Australian Digital Currency Industry Code of Conduct

A voluntary code establishing externally reviewable best-practice standards of conduct for businesses operating in the Australian digital currency industry.

October 2021

1. Purpose

1.1. This Code of Conduct sets out Best Practice Standards for the operation of a Digital Currency Business in Australia.

1.2. The Code of Conduct intends to provide assurance to consumers, regulators and commercial partners that a certified member of Blockchain Australia has implemented Best Practice Standards in their business.

1.3. Certification by Blockchain Australia indicates that implementation of and adherence to Best Practice Standards by the member has been reviewed by an independent, accredited third party and then approved by Blockchain Australia in accordance with this Code of Conduct.

1.4. This Code of Conduct is a contract between Blockchain Australia and a Blockchain Australia Certified Digital Currency Businesses, and is not intended to form contractual rights or obligations as between Blockchain Australia Certified Digital Currency Businesses and their customers.

2. Defined Terms

In this Code of Conduct, unless the context otherwise requires:

AML/CTF Law means the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, associated rules and other instruments.

ASIC means the Australian Securities & Investments Commission.

AUSTRAC means the Australian Transaction Reports and Analysis Centre.

Blockchain Australia means Blockchain Australia Ltd.

Blockchain Australia Certification Mark means the logo described in Appendix 1 that may be used by a Digital Currency Business to indicate that Blockchain Australia Certification under this Code of Conduct has been granted.

Blockchain Australia Certified (or Certified, Certification) means a Digital Currency Business that has been certified by the Committee as adhering to this Code of Conduct in accordance with the requirements in Part 6 of this Code of Conduct.

Best Practice Standards means the standards of conduct for the operation of a Digital Currency Business described in Part 4 of this Code of Conduct.

Cash or Cash Equivalent has the meaning defined in the Australian Securities and Investments Commission's Regulatory Guide 166 as applicable to custodians.

Certification Date means the date that Blockchain Australia Certification is granted by the Committee to an applicant Digital Currency Business.

Code of Conduct means this document, which is also referred to as the Australian Digital Currency Industry Code of Conduct.

Committee means the Blockchain Australia Code Compliance Committee, the independent body established by Blockchain Australia to administer this Code of Conduct including the granting, administration (including suspension) and withdrawal of Blockchain Australia Certification.

Company Officer means "officer" as defined in the Corporations Law.

Corporations Law means the *Corporations Act 2001* and related regulations and instruments.

Digital Currency means a digital representation of value that can be digitally traded or transferred, and can be used for payment or investment purposes. It also includes the definition of Digital Currency as set out in the AML/CTF Law. It does not include digital representations of fiat currencies, securities and other financial assets that are covered elsewhere in the FATF Recommendations other than in FATF's guidance on Virtual Assets and Virtual Asset Service Providers. To the extent of inconsistency between the definition above and the definition of Digital Currency in the AML/CTF Law, the wider definition applies. [1]

Digital Currency Business means an Industry Member that carries on a business of providing or facilitating the:

(a) purchase or sale of a Digital Currency;

(b) purchase or sale of a fiat currency in connection with a Digital Currency; or

(c) storage of a Digital Currency;

[1] ADCA has adopted the FATF's definition of virtual asset, found here: https://www.fatf-gafi.org/glossary/u-z/. It has also adopted the definition of Digital Currency set out in the AML/CTF Law.

but does not include an Industry Member that uses Digital Currency for purposes other than described in (a), (b) or (c) above (for example, purely for blockchain or other technology purposes where there is no transfer of material monetary value attached to the use of Digital Currency).[2]

Director has the meaning defined in the Corporations Law.

External Dispute Resolution Scheme or EDR means a scheme approved by ASIC that accepts Digital Currency Businesses as members.

FATF means the Financial Action Task Force - an international policy-making body established by the G7 countries in 1989.

FATF Recommendations means the current version FATF Recommendations as adopted by FATF from time to time, available at www.fatf-gafi.org.

Industry Member means an entity which is:

(a) legally incorporated under the laws of Australia or other country approved by the Directors of Blockchain Australia from time to time;
(b) a FinTech or digital economy centric business (including blockchain and Digital Currency); and
(c) nominated for membership by an existing fully paid up Voting Member (as defined in Blockchain Australia's Constitution) and accepted for membership by Blockchain Australia.

PEP means Politically Exposed Person for the purposes of AML/CTF Law.

Privacy Law means the *Privacy Act 1988* and related regulations and other instruments.

Sanctions Law means the *Charter of the United Nations Act 1945*, *Autonomous Sanctions Act 2011*, associated rules and other instruments.

Substantial Shareholder or Controller means a shareholder who owns (directly or indirectly) at least 25% of a company or its ultimate controlling entity or otherwise controls the company or its ultimate controlling entity. "Controls" in this context adopts the definition of "Control test" in the AML/CTF Law.

3. Eligibility and Operation

[2] For example, one Satoshi of BTC is required to access the BTC blockchain, but only represents a small fraction of a BTC and poses no money laundering or terrorism financing risks.

3.1. This Code of Conduct has been adopted by the Directors of Blockchain Australia as Blockchain Australia Standards in accordance with Section 2 of Schedule 3 of the Blockchain Australia Constitution.

3.2. This Code of Conduct is available for voluntary adoption by Industry Members that operate a Digital Currency Business in Australia, including Digital Currency Businesses domiciled outside Australia but which provide services within Australia.

3.3. Blockchain Australia Certification is available to Industry Members that can demonstrate by means of a review process that its business processes, systems and policies comply with the provisions of this Code of Conduct in accordance with Part 6.

3.4. A Blockchain Australia Certified Digital Currency Business must comply with all relevant obligations under this Code of Conduct except where doing so would lead to a breach of a law. This Code of Conduct makes reference to Australian law. If an Australian law is inconsistent with a non-Australian law which also applies to the Blockchain Australia Certified Digital Currency Business, the Australian law shall prevail to the extent of the inconsistency.

3.5. This Code of Conduct is binding upon a Blockchain Australia Certified Digital Currency Business from the Certification Date until such time as certification is terminated by the member by the provision of written notice to Blockchain Australia, or is withdrawn or suspended by Blockchain Australia. Termination, withdrawal or suspension does not result in a rebate of any fees paid to Blockchain Australia.

3.6. A Blockchain Australia Certified Digital Currency Business must implement and effectively operate business practices, systems and policies that enable it to comply with the Code of Conduct.

3.7. A Blockchain Australia Certified Digital Currency Business must take reasonable steps to ensure that any director, employee or agent that acts on its behalf in the conduct of its Digital Currency Business also adheres to the Code of Conduct and is responsible for any breach of the Code of Conduct as if the breach had been committed by the Digital Currency Business directly.

3.8. Blockchain Australia must maintain a register of all Blockchain Australia Certified Digital Currency Businesses on its website along with a record of the most recent date and status of certification or re-certification.

