Australian Digital Currency Industry Code of Conduct

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

November 30, 2016

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 an accredited member of ADCCA has implemented Best Practice Standards in their business.

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

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

2. Defined Terms

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

ADCCA means the Australian Digital Currency Commerce Association Ltd.

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

ADCCA Certified (or Certification) means a Digital Currency Business that has been certified by the Committee as adhering to this Code of Conduct.

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.

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.

Certification Date means the date that ADCCA 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 ADCCA Code Compliance Committee, the independent body established by ADCCA to administer this Code of Conduct including the granting, administration (including suspension) and withdrawal of ADCCA 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 and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in

any jurisdiction. It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.[1]

Digital Currency Business means an Industry Member that provides or facilitates 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;

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 tangible 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.

Industry Member means an entity which is:

(a) legally incorporated under the laws of Australia or other country approved by the Directors of ADCCA 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 ADCCA's Constitution) and accepted for membership by ADCCA.

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.

[1] ADCCA has adopted the FATF's definition of virtual currency, found here: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf
[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.

Provisional ADCCA Certification (or Provisionally ADCCA Certified) means a Digital Currency Business that has been provisionally certified by the Committee as adhering to this Code of Conduct.

Provisional Certification Date means the date Provisional ADCCA Certification is granted by the Committee to an applicant Digital Currency Business.

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. "Control" in this context adopts the same meaning as in the AML/CTF Law.

3. Eligibility and Operation

3.1. This Code of Conduct has been adopted by the Directors of ADCCA as ADCCA Standards in accordance with Section 2 of Schedule 3 of the ADCCA 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. ADCCA Certification and Provisional ADCCA 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 7.

3.4. An ADCCA 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 ADCCA Certified Digital Currency Business, the Australian law shall prevail to the extent of the inconsistency.

3.5. This Code of Conduct is binding upon an ADCCA Certified Digital Currency Business from the date upon which ADCCA Certification (whether or not it is provisional) is granted (the Certification Date or the Provisional Certification date, as applicable) until such time as certification is terminated by the member by the provision of written notice to ADCCA, or is withdrawn or suspended by ADCCA. Termination, withdrawal or suspension does not result in a rebate of any fees paid to ADCCA.

3.6. An ADCCA Certified Digital Currency Business must implement business practices, systems and policies that will enable it to comply with the Code of Conduct.

3.7. An ADCCA 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. ADCCA must maintain a register of all ADCCA 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. ADCCA Certified Digital Currency Businesses must comply with or observe 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. ADCCA 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) ADCCA;
(b) ADCCA members;
(c) their own employees or customers, past or present;
(d) the provision of Digital Currency services and its allied services.

4.1.3. ADCCA Certified Digital Currency Businesses must conduct an annual ASIC register search, bankruptcy and National Police Clearance Certificate on all Directors, 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. ADCCA Certified Digital Currency Businesses must maintain a risk-based level of professional indemnity insurance cover for not less than $1 million and such other insurances as are appropriate.

4.1.5. ADCCA 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. ADCCA 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. ADCCA 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 credit card information. The ADCCA 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; and
(f) maintain an information security policy.

4.2.3. Where customer fiat currency funds are received but not applied to the provision of a product or service within 24 hours, ADCCA Certified Digital Currency Businesses must 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 ADCCA 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. Unallocated customer funds must be returned to customers within 30 days of receipt.

4.2.4. Where an ADCCA 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 sell, transfer, assign, lend, hypothecate, pledge, encumber or otherwise use the Digital Currency except in accordance with the express directions of the customer.

4.2.5. ADCCA Certified Digital Currency Businesses must maintain membership of an External Dispute Resolution Scheme to facilitate fair resolution of customer complaints and disputes.

4.2.6. ADCCA Certified Digital Currency Businesses must clearly describe their pricing and fee structures on their websites.

4.2.7. ADCCA Certified Digital Currency Businesses must clearly describe their complaints handling process and contact details on their websites.

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

4.3.1. ADCCA 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 Digital Currency Businesses.

AML/CTF and Sanctions Compliance Program

4.3.2. ADCCA 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) and monitoring (to the extent permitted by AUSTRAC);
(i) for businesses with majority owned 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 ADCCA Certified Digital Currency Business must ensure the independence of the reviewer (see Part 5).

4.3.4. In addition to collecting and verifying the minimum KYC information required by the AML/CTF Law,[11] the ADCCA Certified Digital Currency Businesses must collect at a minimum:

(a) the customer's location at the time of the transaction, or their IP address;
(b) details about the customer's funding provider, (e.g. a bank in the case of fiat currency or e-wallet provider in the case of Digital Currency), and its location; and
(c) in the case of a value transfer from the customer to another person, the payee's name and location.

