IN THE HIGH COURT OF NEW ZEALAND
CHRISTCHURCH REGISTRY

I TE KŌTI MATUA O AOTEAROA
ŌTAUTAHI ROHE

CIV 2019-409-544

Under   Part 19 of the High Court Rules and Part 16 of the
                          Companies Act 1993

In the matter of   an application concerning **CRYPTOPIA LIMITED (IN
                          LIQUIDATION)**

And

In the matter of   an application by **DAVID IAN RUSCOE and MALCOLM
                          RUSSELL MOORE of GRANT THORNTON NEW
                          ZEALAND LIMITED**

                          Applicants

SECOND AFFIDAVIT OF DAVID IAN RUSCOE IN SUPPORT OF ORIGINATING APPLICATION FOR ORDERS FOR DIRECTIONS REGARDING THE DIGITAL ASSETS

Dated: 8 NOVEMBER 2019

BUDDLEFINDLAY
NEW ZEALAND LAWYERS
Barristers and Solicitors
Wellington

Solicitor Acting: **Scott Barker/Bridie McKinnon**
Email: scott.barker@buddlefindlay.com/bridie.mckinnon@buddlefindlay.com
Tel 64 4 499 4242 Fax 64 4 499 4141 PO Box 2694 DX SP20201 Wellington 6140

SECOND AFFIDAVIT OF DAVID IAN RUSCOE IN SUPPORT OF ORIGINATING APPLICATION FOR ORDERS FOR DIRECTIONS REGARDING THE DIGITAL ASSETS

I, **David Ian Ruscoe**, of Wellington, Chartered Accountant and accredited insolvency practitioner, swear:

1.   I am a Chartered Accountant by profession, and I am a partner in the Wellington office of the firm Grant Thornton. I am also a RITANZ accredited insolvency practitioner. I am authorised to swear this affidavit on behalf of the Applicants.

2.   I wish to refer to the evidence in the following affidavits by way of background to this application:

   (a)   The affidavit I swore on 17 May 2019 in support of an application by the liquidators of Cryptopia Limited (in liquidation) (**Cryptopia** or the **Company**) for orders varying the mode and timing of sending the various Liquidators' Reports under ss 255 and 257 of the Companies Act 1992, including the declaration that I made in support of Chapter 15 bankruptcy proceedings in the United States, which is annexed at DIR1/1 to that affidavit. The Court filing number for that proceeding is CIV 2019-409-247.

   (b)   The affidavit I swore on 22 May 2019 seeking variation to the service orders in respect of the proceedings referred to as CIV 2019-409-247.

   (c)   The affidavit I swore on 28 May 2019 in support of an application by the liquidators of Cryptopia for directions in relation to digital assets of Cryptopia. The Court filing number for that proceeding is CIV 2019-409-286.

   (d)   The affidavit I swore on 1 October 2019 in support of the interlocutory application for directions as to representation and service filed in this proceeding.

3.   I make this further affidavit to provide the Court with a more detailed explanation of what we have been able to ascertain about the Account Holders and their actual or assumed holdings in the Digital Assets, as well as unsecured creditors and assets of the Company.

Background

4.   Cryptopia was incorporated on 29 July 2014. As outlined in my earlier affidavit, it carried out business as a cryptocurrency exchange, that allowed users to register an account and trade various cryptocurrencies.

5.   There are over 2 million registered accounts with Cryptopia. In January 2017 Cryptopia had only 30,000 users. The majority of users joined from November 2017 to January 2018 following the Bitcoin price explosion from approximately USD4,350 to almost USD14,000. The number of registered users grew by over 940% in this quarter. Cryptopia marketed itself through channels like Google and TradeMe ads.

6.   In January this year Cryptopia was hacked, and a significant amount of cryptocurrency was stolen from it. On 14 May 2019, Mr Moore and I were appointed liquidators of Cryptopia by a special resolution of shareholders. A copy of the special resolution is annexed to my earlier affidavit of 17 May 2019 at DIR2.

7.   Cryptopia holds a significant amount of cryptocurrency, both in terms of fiat currency equivalent value and in number. Mr Moore and I have estimated the total NZD value of the cryptocurrency held by Cryptopia to be approximately NZD170 million, based on the data obtained on customer coin balance that we have retrieved from the SQL database (I explain this is further detail below). As explained in earlier affidavits the market values of cryptocurrencies can fluctuate significantly over short periods of time. It is therefore difficult to be precise about the total value of the holdings from day to day.

8.   We have filed this application to seek directions on whether the cryptocurrency is property and whether it is held on trust for account holders, in order to ascertain our obligations in respect of it.

9.   I attach the spreadsheets titled "*user summary 2019-10-18*" (**User Summary spreadsheet**) and "*coin summary 2019-10-24*" (**Coin Summary spreadsheet**) as an annexure to this affidavit, to be provided by way of USB flashdrive, and will refer to the spreadsheets as annexure "**DIR2**". I will refer to the data provided in these spreadsheets within this affidavit.