4. Best Practice Standards

4.1. Reputation and General Conduct

4.1.1. Blockchain Australia Certified Digital Currency Businesses must comply with Australian laws including the Corporations Law, Privacy Law (even if only on an opt-in basis), Sanctions Law and AML/CTF Law (subject to clause 4.3 below), and equivalent laws in jurisdictions outside Australia if they operate a Digital Currency Business in those jurisdictions.

4.1.2. Blockchain Australia Certified Digital Currency Businesses must act with integrity, transparency, competence, diligence, respect and in an ethical manner with its customers, employees, members of the public, government regulators and agencies and other members of the Digital Currency Industry and must not act in a way that may bring into disrepute:

(a) Blockchain Australia;
(b) Blockchain Australia members;
(c) their own employees or customers, past or present;
(d) the provision of Digital Currency services and its allied services.

4.1.3. Prior to certification and re-certification, Blockchain Australia Certified Digital Currency Businesses must conduct ASIC register searches, bankruptcy and National Police checks (or overseas equivalent searches) on all Company Officers and Substantial Shareholders or Controllers to ensure that they are fit and proper persons to operate a Digital Currency Business.

4.1.4. Blockchain Australia Certified Digital Currency Businesses must maintain accurate and complete records of all transactions. Records must be kept up to date and secure for a minimum of 7 years.

4.2. Consumer Protection

4.2.1. Blockchain Australia Certified Digital Currency Businesses must maintain a customer Privacy Policy consistent with the Privacy Law and make it available on their website, and reference to it whenever personal information is collected.

4.2.2. Blockchain Australia Certified Digital Currency Businesses must apply data security systems and processes to protect customer data including any IP addresses, wallet addresses, digital currency identifiers or other customer payment information. The Blockchain Australia Certified Digital Currency Business shall (where applicable):

(a) build and maintain a secure network;

(b) protect customer data, including securely storing the customer data and encrypting any transmission of data across open, public networks;
(c) maintain a vulnerability management program;
(d) implement strong access control measures;
(e) regularly monitor and test networks;
(f) maintain an information security policy; and
(g) comply with the Australian Crypto Assets Data Security Standard, or another standard approved by Blockchain Australia.

4.2.3. Where customer fiat currency funds are received but not applied to the provision of a product or service within 24 hours, Blockchain Australia Certified Digital Currency Businesses must return the funds to the customer, or transfer any such funds to a separate bank account designated as a trust account (where not already held in such an account in the same fiat currency as provided by the customer). It is intended that only customer funds can be held in that account and funds that the Blockchain Australia Certified Digital Currency Business becomes entitled to must be withdrawn from the trust account as soon as practicable and no later than one month after the entitlement arises. Unless prohibited by law, unallocated customer funds must be returned to customers within 30 days of receipt, where the customer can be reasonably identified.

4.2.4. Where a Blockchain Australia Certified Digital Currency Business provides a service of storing, holding, owning or controlling Digital Currency on behalf of a customer, it will:

(a) Hold Digital Currency of the same type and amount as that which is owed or obligated to the customer, and provide evidence of this upon request by the customer;
(b) Not lend, trade, encumber or otherwise use the Digital Currency except in accordance with the express directions of the customer;
(c) Hold in Cash or Cash Equivalent, an amount equal to or greater than the AUD equivalent value of all hot wallet balances; and
(d) Publish prominently on its website (for example, in its terms and conditions):
    i. the capacity (e.g. as principal or agent) in which it holds Digital Currencies; and
    ii. whether third party custodians are relied upon.

4.2.5. Blockchain Australia Certified Digital Currency Businesses must maintain membership and comply with the terms of references of an External Dispute Resolution Scheme to facilitate fair resolution of customer complaints and disputes.

4.2.6. Blockchain Australia Certified Digital Currency Businesses must clearly describe on their websites:

(a) pricing and fee structures;
(b) internal and external complaints handling process and contact details;
(c) rules around accepting and matching or otherwise placing orders; and
(d) A short summary of their internal policy governing:
    i. how and where Digital Currencies and private keys to control the Digital Currencies are held and backed up, and
    ii. recovery arrangements for Digital Currencies and private keys; and
    iii. what happens in the event that Digital Currencies belonging to customers or private keys controlling such Digital Currencies are lost or compromised.

4.3. Anti-Money Laundering and Counter-Terrorism Financing Obligations

4.3.1. Blockchain Australia Certified Digital Currency Businesses must comply with the Sanctions Law and applicable AML/CTF Law, or to the extent that AML/CTF Law does not apply to them, must voluntarily comply with so much of the AML/CTF Law as would be applicable if the AML/CTF Law applied to the Digital Currency Business.

AML/CTF and Sanctions Compliance Program

4.3.2. Blockchain Australia Certified Digital Currency Businesses must adopt, maintain and comply with an AML/CTF and Sanctions compliance program consistent with the requirements of the Sanctions Law, and AML/CTF Law so far as applicable. In particular, the AML/CTF and Sanctions compliance program will cover:

(a) a risk assessment framework[3];
(b) employee due diligence processes;
(c) employee risk awareness training;
(d) financial sanctions;
(e) oversight by board and senior management;
(f) appointment of an AML/CTF compliance officer;
(g) independent review (see Part 7 of this Code of Conduct);
(h) AUSTRAC reporting[4] (including suspicious matter reporting);
(i) for businesses with subsidiaries, branches or agents providing Digital Currency Business services outside Australia, systems to ensure consistent application of AML/CTF obligations across those entities;[5]
(j) collecting and verifying customer and beneficial owner information; and

[3] Benchmarked against FATF Recommendation 1.
[4] Benchmarked against FATF Recommendations 20 and 21.
[5] Benchmarked against FATF Recommendation 18.

(k) ongoing customer due diligence procedures, which provide for the ongoing monitoring of existing customers to identify, mitigate and manage any ML/TF risks. These include a transaction monitoring program and an enhanced customer due diligence program.

4.3.3. A risk assessment framework under 4.3.2(a) must demonstrate that prior to and after[6] accepting a new customer, consideration is given to:

(a) customer type, including PEPs and their associates (also including where the customer is not an individual: beneficial owners or controllers);[7]
(b) the types of designated services provided;[8]
(c) sources of funds and wealth;
(d) purposes and intended nature of the business relationship;
(e) delivery methods and new technologies;[9]
(f) new designated services, and methods of delivering them; and
(g) foreign jurisdictions with which it operates or conducts business.[10]

4.3.4. The AML/CTF and Sanctions program must be independently reviewed at regular intervals and the Blockchain Australia Certified Digital Currency Business must ensure the independence of the reviewer (see Part 5).