4.3.5. The ADCCA Certified Digital Currency Businesses must verify the data collected pursuant to clause 4.3.4 using risk-based controls.[12] For low and medium risk

[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] For example, An AML/CTF program must include a procedure to collect (where the customer is an individual), at a minimum: the customer's full name; date of birth; and residential address. Also, the AML/CTF program must include a procedure to *verify*, at a minimum: the customer's full name; and either: (a) date of birth; or (b) residential address.
[12] Controls may include verifying the payment provider by conducting and recording independent electronic searches on reputable websites, such as a government-controlled banking regulator websites, or an established Digital Currency Industry Body websites.

customers, this includes requiring PEP screening of the payee (if applicable), at a minimum.

4.3.6. Where an ADCCA Certified Digital Currency Business uses a third party[13] (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.

4.3.7. If the ADCCA Certified Digital Currency Business engages liquidity providers (including Digital Currency exchanges) or providers of electronic wallet services[14], 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 ADCCA Certified Digital Currency Business must gather more information about:

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

The ADCCA Certified Digital Currency Business will also:

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

[13] Benchmarked against FATF Recommendation 17.
[14] Benchmarked against FATF Recommendation 13 and 17.

5. The ADCCA 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, an ADCCA 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 ADCCA 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 ADCCA conflict of interest policy. In addition, no ADCCA Digital Currency Business (including its employees, directors, and people with more than 5% shareholding in the business) may be a member of the Committee.

(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 ADCCA Standards Review Committee operates.

(d) Confidentiality: All information disclosed by an applicant or ADCCA 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

ADCCA Board except as required by law or as permitted by the relevant ADCCA 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 ADCCA 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, Annual Review 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. Provisional Certification

6.1. A Digital Currency Business seeking certification as an ADCCA Certified Digital Currency Business may submit an application for Provisional ADCCA Certification by payment of the application fee (see 7.6 below) and submitting to the Code Compliance Committee:

(a) a completed, self-certified Code Compliance Checklist in the form set out in Appendix 2; and,

(b) a written undertaking to instruct an external auditor approved by ADCCA to:

i. conduct a review of its business processes, systems and policies in accordance with Appendix 2 of this Code of Conduct;
ii. provide a report of the review, within 5 months of the Provisional Certification Date; and,

(c) a written undertaking to observe all of the provisions of this Code that apply to an ADCCA Certified Digital Currency Business

6.2. The Committee may grant Provisional ADCCA Certification. In determining whether to grant Provisional ADCCA Certification, the Code Compliance Committee shall consider whether:

(a) the completed Code Compliance Checklist and any supporting materials indicates a very high degree of compliance with the Best Practice Standards set out in Part 4; and,

(b) there is a high degree of confidence that the external audit will verify that the applicant's business processes, systems and policies are adequate to ensure consistent compliance with the Code of Conduct.

6.3. Upon receipt of the self-certification, and before approving the application for Provisional ADCCA Certification, the Committee can require further information including documents supporting the contents of the self-certification in determining whether to grant the Provisional ADCCA Certification.

6.4. Provisional Certification shall automatically lapse in the event that the applicant does not provide an external auditor's report as required by 6.1(b) within 5 months of the Provisional Certification Date or commits any other material act of non-compliance with this Code of Conduct.

7. Certification, Annual Review and Recertification

7.1. A Digital Currency Business seeking certification as an ADCCA Certified Digital Currency Business must commission, at its own expense, and provide to the Committee, an external auditor's report detailing the review by an auditor approved by ADCCA of its business processes, systems and policies in accordance with Appendix 2 of this Code of Conduct, to confirm that they are adequate to ensure consistent compliance with the Code of Conduct.

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

7.3. An ADCCA 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 auditor approved by ADCCA 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; and
(b) for every year that an external audit 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.

7.4. The Committee may grant ADCCA Certification. In determining whether to grant certification or recertification, and before accepting an external audit report prepared in accordance with clauses 7.1 and 7.3(a), the Committee can require from the Industry Member:

(a) documents supporting the contents of the audit report conclusions; and/or
(b) evidence supporting the independence or competence of the auditor.

7.5. 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.

7.6. The ADCCA Board must determine a Code of Conduct Certification Fee that must be paid by the applicant for certification (including provisional certification) or re-certification 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 auditor.