Digital Assets in respect of which directions are sought

10.   We have created a list of all of the types of cryptocurrency in our control. This list is provided in the "Coin Summary" tab of the Coin Summary spreadsheet.

11.   We are currently in the process of reconciling the total amount of cryptocurrency that is actually held by Cryptopia. Once we have ascertained the amount of cryptocurrency that is held, we will be able to reconcile the Company's holdings with Account Holders' coin balances.

12.   We have recovered and secured approximately 75% by volume of currencies, namely those in cold wallets. The remaining 25% were held in hot wallets on the servers in Phoenix, Arizona that were compromised in the January hack. To verify the cryptocurrencies held the coding needs to be recreated and the wallets 'stood up' to verify the contents of each wallet to the appropriate crypto blockchain.

13.   Cold wallets are held offline, and hot wallets are held online. The verification process is time intensive, because the hot wallets that were compromised in Phoenix might still have traces of malware left over from the hack, necessitating some re-writing of computer code. We understand that Cryptopia typically held:

  (a)   One hot wallet per currency; and

  (b)   separate cold wallets for supposed company holdings and customer holdings of the same currency.

14.   For example, with Bitcoin (BTC) the Company had more than one cold wallet to allow top-ups of the hot wallet, which may have been needed when withdrawals reduced the hot wallet balance to less than was needed to meet withdrawal requests.

15.   Cold wallets are more secure than hot wallets, because they cannot be hacked. We understand that this is why Cryptopia held multiple cold wallets for some cryptocurrencies. That way, if a cold wallet had to be put online (making it a hot wallet) in order to top up the amount available for withdrawals, security would not be compromised for the cryptocurrency held in the other cold wallets.
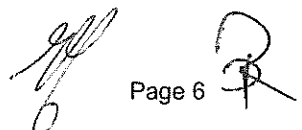
Contractual terms

16.   The only written contractual terms and conditions governing the users' relationship with Cryptopia that have been found were the two sets annexed to my earlier affidavit sworn on 1 October 2019 at pages 2 to 20 of DIR1, along with the risk statement and privacy policy, attached at pages 1 to 11 of DIR3.

17.   The most recent terms and conditions came into effect on 7 August 2018. The Company was solvent at this time. Attached at pages 12 to 15 of DIR3 is the balance sheet and profit and loss statement at 8 August 2018, which evidences this.

Explanation of how the exchange worked

18.   In preparation for this application we requested that Cryptopia staff members provide a detailed explanation, with screenshots of key steps, on the process for making a deposit, withdrawal, trade and transfer of cryptocurrency on the Cryptopia exchange, and the process for converting fiat currency into a bank account into cryptocurrency that was able to be traded on the exchange. Attached at pages 16 to 56 of DIR3 are five documents that set out a detailed explanation of the process for each of the following:

(a)   Making a deposit;

(b)   Making a transfer;

(c)   Making a trade;

(d)   Making a withdrawal;

(e)   Depositing cash to receive NZDT.

19.   These documents were prepared by Malcom Gray, a Customer Support Officer at Cryptopia.

20.   From 25 May 2018 Cryptopia had an internal manual for its staff members, that sets out useful information on how the exchange operated. The Customer Support Training Manual, version 1.1, dated 25 May 2018 is attached at pages 57 to 92 of DIR3. On 7 October 2018 version 2.0 of the Manual came into effect (**Updated Manual**) (together with version 1.1, the

Manuals). A copy of version 2.0 is attached at pages 93 to 198 of DIR3. This is the most recent version and was in effect at the date of liquidation.

21.   I will refer to these documents in providing an explanation of how the exchange operated.

22.   In order to trade cryptocurrencies on Cryptopia's exchange, a user was first required to register with Cryptopia to open an account and to make a deposit or purchase in one of the 5 'base currencies'. A deposit would be made into a hot wallet for the cryptocurrency in question. (Once deposited the currency could be left in the hot wallet to meet withdrawal requests from other users or be transferred to a cold wallet at Cryptopia's discretion.)

23.   The process for making a deposit is described in the deposit document, and the cashing in/ out with NZDT document prepared by Mr Gray at pages 16 to 19 and 55 to 56 of DIR3 respectively. The registration and deposit process is also described in the Updated Manual at pages 103 to 106 and 126 to 138 of DIR3 respectively.

24.   Once the registration process was complete, and Cryptopia had processed the deposit, Cryptopia would provide the user with a positive coin balance in the user's account on the exchange in an equivalent amount to the customer's deposit. Once the user had a positive coin balance, the user would be able to transfer, trade or withdraw that coin balance (in whole or in part).

25.   There is a difference between digital wallets that are used to trade cryptocurrency outside of the exchange, and the accounts that allowed users to trade on the exchange. The exchange was essentially like a closed-circuit system. When a deposit was made, the actual cryptocurrency that had been deposited was not stored in the user's account. It was stored in digital (hot or cold) wallets exclusively controlled by Cryptopia. The wallets effectively backed the exchange. A user's account only contained a statement of the user's coin balance, which was the amount that the user was able to trade or transfer with other users on the exchange, or apply to withdraw from the exchange, and send to a digital wallet outside of the exchange.