4.3.5. Where a Blockchain Australia Certified Digital Currency Business uses a third party[11] (including an agent) to provide their services or perform customer due diligence measures, they will:

(a) remain solely responsible for the delivery of their services and full compliance with this Code of Conduct; and
(b) adopt a risk-based approach when engaging and monitoring those third parties.

4.3.6. If the Blockchain Australia Certified Digital Currency Business engages liquidity providers (including Digital Currency exchanges), providers of electronic wallet services[12] or other providers of core business services, those providers will be treated like a special category of high risk customers in that, in addition to performing normal customer due diligence measures, the Blockchain Australia Certified Digital Currency Business must gather more information about:

[6] Benchmarked against FATF Recommendation 5 and 6.
[7] Benchmarked against FATF Recommendations 8 and 12.
[8] If the Digital Currency Business also offered traditional remittance services, this is an example of a "designated service".
[9] Benchmarked against FATF Recommendations 15 and 16.
[10] Benchmarked against FATF Recommendation 19.
[11] Benchmarked against FATF Recommendation 17.
[12] Benchmarked against FATF Recommendation 13 and 17.

(a) their reputation;
(b) the quality of supervision;
(c) regulatory history;
(d) their AML/CTF Law (or equivalent to their jurisdiction) compliance;
(a) adequacy of their customer due diligence procedures including ability to provide customer identification data and other relevant documentation upon request without delay; and
(b) adequacy of their cyber resilience program.

The Blockchain Australia Certified Digital Currency Business will also:

(a) obtain approval from senior management before establishing such new relationships;
(b) clearly understand the respective responsibilities of themselves and the third party; and
(c) with respect to electronic wallets providers, be satisfied that the electronic wallet provider has conducted customer due diligence on their customers.

5. The Blockchain Australia Code Compliance Committee

5.1. The Committee is to be determined by the Board.

5.2. The Committee must consist of at least three people, each of whom:
(a) must be independent from the Board;
(b) must have the necessary skills and expertise;
(c) will be reimbursed for any Board approved out-of-pocket expenses incurred in connection with the performance of their duties as a Committee member;
(d) may be paid a sitting fee or other remuneration as determined by the Board from time to time; and
(e) must agree to be bound by and follow the terms of reference for the Committee.

5.3. The members of the Committee must appoint a chair from their number and may also appoint a deputy chair.

5.4. Except in circumstances where the Board is the respondent in a matter to be determined by the Committee, the Board has the right to appoint an observer to the Committee. The appointed observer will have the right to attend meetings of the Committee but will not be permitted to vote on Committee decisions or contribute to its deliberations. For the avoidance of doubt, the appointed observer may be, but does not need to be, a Blockchain Australia director.

5.5. The Committee will administer this Code of Conduct according to the following guidelines:

(a) Jurisdiction: The Committee will only consider matters directly related to granting, administration (including suspension) and withdrawal of Blockchain Australia Certification.

(b) Conflicts of interest: Committee members will disclose any conflicts of interest connected to any decision making and the chair or deputy chair will manage the conflict in accordance with the Blockchain Australia conflict of interest policy. In addition:

i. no Blockchain Australia Certified Digital Currency Business (including its employees, directors, and people with more than 5% shareholding in the business) may be a member of the Committee; and
ii. where a Committee member is an external reviewer or an associate or representative of a Committee member is an external reviewer, the Committee Member will not vote on the Certification Application.

(c) Fairness, transparency and openness: The Committee's administration of affairs will be fair and have regard to the principles of natural justice, be transparent and open in the same way that the Blockchain Australia Standards Review Committee operates.

(d) Confidentiality: All information disclosed by an applicant or Blockchain Australia Certified Digital Currency Business for certification or recertification under this Code of Conduct must be regarded as confidential and must not be used or disclosed by any member of the Committee or Blockchain Australia Board except as required by law or as permitted by the relevant Blockchain Australia Certified Digital Currency Business. However, the Committee may advise the Board or a government body, or otherwise make public with the Board's consent, any information arising from consideration by the Committee that it believes may have sector wide significance. Where the Committee advises the Board about issues arising from a Complaint, applicants or Blockchain Australia Certified Digital Currency Businesses (as the case may be) will not be identified unless the Committee has made a decision to name the person, with the consent of the Board.

(e) Initial certification, self-certification and recertification: See Part 6 of this Code of Conduct.

(f) Corrective action: See Part 7 of this Code of Conduct.

(g) Risk-based: The Committee will take a risk-based approach in determining how to exercise its powers.

6. Certification and Recertification

Certification

6.1. A Digital Currency Business seeking certification as a Blockchain Australia Certified Digital Currency Business must commission, at its own expense, and provide to the Committee, an external reviewer's report.

6.2. In particular, the report must:

(a) make reference to each requirement set out in Appendix 2, and provide the reviewer's view on whether the Digital Currency Business has in place all the procedures and processes required in that Appendix 2, and whether those procedures and processes have been effectively implemented;

(b) provide the level of assurance expected of an independent review under the AML/CTF Law.

6.3. In particular, the external reviewer must:

(a) be independent in the manner required for an independent review conducted pursuant to the AML/CTF law, but must also be external to the Digital Currency Business;

(b) seek approval from the Committee, before conducting the review, using the form set out in Appendix 3;

(c) be approved by the Committee. The reviewer will only be approved by the Committee after demonstrating expertise in AML/CTF Law and expertise in Digital Currency Businesses.

6.4. Where the report provided to the Committee, as required by clause 6.1 above provides recommendations to the Digital Currency Business or the Committee has additional queries of the reviewer, the reviewer must, at the expense of the Digital Currency Business, confirm that recommendations in the report or the Committee's queries have been satisfactorily addressed.

6.5. Blockchain Australia Certification automatically lapses on the anniversary of the Certification Date unless re-certification has been approved by the Committee or, in extraordinary circumstances, the Blockchain Australia Board has approved an extension. An extension may only be granted once and for no longer than two months.

Recertification

6.6. A Blockchain Australia Certified Digital Currency Business must:

(a) commission, at its own expense, a two-yearly external review of its business processes, systems and policies to confirm in accordance with Appendix 2, that they remain adequate to ensure compliance with the Code of Conduct. The two-yearly review must be completed by an external reviewer approved by Blockchain Australia in the manner described in clauses 6.1 to 6.4 above, and the report provided to the Committee within 23 months of the last Certification Date, in order to allow sufficient time for the report to be considered by the Committee. The report must be prepared in accordance with clause 6.2 of this Code of Conduct; and

(b) for every year that an external review is not conducted, self-certify that it has adequate processes, systems and policies in place to remain compliant with the Code of Conduct, in accordance with Appendix 2 of this Code of Conduct. The self-certification must be provided to the Committee no later than one month prior to the anniversary of the Certification Date, and must be in the format set out in Appendix 2.