7.7. The Committee must maintain a Code Compliance Checklist (see Appendix 2) which will be used by the external auditors approved by ADCCA as the basis of the initial and subsequent two-yearly external certification and recertification reviews. It will also be used for self-certification. 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 impartiality and professional competence of the external auditor.

7.8. External auditors must be required by the ADCCA 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.

7.9. The Committee must consider the report prepared by the external auditor or the self-certification and must make a determination that certification or recertification under this Code of Conduct be:

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

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

7.11. 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.

7.12. The Committee may amend the Code Compliance Checklist from time to time, and has a discretion to impose extra or waive various elements of the Code Compliance Checklist based on the guidelines set out in clause 5.5.

8. Non-Compliance Reporting, Complaints and Sanctions Process

8.1. An ADCCA Certified Digital Currency Business must undertake to promptly report all incidences of material non-compliance with the Code of Conduct to the Committee.

8.2. 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 ADCCA Certified Digital Currency Business's ability to provide the service;
(c) The extent to which the incident or likely incident indicates that the ADCCA Certified Digital Currency Business's arrangements to ensure compliance with those obligations is inadequate; and,
(d) the actual or potential financial loss to customers arising from the incident or likely incident.

8.3. Where a complaint is made to the EDR scheme and an adverse finding is made against the ADCCA 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.

8.4. Upon investigation of an incident of material non-compliance under clause 8.2 or notification of an adverse finding under clause 8.3, the Committee may:

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

8.5. The Committee will not exercise its discretion to withdraw certification without first giving the ADCCA 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.

8.6. 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.

8.7. An ADCCA Certified Digital Currency Business that receives an adverse finding under the Code of Conduct may appeal the decision to the ADCCA Standards Review Committee, in which

case the ADCCA Standards, Disputes, Complaints Handling and Reviews policy will apply.

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

9. ADCCA Certification Mark

9.1. An ADCCA Certified Digital Currency Business will be entitled to describe itself as “ADCCA Certified” and to use the ADCCA Certification Mark described in Appendix 1.

9.2. A Provisionally ADCCA Certified Digital Currency Business will be entitled to describe itself as “Provisionally ADCCA Certified” or “ADCCA Certification Requested” and to use the Provisional ADCCA Certification Mark described in Appendix 1.

9.3. An ADCCA Certified Digital Currency Business must include a section on its website in the form prescribed in Appendix 1 that explains the nature and purpose of ADCCA Certification and includes a link to this Code of Conduct on the ADCCA website.

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

10. Limitation of Liability

10.1. ADCCA Certified Digital Currency Businesses and applicants for ADCCA 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 ADCCA does not provide products or service to those customers or prospective customers.

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

10.3. Applicants for ADCCA Certification or recertification under this Code of Conduct who are unsuccessful and ADCCA Certified Digital Currency Businesses whose ADCCA 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 ADCCA is in no way liable for any economic loss, loss of profit or other loss associated with the denial or withdrawal of ADCCA Certification. To the extent that ADCCA is found liable, liability is limited to the amount paid to ADCCA by the Digital Currency Business for ADCCA Certification.

10.4. ADCCA excludes all liability it may have to ADCCA 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 ADCCA for such acts or omissions to the total amount of the fees paid by the relevant Member to ADCCA in the relevant financial year.

APPENDIX 1: ADCCA Certification Marks & Explanatory Text

1A: ADCCA Certification Marks

The ADCCA Certification Marks are shown below. They may not be reproduced in any other format or colours and must not be less than 366 by 80 pixels.

Appendix 1B: ADCCA Certification Explanatory Text

The following text explaining the nature and purpose of ADCCA Certification must be included on the website of an ADCCA 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 auditable best practice standards for businesses operating in the Australian Digital Currency industry.
>
> The Code of Conduct is administered by the Australian Digital Currency & Commerce Association 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.
>
> ADCCA 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 an ADCCA approved external auditor and self-certified every other year.
>
> [Company Name] is a member of ADCCA and has held ADCCA 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

Note: For self-certification, print this checklist out and complete the Self-Certification Instructions in the right column, and return to membership@adcca.org.au with all attachments clearly marked in PDF format.

