gaining entry to these groups often requires a financial contribution.

The most commonly seen influencer advice scheme is the "pump and dump".

> *A pump and dump scheme involves a small group of influencers and their friends purchasing large amounts of a low-volume cryptocurrency/coin/token in order to generate hype around it. They will then inform their audience about this "lucrative trading opportunity" and encourage them to invest. This further increases the market price (the pump). Once the hype subsides, the small group will sell their holdings at a significant profit, but at the cost of a market crash (the dump). Unfortunately, this results in many consumers losing money because their investment (which was purchased at a premium) is now worthless.*

7.3.2: Solution: Unlicensed social media "crypto influencers" giving illegal advice

Unlicensed financial advice is prohibited for a variety of financial products. While it is debatable whether cryptocurrency is a "financial product," it should be treated similarly when providing consumer advice.

1. Individuals providing financial advice should be licenced under an existing or newly enacted AFSL/ASIC regime and be sufficiently competent to do so.
2. Relevant industries (ASIC, ACCC, etc.) should be enlisted to crack down on those who continue to provide unlicensed financial advice following the implementation of licencing. Additionally, industry associations should collaborate with social media platforms (Facebook, Instagram, Twitter, and YouTube, among others) to aid in the removal of Australian-created/accessible content that offers advice or other similar services.

8: Closing Recommendations

The overall goal, regardless of the issue being treated, is to encourage open communication across all relevant sectors. Industry participation is important in resolving problems and offering chances to improve industry to ensure Australia becomes the front-runner for new and existing digital currency projects, products, businesses, and services. By becoming a “cryptocurrency positive” country, Australia can retain local tax revenue, create new employment opportunities and innovation prospects, thus boosting economic growth within the sector.

No matter how open dialogue is achieved through working groups, online surveys, or individual engagement, diversification of representation from all aspects of the industry (small and medium-sized businesses (SMBs), enterprise, and government) will be critical to ensuring that all possibilities are discovered and greater unity within the sector is attained.

Bitcoin Babe PTY LTD www.bitcoin-babe.com **ACN:** 613 688 707
DCE: DCE100575454-001 PO Box 4228 Penrith Plaza NSW 2750 enquiries@bitcoin-babe.com

9: Resources

ASIC - Australian Securities and Investments Commission. (2021). Retrieved 23 September 2021, from https://asic.gov.au/

Australian Competition and Consumer Commission. (2021). Retrieved 23 September 2021, from https://www.accc.gov.au/

Australian Financial Complaints Authority (AFCA). (2021). Retrieved 23 September 2021, from https://www.afca.org.au/

Australian Tax Office. (2021). Retrieved 23 September 2021, from https://www.ato.gov.au/

Australian Transaction Reports and Analysis Centre. (2021). Retrieved 23 September 2021, from https://www.austrac.gov.au/

Blockchain Australia | Australia's Peak Blockchain Industry Body. (2021). Retrieved 23 September 2021, from https://blockchainaustralia.org/

Currency (Restrictions on the Use of Cash) Bill 2019 – Parliament of Australia. (2021). Retrieved 23 September 2021, from https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r6418

Digital Finance CRC. (2021). Retrieved 23 September 2021, from https://www.dfcrc.com.au/

Reserve Bank of Australia. (2021). Retrieved 23 September 2021, from https://www.rba.gov.au/

Scamwatch. (2021). Retrieved 23 September 2021, from https://www.scamwatch.gov.au/

The Australian Prudential Regulation Authority. (2021). Retrieved 23 September 2021, from https://www.apra.gov.au/

The Banking Code Compliance Committee. (2021). Retrieved 23 September 2021, from https://bankingcode.org.au/