Committee has power to grant certification or recertification

6.7. The Committee may grant Blockchain Australia Certification. In determining whether to grant certification or recertification, and before accepting an external review report prepared in accordance with clauses 6.2 to 6.4, the Committee can require from the Industry Member:

(a) documents supporting the contents of the review report conclusions; and/or

(b) evidence supporting the independence or competence of the reviewer (in addition to Appendix 3).

6.8. Upon receipt of the self-certification, and before recertifying a Digital Currency Business, the Committee can require further information including documents supporting the contents of the self-certification in determining whether to grant the recertification.

6.9. The Blockchain Australia Board must determine a Code of Conduct Certification Fee that must be paid by the applicant for certification or re-certification, and the Digital Currency Business must pay that fee in full, prior to consideration of the application by the Committee. The fee shall not be refundable in the event of an adverse determination, and is in addition to any fee payable to the external reviewer.

6.10. The Committee must maintain a Code Compliance Checklist (see Appendix 2), which will be used by the external reviewer as the basis of the initial and subsequent two-yearly external certification and recertification reviews. The Code Compliance Checklist shall comprise of the following sections:

(a) Code of Conduct review, including a summary of recommended and required improvements in light of the findings; and

(b) Evidence of the independence and professional competence of the external reviewer. It will also be used for self-certification.

6.11. External reviewers must be required by the Blockchain Australia Certified Digital Currency Business to produce a review report using the format prescribed by the Code Compliance Checklist in order to ensure consistency and comparability of assessments.

6.12. Within 1 month of receipt, the Committee must consider the report prepared by the external reviewer or the self-certification and must request further information, or make a determination that certification or recertification under this Code of Conduct be:

(a) granted;
(b) granted subject to conditions; or
(c) refused.

6.13. An applicant for certification or recertification under this Code of Conduct may appeal a decision of the Committee to the Blockchain Australia Standards Review Committee, which is governed by the Blockchain Australia Standards, Disputes, Complaints Handling and Reviews policy.

6.14. This Code of Conduct and the activities contemplated by it are governed by the law in force in New South Wales, Australia. Each party irrevocably and unconditionally submits to the non-exclusive jurisdiction of the courts of New South Wales, Australia and courts of appeal from them for determining any dispute concerning this Code of Conduct or the activities contemplated by this Code of Conduct.

6.15. The Committee may amend the Code of Conduct from time to time, and has a discretion to impose extra or waive various elements based on the guidelines set out in clause 5.5. It will provide at least 30 days' notice to existing Certified Digital Currency Businesses, during which time they have an opportunity to respond before the changes are finalized. Blockchain Australia will make the final decision on whether to implement the changes after considering feedback.

7. Non-Compliance Reporting, Complaints and Sanctions Process

7.1. A Blockchain Australia Certified Digital Currency Business must undertake to promptly report all incidences of material non-compliance with the Code of Conduct to the Committee.

7.2. An incident of non-compliance will be considered material after considering the following:

(a) the number and frequency of previous similar incidences;

(b) the impact of the incident or likely incident on the Blockchain Australia Certified Digital Currency Business's ability to provide the service;
(c) The extent to which the incident or likely incident indicates that the Blockchain Australia Certified Digital Currency Business's arrangements to ensure compliance with those obligations is inadequate;
(d) the actual or potential financial loss to customers arising from the incident or likely incident; and
(e) whether the incident raises any industry-wide systemic issues.

7.3. Where a complaint is made to the EDR scheme and an adverse finding is made against the Blockchain Australia Certified Digital Currency Business, it must notify the Committee immediately. The Committee will review the circumstances of the complaint **only** for the purposes of determining whether it provides evidence of material non-compliance with this Code of Conduct.

7.4. Upon investigation of an incident of material non-compliance under clause 7.2 or notification of an adverse finding under clause 7.3, the Committee may:

(a) take no action;
(b) require that a specific corrective action be undertaken within a nominated period; or
(c) withdraw certification.

7.5. The Committee will not exercise its discretion to withdraw certification without first giving the Blockchain Australia Certified Digital Currency Business a period of not less than 14 days to respond to the Committee's concerns and provide reasons as to why certification should not be withdrawn.

7.6. In making its decision, the Committee will consider whether the incident of non-compliance is evidence of a systemic failure of business processes, systems or policies such that they are inadequate to ensure consistent compliance with the Code of Conduct.

7.7. A Blockchain Australia Certified Digital Currency Business that receives an adverse finding under the Code of Conduct may appeal the decision to the Blockchain Australia Standards Review Committee, in which case the Blockchain Australia Standards, Disputes, Complaints Handling and Reviews policy will apply.

7.8. The Committee will not consider individual consumer complaints. Complaints management will be facilitated through the internal dispute resolution processes of the Blockchain Australia Certified Digital Currency Business or the EDR scheme appointed under clause 4.2.5.

8. Blockchain Australia Certification Mark

8.1. A Blockchain Australia Certified Digital Currency Business will be entitled to describe itself as "Blockchain Australia Certified" and to use the Blockchain Australia Certification Mark described in Appendix 1.

8.2. A Blockchain Australia Certified Digital Currency Business must include a section on its website in the form prescribed in Appendix 1B that explains the nature and purpose of Blockchain Australia Certification and includes a link to this Code of Conduct on the Blockchain Australia website.

8.3. Use of the description "Blockchain Australia Certified" and the Blockchain Australia Certification Mark is limited exclusively to current Blockchain Australia Certified Digital Currency Businesses and must be immediately discontinued in the event that Blockchain Australia certification lapses, is suspended or terminated by Blockchain Australia, or withdrawn by the Digital Currency Business.

9. Limitation of Liability

9.1. Blockchain Australia Certified Digital Currency Businesses and applicants for Blockchain Australia Certification (whether successful or not) agree that they are solely responsible for the provision of products and services to their customers and prospective customers and that Blockchain Australia does not provide products or service to those customers or prospective customers.

9.2. Blockchain Australia Certified Digital Currency Businesses and applicants for Blockchain Australia Certification (whether successful or not) agree that Blockchain Australia is not liable for any act or omission of a Digital Currency Business and holds Blockchain Australia harmless against any suit, claim, action, investigation, complaint or other request for compensation to the fullest extent permitted by law. To the extent that Blockchain Australia is found liable, liability is limited to the amount paid to Blockchain Australia by the Digital Currency Business for Blockchain Australia Certification.

9.3. Applicants for Blockchain Australia Certification or recertification under this Code of Conduct who are unsuccessful and Blockchain Australia Certified Digital Currency Businesses whose Blockchain Australia Certification is suspended or terminated for material non-compliance with the Code of Conduct, and upon exhaustion of the appeal processes described in this Code, agree that Blockchain Australia is in no way liable for any economic loss, loss of profit or other loss associated with the denial or withdrawal of Blockchain Australia Certification. To the extent that Blockchain Australia is found liable, liability is limited to the amount paid to Blockchain Australia by the Digital Currency Business for Blockchain Australia Certification.