	Area	Audit Criteria (Code reference)	Self-Certification Instructions
Part 3 – Eligibility and Operation			
1.	ABN/ACN	Check the entity is active and not deregistered. (3.2)	*[Set out ABN/ACN here]*
2.	Address of principal place of business	Confirm principal place of business via company search, and confirm subsidiary and branch locations. (3.2)	*[Set out all business locations for subsidiaries and branches of your entity here.]*
3.	Nature of business (are you a dedicated Digital Currency Business or do you also provide other services?)	Profile the entity and identify any ML/TF risks associated with the core business and other services provided.	*[Describe 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?	Assess steps taken by the entity to ensure those acting on behalf of the entity, also adhere to the Code of Conduct. (3.7)	*[Set out here all reasonable steps taken.]*
Part 4 – Best Practice Standards			
Part 4.1 – Reputation and General Conduct			
1.	Are any parts of your business or agents registered with AUSTRAC? If yes, what are they (e.g. money remittance or currency exchange)	Ensure entity is registered with AUSTRAC if required by law (e.g. If they provide a designated service under the AML/CTF Law such as remittance or as an AFSL holder arranging for a person to receive a designated service). (4.1.1)	*[If any parts of your business are registered with AUSTRAC, please provide evidence of which designated services you provide (eg. Attach extract from AUSTRAC's Reporting Entities Roll showing the designated services. Designated services include money remittance, currency exchange or holding an AFSL and arranging for a person to receive a designated service.]*
2.	Is your business subject to any other regulation, domestic or foreign, (for example, regulation by ASIC under an ASIC-issued Australian Financial Services Licence (AFSL) or Australian Credit Licence (ACL))?	Test regulatory status of entity. Eg. Check ASIC register to ensure entity holds a current AFSL or ACL if required by law. (4.1.1)	*[Attach evidence of ASIC-issued AFSL or ACL if you are required to hold such a licence.* *Attach evidence of any other licence or registration that you think is relevant to this Code of Conduct.]*

	Area	Audit Criteria (Code reference)	Self-Certification Instructions
3.	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)?	Assess steps taken (if any) by the entity to ensure compliance with all relevant laws. Randomly test whether those policies and procedures are implemented in practice. For example, work through the onboarding process that the entity offers for new customers. (4.1.1, 4.2.1, 4.3.2)	*[Set out here all reasonable steps taken. For example:* *a) provide links to your privacy policy,* *b) provide a copy of your AML/CTF and Sanctions Program and working documents, and* *c) provide a copy of relevant compliance manuals.]*
4.	Please provide full names of key personnel of your business including directors, shareholders, and other decision makers.	Screen the names of key personnel against the ASIC and AUSTRAC registers including AUSTRAC suspension and cancellation of remittance providers and the Sanctions and PEP lists. Consider bankruptcy and criminal record checks on all Directors, Company Officers and Substantial Shareholders or Controllers. (4.1.2, 4.1.3)	*[Set out full names of key personnel of your business here, including decision makers not recorded with ASIC.* *Attach evidence that demonstrates annual checks have been done against the ASIC and AUSTRAC registers including AUSTRAC suspension and cancellation of remittance providers and the Sanctions and PEP lists. This also includes bankruptcy and criminal record checks on all Directors, Company Officers and Substantial Shareholders or Controllers.]*
5.	For all key personnel, are they able to provide Digital Currency services with integrity, transparency, diligence, and in an ethical manner?	Consider whether each key person has: • competency to operate a Digital Currency Business (as demonstrated by their knowledge, skills and experience); • the attributes of good character, diligence, honesty, integrity and judgement; • not been disqualified by law from performing their role in your business; and • any conflict of interest in performing their role in the Digital Currency Business. (4.1.1, 4.1.2, 4.1.3)	*[Attach information demonstrating that each key person has met the following requirements:* *a) competency to operate a Digital Currency Business (as demonstrated by the person's knowledge, skills and experience);* *b) the attributes of integrity, transparency, diligence;* *c) has not at any time been disqualified by law from performing their role in your business; and* *d) is managing any conflict of interest in performing their role in the Digital Currency Business.]*
6.	Do you maintain a risk-based level of professional indemnity insurance cover for not less than $1 million, and such other insurances as are appropriate?	Check for evidence of professional indemnity insurance cover and any other insurances as are appropriate. (4.1.4)	*[Attach evidence of professional indemnity insurance cover for not less than $1 million.* *Attach evidence of other insurances (eg. A Cyber security protection policy)*