9.4. Blockchain Australia excludes all liability it may have to Blockchain Australia Certified Digital Currency Businesses and applicants for the acts and omissions, negligent or otherwise of its officers, employees and other representatives in connection with this Code of Conduct, and to the extent it is unable to rely on such exclusion, limits the total liability of Blockchain Australia for such acts or omissions to the total amount of the fees paid by the relevant Member to Blockchain Australia in the relevant financial year.

APPENDIX 1: Blockchain Australia Certification Marks & Explanatory Text

Appendix 1A: Blockchain Australia Certification Mark

The Blockchain Australia Certification Mark is shown below. It may not be reproduced in any other format or colours and must not be less than 366 by 80 pixels.

Appendix 1B: Blockchain Australia Certification Explanatory Text

The following text explaining the nature and purpose of Blockchain Australia Certification must be included on the website of a Blockchain Australia Certified Digital Currency Business as required by clause 8.3 of the Code:

> The Australian Digital Currency Industry Code of Conduct is a voluntary scheme that establishes externally reviewable best practice standards for businesses operating in the Australian Digital Currency industry.
>
> The Code of Conduct is administered by Blockchain Australia Ltd and is available for adoption by businesses operating in Australia that provide or facilitate the:
>
> - purchase or sale of a Digital Currency;
> - purchase or sale of a fiat currency in connection with a Digital Currency; or
> - storage of a Digital Currency.
>
> The Code of Conduct establishes Best Practice Standards covering:
>
> - reputation and general business conduct;
> - consumer protection; and,
> - AML/CTF obligations.
>
> Blockchain Australia Certification means that the participating Digital Currency Business has been assessed to have business processes, systems and policies in place that will ensure consistent compliance with the Code of Conduct, including the Best Practice Standards. Compliance with the Code of Conduct is independently reviewed every two years by a Blockchain Australia approved external reviewer and self-certified every other year.
>
> [Company Name] is a member of Blockchain Australia and has held Blockchain Australia Certification under this Code of Conduct since [Month Year].
>
> The full text of the Australian Digital Currency Industry Code of Conduct is available here.

APPENDIX 2: Code Compliance Checklist

The certification and self-certification process:

1. Year 1: Certification – External Review
2. Year 2: Recertification – Self certification
3. Year 3: Recertification – External Review
4. Year 4: Recertification – Self-certification
5. Future years: Recertification – Alternate between External Review and Self Certification

Note for self-certification:

6. Complete the Self-Certification Instructions in the right column, and return to members@blockchainaustralia.org.au. If you are a Digital Currency Exchange registered with AUSTRAC, you can attach your AUSTRAC registration application to this self-certification, and in some of the rows below, you can simply refer to that application. It may save you time.
7. If a field is not applicable, explain why. Failure to complete every section of this table in detail may result in the application being rejected as incomplete.

Note for external reviewers:

1. All elements of this checklist that relate to the external review must be referred to in your review report.
2. Your review report must comply with clauses 6.1 to 6.3 of the Code of Conduct.

	Area (Code Reference)	**External Review Criteria**	**Self-Certification Instructions**	**Self-Certification Attestation**
Part 3 – Eligibility and Operation				
1.	ABN/ACN (3.2)	Check the entity is active and not deregistered.	Set out ABN/ACN	
2.	Address of principal place of business (3.2)	Confirm principal place of business via **paid company search**, and confirm subsidiary and branch locations.	Set out your principal place of business and all business locations for subsidiaries and branches of your entity. Tell us if you do not have subsidiaries or alternate locations from your primary address.	

3.	Nature of business (are you a dedicated Digital Currency Business or do you also provide other services (e.g. money transfer business, etc.)?) (3.4)	Review the entity's website and AUSTRAC enrolment form and ensure that the entity is a Digital Currency Business.	Describe your core business activities. Describe other services offered by your entity. Outline the ML/TF risks associated with the services provided. State the number of employees in your entity.	
4.	What steps are taken to ensure any director, employee or agent that acts on your behalf, also adheres to the Code of Conduct? (3.7)	Assess steps taken by the entity to ensure those acting on behalf of the entity, also adhere to the Code of Conduct. Assess whether the relevant procedures (e.g. HR policy and employment agreement) implemented and effective	Set out all reasonable steps taken to ensure directors, employees and agents acting on the entity's behalf adhere to the Code.	
Part 4 – Best Practice Standards				
Part 4.1 – Reputation and General Conduct				
5.	Are any parts of your business or agents registered with AUSTRAC? If yes, what are they (e.g. money remittance or currency exchange) (4.1.1)	Ensure the entity is enrolled and registered with AUSTRAC (if required by law) and ensure its processes to renew registration are implemented and effective. Relevant designated services could also include remittance or as an AFSL holder arranging for a person to receive a designated service.	List the designated services you provide. Provide your AUSTRAC registration number, enrolment details and registration or last renewal date.	

6.	Is your business subject to any other regulation, domestic or foreign (e.g. regulation by ASIC under an ASIC-issued Australian Financial Services Licence (AFSL) or Australian Credit Licence (ACL))? (4.1.1)	Test regulatory status of entity and assess whether the entity has procedures that are implemented and effective to ensure it considers whether it must comply with additional regulatory regimes (i.e. AFSL, ACL or foreign regulation). Check ASIC register to ensure entity holds a current AFSL or ACL, if required by law.	Set out whether your business is subject to other regulations and if so, provide licence or registration number and details (e.g. AFSL, ACL, other).	
7.	What steps are taken to comply with or observe the Corporations Law, Privacy Law and AML/CTF Law (including equivalent jurisdictions outside Australia if you operate a Digital Currency Business in those jurisdictions)? (4.1.1, 4.2.1, 4.3.2)	Assess steps taken by the entity to ensure compliance with all relevant laws. Randomly test whether their policies and procedures are implemented in practice and are effective. In terms of sample sizes or data sets, choose a sample size or data set similar to what you would do if you were undertaking an Independent Review as required by the AML/CTF Law. In other words, it's not enough to confirm that a policy *exists* – you need to collect enough evidence so that you're comfortable providing assurance that the policy is *effective*. Relevant policies include: a) Privacy policy; b) AML/CTF and Sanctions Program and working documents; and	Set out all reasonable steps taken to comply with the relevant laws. Include links to your privacy policy and refer to relevant compliance manuals and procedures you have implemented.	

		c) Other relevant compliance manuals. For example, work through the onboarding process that the entity offers for new customers.		
8.	Please provide full names of key personnel of your business including directors, officers, substantial shareholders, and other decision makers. (4.1.2, 4.1.3)	Assess whether the entity's employee due diligence procedure is implemented and effective. Randomly test whether the entity has: screened the names of key personnel against: a) the ASIC banned and disqualified persons list; b) AUSTRAC registration suspensions and cancellations; c) Sanctions and PEP lists; d) bankruptcy; and e) criminal records.	Set out full names of key personnel of your business (including decision makers not recorded with ASIC) and set out screening results in relation to: a) the ASIC banned and disqualified persons list; b) AUSTRAC registration suspensions and cancellations; c) Sanctions and PEP lists; d) bankruptcy; and e) criminal history.	
9.	Are all key personnel able to provide Digital Currency services with integrity, transparency, diligence, and in an ethical manner? (4.1.1, 4.1.2, 4.1.3)	Assess whether the entity has implemented a procedure which is effective, to consider whether each key person has: a) competency to operate a Digital Currency Business (as demonstrated by their knowledge, skills and experience); b) the attributes of good character, diligence, honesty, integrity and judgement.* c) not been disqualified by law from performing their role; and	Explain how key personnel are fit and proper persons to provide Digital Currency services, considering: a) their competency to operate a Digital Currency Business (demonstrated by their knowledge, skills and experience); b) their attributes of integrity, transparency, diligence; c) whether they have at any time been disqualified by law from performing their role in your business; and	

		d) any conflict of interest in performing their role in the Digital Currency Business. Assess whether the entity's conflicts of interest policy is implemented and effective.	d) the management of any conflict of interest in performing their role in the Digital Currency Business.	
10.	Are accurate and complete records of all transactions kept up to date and secure for a minimum of 7 years? (4.1.4)	Test whether the entity's record keeping process is implemented and effective and require accurate and complete records of all transactions are kept up to date for a minimum of 7 years. Test a sample of records to prove the following have been retained: a) AML/CTF program; b) customer due diligence; and c) transactions. Test the records are kept securely.	Explain how accurate and complete records of transactions are kept up to date and secure for a minimum of 7 years, referencing the relevant policies and procedures.	
4.2 – Consumer Protection				
11.	Do you maintain a customer Privacy Policy? (4.2.1) (4.2.2)	Assess appropriateness of the customer Privacy Policy. Test whether the policy is easily accessible on the entity's website and whether it is referred to when personal information is collected. Test whether the entity complies with Australian Privacy Principle 11: Security of Personal Information, by asking for evidence of compliance.	Explain when your Privacy Policy was last updated, whether it is easily available on your website and referred to whenever personal information is collected. Explain how you comply with Australian Privacy Principle 11: Security of Personal Information. This is: how do you protect, hold and then delete or de-identify personal information once it is no longer needed for any purpose for which the information was collected?	

		This includes testing the procedures for how the entity protects, holds, and then deletes or de-identifies personal information once it is no longer needed for any purpose for which the information was collected.	Go to the www.OAIC.gov.au website for guidance on this obligation.	
12.	How do you manage data security? (4.2.2)	Test the entity has effective procedures to ensure it complies with its obligations to: a) build and maintain a secure network; b) protect customer data, including securely storing the customer data and encrypting any transmission of data across open, public networks; c) maintain a vulnerability management program; d) implement strong access control measures; e) regularly monitor and test networks; f) maintain an information security policy; and g) comply with the Australian Crypto Assets Data Security Standard, to the extent that it is applicable. If the entity has had an external certification, you can rely on this after checking the scope of the external review. For example, consider if the entity: ● Is certified to the relevant industry standard – ISO 27001	Referring to your policies and procedures, explain how you: a) build and maintain a secure network; b) protect customer data, including securely storing the customer data and encrypting any transmission of data across open, public networks; c) maintain a vulnerability management program; d) implement strong access control measures; e) regularly monitor and test networks; f) maintain an information security policy; and g) comply with the Australian Crypto Assets Data Security Standard, to the extent that it is applicable; or h) complies with another external security standard approved by Blockchain Australia (see examples below). If the entity has had an external certification in the last 2 years, you can possibly rely on this after checking the scope of the external review.	

		● Attained SOC-2 Compliance ● Has been reviewed by a CREST-registered penetration (PEN) tester and consider the scope and outcomes of that report. Ensure these procedures have been implemented.	For example, are you (or have you been): ● certified to the relevant industry standard – ISO 27001 ● SOC-2 Compliant ● Reviewed by a CREST-registered penetration (PEN) tester and does the scope and outcomes of those reviews or accreditations cover the matters listed in 4.2.2?	
13.	Do you operate a separate trust account in accordance with the requirements in the Code of Conduct? (4.2.3)	Test whether trust account procedures have been implemented in line with the Code of Conduct obligation and are effective. Review evidence of this account in operation. A trust account is a bank account that does not include money that belongs to the entity. It only includes client money.	Set out the steps taken to open and maintain a separate trust account and an explanation as to how you manage the account. A trust account is a bank account that does not include money that belongs to the entity. It only includes client money.	
14.	If you provide a service of storing, holding, owning or controlling Digital Currency, do you follow appropriate procedures for this service? (4.2.4)	Assess whether the procedures used by the entity if providing the service of holding, owning or controlling Digital Currency are in line with the Code of Conduct obligation and are implemented and effective. Test the procedures are implemented and effective to ensure that the entity:	If you provide this service, set out, referring to your policies and procedures how you: a) hold Digital Currency of the same type and amount as that which is owed to the customer; b) do not use the Digital Currency unless directed by the customer; e) holds Cash or Cash Equivalent in an amount greater than the AUD equivalent of hot wallet balances; and	

		a) holds Digital Currency of the same type and amount as that which is owed to the customer; b) does not use the Digital Currency unless directed by the customer; c) holds Cash or Cash Equivalent in an amount greater than the AUD equivalent of hot wallet balances; and d) publishes the capacity in which it holds digital currencies and reliance on third party custodians. Some entities prepare externally audited financial reports about their crypto holdings and cash holdings, for their investors. You can use this information to form a view about whether they comply with this obligation.	c) publishes the capacity in which it holds digital currencies and reliance on third party custodians and include a link to where this information is available.	
15.	Are you a member of an External Dispute Resolution (EDR) Scheme? (4.2.5)	Check for details of the entity's membership of an EDR Scheme and procedures for maintaining membership.	Set out details of your EDR membership.	
16.	Do you clearly describe your pricing and fee structures on your website? (4.2.6)	Check that the entity has effective procedures that have been implemented to ensure the entity clearly discloses pricing and fee structures. Review the entity's website to ensure clear disclosure of pricing and fee structures.	Explain your pricing and fee structure and provide a link to the relevant part of your website where pricing and fee structures are set out.	
17.	Do you clearly describe your complaints handling process and	Test the entity's procedures for complaints handling is implemented	Explain your complaints handling process and provide a link to the relevant part of your website where	