	Area	Audit Criteria (Code reference)	Self-Certification Instructions
7.	Are accurate and complete records of all transactions kept up to date and secure for a minimum of 7 years?	Test record keeping process. (4.1.5)	*[Set out here a sample of records to prove a copy of AML/CTF program, customer due diligence and transactions have been retained.* *Set out here a test for record keeping processes to demonstrate effectiveness.* *Attach any record keeping policies.]*
4.2 – Consumer Protection			
8.	Do you maintain a customer Privacy Policy?	Assess appropriateness of 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. (4.2.1) Test whether the entity complies with Australian Privacy Principle 11: Security of Personal Information, by asking for evidence of compliance. (4.2.2)	*[You have already provided links to, or attached your Privacy Policy.* *Attach evidence that shows it is available and referred to whenever personal information is collected.* *Show how you comply with Australian Privacy Principle 11: Security of Personal Information. This includes showing how you protect, hold, and then delete or deidentify personal information once it is no longer needed for any purpose for which the information was collected. Go to the OAIC.gov.au website for guidance on this obligation.]*
9.	How do you manage data security?	Test that the entity has complied with its obligations to: • build and maintain a secure network; • protect customer data, including securely storing the customer data and encrypting any transmission of data across open, public networks; • maintain a vulnerability management program; • implement strong access control measures; • regularly monitor and test networks; and • maintain an information security policy. (4.2.2)	*[Provide evidence that shows 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; and* *f) maintain an information security policy.]*

	Area	Audit Criteria (Code reference)	Self-Certification Instructions
10.	Do you operate a separate trust account?	Check for separate trust account details, or attempts to open a separate trust account. Test whether trust account procedures have been implemented in line with the Code of Conduct obligation (4.2.3)	*[Set out here the steps taken to open and maintain a separate trust account. Attach your policy or an explanation as to how you manage the account.* *Attach evidence of this account in operation.]*
11.	If you provide a service of storing, holding, owning or controlling Digital Currency, do you follow appropriate procedures for this service?	Assess procedures used by the entity if providing this service, and whether they are in line with the Code of Conduct obligation. (4.2.4)	*[If you provide this service, attach evidence that you hold Digital Currency of the same type and amount as that which is owed to the customer.* *If you provide this service, attach evidence that you do not use the Digital Currency unless directed by the customer.]*
12.	Are you a member of an External Dispute Resolution (EDR) Scheme?	Check for details of the entity's membership of an EDR Scheme. (4.2.5)	*[Attach evidence of your membership of an EDR Scheme.]*
13.	Do you clearly describe your pricing and fee structures on your website?	Check for clear disclosure of pricing and fee structures on website. (4.2.6)	*[Provide a link to the relevant part of your website where pricing and fee structures are set out.]*
14.	Do you clearly describe your complaints handling process and contact details on your website?	Check for clear disclosure of complaints handling process and contact details on website (4.2.7)	*[Provide a link to the relevant part of your website where the complaints handling process and contact details are set out.]*
Part 4.3 – Anti-Money Laundering and Counter-Terrorism Financing Obligations			
15.	Have you established a AML/CTF and Sanctions Compliance Program?	Ensure that the AML/CTF and Sanctions Compliance Program includes the elements required by clause 4.3.2 of the Code of Conduct, and randomly test that it is being complied with.	*[Provide examples of how your AML/CTF and Sanctions Compliance Program is working or wll worki 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) Example of employee training taking place.* *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*

	Area	Audit Criteria (Code reference)	Self-Certification Instructions
			compliance meeting discussing AML/CTF risks). *f) Example of AUSTRAC "dob-in" reporting (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.]*
16.	Do you ensure your customers or their payees* (if applicable) are not in countries subject to a Sanctions regime (see dfat.gov.au website for a comprehensive list of countries) or to other High Risk countries?	Review list of customer or payee (if applicable) countries. (4.3.2(3), 4.3.3(g))	*[Set out here 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.]*
17.	Do you ensure that your customers or their payees (if applicable) are not themselves on any Sanctions lists?	Review Sanctions checking processes. Sanctions screening must either be done manually incorporating the relevant lists below, or done via subscriptions with a reputable provider. (4.3.2(3)).	*[Describe how you check customers and their payees (if applicable) against Sanctions lists and provide examples.* *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.]*