	contact details on your website? (4.2.5, 4.2.6)	and effective and is consistent with the disclosed process on its website. If an EDR member, search the EDR (eg. AFCA) member register to confirm registration. Review the entity's website for clear disclosure of complaints handling process and contact details.	the complaints handling process and contact details are set out. Provide your EDR membership number.	
18.	Do you clearly describe the rules around accepting and matching or otherwise placing orders on your website? (4.2.6)	Review the entity's procedures and rules around accepting and matching or otherwise placing orders and consider whether they are implemented and effective and consistent with the disclosed process on its website.	Explain your rules around accepting and matching or otherwise placing orders and provide a link to the relevant part of your website where the details are set out.	
19.	Do you have an internal policy governing private keys? (4.2.6)	Review the entity's procedures and processes and consider whether they are implemented and effective, in relation to: a) how and where Digital Currencies and private keys to control the Digital Currencies are held and backed up; b) recovery arrangements for Digital Currencies and private keys; and c) what happens in the event that Digital Currencies belonging to customers or private keys controlling such Digital Currencies are lost or compromised.	Explain your internal policy in relation to: a) how and where Digital Currencies and private keys to control the Digital Currencies are held and backed up; b) recovery arrangements for Digital Currencies and private keys; and c) what happens in the event that Digital Currencies belonging to customers or private keys controlling such Digital Currencies are lost or compromised.	
Part 4.3 – Anti-Money Laundering and Counter-Terrorism Financing Obligations				

20.	Have you established an AML/CTF and Sanctions Compliance Program? (4.3.1, 4.3.2)	Ensure that the AML/CTF and Sanctions Compliance Program includes the elements required by clause 4.3.2 of the Code of Conduct, and test that it is implemented and effective. Assess implementation and effectiveness of the following procedures: a) risk assessment framework; b) employee due diligence process; c) risk awareness training (including training register); d) PEP and sanctions screening; e) board and senior management oversight of the program (e.g. Directors resolution approving the program and minutes of a compliance meeting discussing AML/CTF risks); f) appointment and responsibilities of the AML/CTF compliance officer; g) AUSTRAC "dob-in" reporting or suspicious matter reporting (de-identified) (as relevant); h) IFTI reporting (if relevant); i) TTR reporting (if relevant); j) monitoring of branches or agents in other countries for compliance with equivalent Australian requirements (if applicable); k) customer and beneficial owner data collection and verification; and l) the transaction monitoring program and enhanced customer	Provide examples of how your AML/CTF and Sanctions Compliance Program is working in practice. This should include: a) copy of your risk assessment framework (but see Row 16 below). b) example employee due diligence process being followed. c) training register. d) example of how sanctions lists are used. e) example of Board oversight of the program (e.g. Directors resolution approving the program or minutes of a compliance meeting discussing AML/CTF risks). f) example of AUSTRAC "dob-in" reporting or suspicious matter report (de-identified). g) evidence of how branches or agents in other countries are monitored for compliance with equivalent Australian requirements (if applicable). h) examples of how customers and beneficial owners' data is collected and verified. i) example of how the transaction monitoring program and enhanced customer due diligence processes trigger the requirement for further information to be collected, or for other actions to be taken.	

		due diligence processes (including the triggers for further information to be collected, or for other actions to be taken). You may be able to do this by reviewing an external Independent Review undertaken in accordance with the AML/CTF Law. We think it would need to be no more than a year old. In terms of sample sizes or data sets, choose a sample size or data set similar to what you would do if you were undertaking an Independent Review as required by the AML/CTF Law. In other words, it's not enough to confirm that a policy *exists* – you need to collect enough evidence so that you're comfortable providing assurance that the policy is *effective*.		
21.	Do you ensure your customers or their payees* (if applicable) are not in countries subject to a Sanctions regime (see www.dfat.gov.au website for a comprehensive list of countries) or to other High Risk countries? (4.3.2(d), 4.3.3(g))	Confirm whether the entity's policy in relation to Sanctions and High Risk Countries is implemented and effective. Review the entity's list of customer and payee (if applicable) countries.	Set out a list of customer and their payee* (if applicable) countries. *Payees are the beneficiaries of a payment (whether digital or fiat currency) where your customer has instructed you to send the payment. If you don't offer a remittance or transfer service, you still need to show how you treat your customers in connection with Sanctions Laws.	

22.	Do you ensure that your customers or their payees (if applicable) are not themselves on any Sanctions lists? (4.3.2(d))	Review the entity's Sanctions checking processes to ensure they are implemented and effective, testing the processes have been followed. Sanctions screening must either be done manually incorporating the relevant lists below, or done via subscriptions with a reputable provider.	Referring to relevant policies and procedures, describe how you check customers and their payees (if applicable) against Sanctions lists, explain which Sanctions lists you screen customers and their payees (if applicable) against and whether you use service providers to conduct that screening for you.	
23.	Have you terminated any staff, agents or third parties due to non-compliance with the AML/CTF Laws, Sanctions Laws, or business policy? (4.3.2(b), 4.3.6)	Review employee due diligence procedures to determine if procedures in relation to non-compliance have been implemented and are effective. Has termination of an employee, agent or third party occurred due to non-compliance with the AML/CTF Laws or Sanctions Laws obligations has occurred or not and if consequences are appropriate.	Set out whether there have been any incidents of non-compliance with the AML/CTF Laws, Sanctions Laws or a business policy. Referring to your policies and procedures, set out whether the non-compliance has resulted in termination of an employee, agent or third party. If non-compliance has not resulted in termination, explain why this has not occurred.	
24.	Does your ML/TF risk assessment framework meet the minimum requirements? (4.3.3)	Ensure that the ML/TF risk assessment framework is implemented and effective and includes the elements required by clause 4.3.3 of the Code of Conduct. I.e. the ML/TF risk assessment framework must consider the risks associated with: a) customer type, including PEPs and their associates (also including where the customer is not an individual: beneficial owners or controllers);	Set out when your ML/TF risk framework was last reviewed and updated and why. Referring to your policies and procedures, set out how you ensure your ML/TF risk assessment framework considers the risks associated with: a) customer type, including PEPs and their associates (also including where the customer is not an individual: beneficial owners or controllers);	

		b) the types of designated services provided; c) sources of funds and wealth; d) purposes and intended nature of the business relationship; e) delivery methods and new technologies; f) new designated services, and methods of delivering them; and g) foreign jurisdictions with which it operates or conducts business Randomly test that the ML/TF risk assessment is implemented, effective and being complied with. For example, if all customers are being treated in the same way, (e.g. "All customers are considered High Risk") the framework will not be effective. Review a sample of low risk customer files, medium risk customer files and high risk customer files that demonstrate the application of the above risk assessment framework.	b) the types of designated services provided; c) sources of funds and wealth; d) purposes and intended nature of the business relationship; e) delivery methods and new technologies; f) new designated services, and methods of delivering them; and g) foreign jurisdictions with which it operates or conducts business.	
25.	Has your AML/CTF and Sanctions Compliance Program been independently reviewed? (4.3.4)	Review the entity's procedures for conducting an independent review and whether they are implemented and effective. Consider the entity's previous independent review. Is it clear that the reviewer was sufficiently independent? Did the entity update their AML/CTF Program and procedures in light of its	Set out when you last conducted an independent review, who undertook it, why they were independent, the material findings and whether your AML/CTF Program was updated subsequently. If you have not conducted an independent review, explain why.	

		recommendations in a timely manner? Consider when the last independent review was conducted and whether it complied with the Code of Conduct 2-yearly requirements (see clause 6.7).		
26.	Do you engage third parties or agents that you rely on to provide your services or perform customer due diligence, including liquidity providers (e.g. Digital Currency exchanges) or providers of electronic wallet services? If so, please provide details about who they are and how you monitor them. (4.3.6)	Review the entity's procedures for engaging third parties and agents to ensure it is implemented and effective. Ensure that the: a) entity performed normal customer due diligence (CDD) measures on third parties b) information required by clause 4.3.6 of the Code of Conduct has been collected; c) entity had approval from senior management before the relationship was established; d) entity clearly understands the respective responsibilities of themselves and the third party. Review the entity's procedures for monitoring and supervision of third party providers and agents to ensure they are risk based, implemented and effective. Ensure that third party providers are treated according to a risk-based methodology. For example, liquidity providers and electronic wallet service providers should be considered as high risk customers,	Set out the name(s) of the third party/agent(s) that you rely on to provide your services (e.g., to perform customer due diligence, liquidity providers, electronic wallet services etc.). Referring to your policies and procedures, explain the information you collect about them before onboarding, and as part of your ongoing monitoring of their performance. Explain how you appoint and monitor high risk third parties, including (where applicable): a) liquidity providers; b) digital currency exchanges; and c) providers of electronic wallet services. Set out examples of monitoring third party providers, including meeting with them and sighting evidence of how they externally test their own risk controls. In the case of high risk third parties, explain whether and how you have considered their reputation, the	

		and the information set out in clause 4.3.7 of the Code of Conduct should be considered as part of the onboarding process of that third party. With respect to high risk third parties, test the entity's understanding of responsibilities of themselves and the third party (e.g. whether they have clear written Service Level Agreements with third parties that the entity understands and that can be enforced).	quality of supervision, regulatory history, their AML/CTF Law (or non-Australian equivalent) compliance, and the adequacy of their CDD procedures. Explain whether and how you ensure senior management approval is given before a relationship is established with a high risk third party.	
27.	Do you use third party electronic wallet providers? (4.3.6)	Review the entity's procedures in relation to monitoring third party wallet providers to see if they are implemented and effective. Specifically test whether the entity has ensured that their electronic wallet providers are conducting CDD on their customers.	Set out your third party electronic wallet provider (if applicable). Explain how you test third party wallet Customer Due Diligence and ensure that is undertaken.	
Part 9 – Non-Compliance Reporting, Complaints and Sanctions Process				
28.	Does your business have a procedure in place to report all incidences of material non-compliance with the Code of Conduct, to the Committee? (7.1, 7.2)	Review the entity's procedure for identifying non-compliance with the Code and reporting material breaches and test whether it is implemented and effective.	Referring to your appropriate policies and procedures, explain your procedure that describes how breaches and incidents of non-compliance with the Code are reported.	
29.	Do you notify Blockchain Australia when you are required to? (7.3)	Test whether the entity's has a process for notifying Blockchain Australia when it is required to (e.g. if an adverse finding is made under an EDR Scheme or if a material breach is	Explain your complaints handling procedure, including your process for notifying Blockchain Australia of adverse findings or material breaches of the Code of Conduct.	

		identified) and whether it is implemented and effective.		
30.	Has your business been subject to any investigation or enforcement action by an Australian Regulator, including ASIC, ACCC or AUSTRAC? If so, what is the status of that investigation or action? (7.1, 7.2)	Check whether there is or has been regulatory action undertaken against the entity. Review the entity's remediation effort.	Set out details of any regulator action, and the status of any remediation. If there has been no regulator action, state that.	
Part 8 – Blockchain Australia Certification Mark				
31.	Do you have a Blockchain Australia Certification Mark and Explanatory Text included on your website? (8.1, 8.2)	Review the entity's website and a sample of publicly available content (such as statements or marketing material) for references to Blockchain Australia to ensure no misrepresentations or misleading statements are made. For certification: once certification is granted by the Committee, review appropriate inclusion of the Blockchain Australia Certification Mark and Explanatory Text on the entity's website, in line with Appendix 1 of the Blockchain Australia Code of Conduct. For recertification: review appropriate inclusion of the Blockchain Australia Certification Mark and Explanatory Text on the entity's website, in line with Appendix 1 of the Blockchain Australia Code of Conduct.	Provide link(s) to where the Blockchain Australia Certification Mark and Explanatory Text is published on your website and any other instances where Blockchain Australia is referred to on your website.	
Part 6 – Certification and Recertification				
32.	Does the reviewer have independence and competence to perform the review? (6.3)	Explain why the reviewer is independent and competent to perform the review.	N/A	

APPENDIX 3: Form for seeking approval from Committee to conduct independent review

Code Compliance Committee
Blockchain Australia
GPO Box 153
Albert Park Vic 3206

<Date>

Dear Committee Members,

Re: Appointment as independent reviewer for Code of Conduct

<Name of DCE> (the **DCE**) has proposed to engage me, <Individual Name>, of <Company Name> to conduct an independent review of its business operations for the purposes of seeking certification under the Australian Digital Currency Industry Code of Conduct (**Code**).

Before commencing the review process, I seek approval from the Code Compliance Committee that I meet the requirements of an independent reviewer as detailed in Section 6.3 of the Code.

I make the following declarations:

- I am independent of the DCE and have no ownership stake in that business or other close involvement with the business;

- I have not been involved in the design or implementation of any aspect of the business operations of the DCE subject to this audit;

- My professional competence to carry out this audit is demonstrated by

  <insert brief description of:
  - membership of professional bodies,
  - experience undertaking independent reviews, and
  - relevant DCE experience>;

- I have a good understanding of the Digital Currency sector;

- I understand that I will be required to prepare a report assessing the compliance of the DCE against each item in the checklist contained in Appendix Two of the Australian Digital Currency Industry Code of Conduct and ensure that there is evidence to support that assessment for each criteria; and,

- I understand that the level of assurance expected of me is that same as if I were preparing an Independent Review under the *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)*, section 8.6 or 9.6.

- I agree to attend a review meeting with the Code Compliance Committee along with the DCE to discuss the written audit report and answer any questions that the Committee may have.

I look forward to your response.

Kind Regards

<Individual Name>
<Business Name>