	Area	Audit Criteria (Code reference)	Self-Certification Instructions
18.	Have you terminated any staff, agents or third parties due to non-compliance with the AML/CTF Laws, Sanctions Laws, or business policy?	Test for termination of employee, agent or third party. (4.3.2(b), 4.3.6, 4.3.7)	*[Attach evidence that reflects a termination of an employee, agent or third party due to non-compliance with the AML/CTF Laws or Sanctions Laws obligations, or explain why this has not occurred.]*
19.	Does your ML/TF risk assessment framework meet the minimum requirements?	Ensure that the ML/TF risk assessment framework includes the elements required by clause 4.3.3 of the Code of Conduct, and randomly test that it is 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 effectively.	*[Before you provide your ML/TF risk assessment framework, make sure that it demonstrates that consideration has been given to 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.* *Provide evidence of a low risk customer file, a medium risk customer file and a high risk customer file that demonstrates the application of the above risk assessment framework. Evidence may include screenshots or PDF documents of collected evidence related to that particular customer, as well as their database profile.]*
20.	Has your AML/CTF and Sanctions Compliance Program been independently reviewed?	Explain why you as auditor, are sufficiently independent. Consider when the last independent review was conducted and whether it complied with the Code of Conduct 2-yearly requirements (see clause 7.7). (4.3.4)	*[If applicable, provide a copy of your last independent review.]*
21.	Does your KYC information include the extra requirements set out in clause 4.3.4 of the Code of Conduct?	Assess the verification and KYC procedures used, when onboarding or reviewing a customer, and ensure that the information required by clause 4.3.4 of the Code of Conduct has been collected.	*[In addition to the minimum KYC information to be collected, attach example transaction data, that shows:* *a) evidence that a customer's location at the time of transaction, or their IP address is collected;*

	Area	Audit Criteria (Code reference)	Self-Certification Instructions
			b) details about the customer's funding provider (e.g. a bank in the case of fiat currency or e-wallet provider in the case of Digital Currency) and its location; and *c) in the case of a value transfer from the customer to another person, the payee's name and location.* *Describe the risk-based procedures used to verify the above information each customer. For example, if the customer or their IP address is in Syria and the customer is using their Australian bank to buy BTC, this should be considered high risk and various verification measures should be in place that are not required for lower risk locations..* *In the case of a value transfer, show how PEP screening is conducted on all payees.*
22.	Do you engage third parties or agents that you rely on to provide your services or perform customer due diligence, including liquidity providers (eg. Digital Currency exchanges) or providers of electronic wallet services? If so, please provide details about who they are and how you monitor them.	Ensure that the entity performed normal customer due diligence (CDD) measures on the third parties. Ensure that the entity had approval from senior management before the relationship was established. 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, 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 (eg. Do they have clear written Service Level Agreements with third parties that the entity understands and that can be enforced?). (4.3.6., 4.3.7)	*[Attach evidence of information you have collected about your third parties, before onboarding them, and as part of your ongoing monitoring of their performance.* *Also, attach information about how you appoint and monitor high risk third parties, including (where applicable):* *a) liquidity providers* *b) digital currency exchanges* *c) providers of electronic wallet services.* *In the case of high risk third parties, show how you have considered their reputation, the quality of supervision, regulatory history, their AML/CTF Law (or non-Australian equivalent) compliance, and the adequacy of their CDD procedures.* *Attach evidence of senior management approval before the relationship was established with the third party.* *Attach written agreements with High Risk third parties.]*

	Area	Audit Criteria (Code reference)	Self-Certification Instructions
23.	Do you use third party electronic wallet providers?	Test whether the entity has ensured that their electronic wallet providers are conducting CDD on their customers. (4.3.7(h))	*[Attach evidence that reflects a termination of an affiliate or third party.]*
Part 9 – Non-Compliance Reporting, Complaints and Sanctions Process			
24.	Does your business have a procedure in place to report all incidences of material non-compliance with the Code of Conduct, to the Committee?	Test whether the entity has a process for identifying non-compliance with the Code and reporting material breaches. (8.1, 8.2)	*[Attach your breach reporting procedure, and evidence that it is working in practice.]*
25.	Do you notify ADCCA when you are required to?	Test whether the entity has a process for notifying ADCCA when it is required to, for example, if an adverse finding is made under an external dispute resolution Scheme or if a material breach is identified.	*[Attach your complaints handling procedure, and ensure that it shows your process for notifying ADCCA of adverse findings or material breaches of the Code of Conduct.]*
26.	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?	Where there is regulatory action, check for remediation effort.	*[Set out details of any regulator action, and the status of any remediation.]*
Part 8 – ADCCA Certification Mark			

	Area	Audit Criteria (Code reference)	Self-Certification Instructions
27.	Do you have an ADCCA Certification Mark and Explanatory Text included on your website?	Review appropriate inclusion of the ADCCA Certification Mark and Explanatory Text on the entity's website, in line with Appendix One of the ADCCA Code of Conduct. (8.2)	*[Attach evidence of ADCCA Certification Mark and Explanatory Text on your website.]*