26.   When a trade occurred between two users the users' respective coin balances would change to reflect the trade, but the balance of the Company's digital wallets did not change. For example, if trader A sold 2

BTC to trader B in return for 1000 Pandacoin, the users' coin balances would update to reflect the transaction, but the amount of cryptocurrency held in the Company's digital wallets would remain the same.
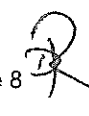
27. Transactions between digital wallets stored outside of the exchange are recorded on a cryptocurrency's public ledger, which is distributed across different networks. Transactions between users on Cryptopia's exchange would be recorded on the internal SQL database, which was Cryptopia's internal ledger of transactions. The trades and transfers that took place on the exchange did not affect the blockchains, and general ledger of ownership that exist for each coin outside of the exchange (i.e. Bitcoin). This is because at all times the coins were held in the Company's digital wallet. The actual cryptocurrency never transfers between users when a trade is made.

28. This 'closed-circuit system' relied on its own internal SQL database to record all transactions between users on the exchange. The internal ledger was able to be controlled by Cryptopia, and if any transactions were made in error, Cryptopia had the ability to reverse the transactions and update account holders' coin balances. This explains how Cryptopia had the ability to reverse trades that occurred on the exchange, but it could not reverse any withdrawals made from the exchange. Once a withdrawal was made, the coins had left the Company's digital wallet, and are unable to be retrieved.

29. I refer to the affidavit of Christopher Kirk Watson sworn 28 May 2019 on a separate directions application that we made in this liquidation. In his affidavit Chris discussed how cryptocurrency transactions occur outside of the exchange, including that both a public key and a private key are required. The public key is essentially the digital wallet address, and the private key is similar to a password, that is known only to the user. A new private key is generated each time cryptocurrency is transferred on the blockchain. Cryptopia exclusively holds the private keys to its digital wallets that contain the cryptocurrencies traded on the exchange. All cryptocurrencies require a private and public key.

30. To be clear, customers did not have access to the private keys of the digital wallets owned by Cryptopia, that stored the cryptocurrency that backed the exchange. Customers had an account on the exchange, which had a password that was only known to the customer. Cryptopia provided a

password recovery service (discussed in detail below and shown in the email correspondence at pages 199 to 201 of DIR3).

31. Cryptopia charged a fee for each trade, and a withdrawal fee. Cryptopia had its own accounts on the exchange, so that when a trade took place the trade fee would be paid into Cryptopia's account for collecting trade fees. The actual cryptocurrency associated with Cryptopia's account holdings on the exchange was held in Cryptopia's digital wallets and pooled along with user holdings.

32. The hack stole cryptocurrency from Cryptopia's digital wallets. The hack affected Bitcoin, Ethereum, Litecoin, Bitcoin Cash (BCH) and ERC20 tokens that were stored in the Company's digital wallets.

Accounts with a positive coin balance of realisable value

33. We have reviewed the SQL database, which includes the data on the coin balance of each account, at the date of liquidation (being the date that the exchange closed). This data had been used in preparing the spreadsheets at annexure DIR2.

34. The SQL database shows the coin balance of all account holders as at 14 May 2019 (the date of liquidation). The coin balance data is subject to change. Some account holders have continued to make deposits into the exchange post liquidation, and we are in the process of verifying whether deposits were processed that are not recorded in the coin balance data taken from the SQL database. We understand that the post liquidation deposits have occurred either because those users have established automatic transfers into their Cryptopia account, and/or they have ignored the multiple notices about the liquidation and continued to transfer currency into their Cryptopia accounts. This is in spite of our multiple requests to users not to send cryptocurrency to the exchange.

35. My colleagues, under my supervision, have carried out an exercise of converting the value of all customer holdings into NZD at available conversion rates to get an approximate value of the customer coin balances and identify the number of account holders that have a positive coin balance of realisable value.

36. This process involved two conversions. First, from the cryptocurrency into BTC, and secondly from the BTC value into NZD. To calculate the estimated total BTC value we used the BTC conversion rate for each

cryptocurrency set in columns AN-AQ of the Coin Summary spreadsheet at DIR2. To calculate the NZD value we converted the estimated total BTC value into NZD using the conversion rate between BTC and NZD of BTC1: NZD11,652.79 that was valid at 24 October 2019.

37. The *User Summary 2019-10-18* spreadsheet shows that there are 960,143 account holders with a positive coin balance. The spreadsheet groups account holders into bands increasing by NZD100 increments, NZD1000 increments and NZD5000 increments. The total NZD value of user coin balances at 24 October 2019 is estimated to be NZD170.95 million.

38. My colleagues also carried out an exercise to identify account holders with a positive coin value of nil NZD value. There are 104,186 account holders with a deemed nil value. Of the 960,143 account holders with a positive coin balance, 855,975 have a positive coin balance of realisable value. The results of the exercise were shown as follows:

A	B	C
Row Labels ▾	Count of UserName	Sum of NZD Equivalent
-1-0	104,186	$ -
>0	855,957	$ 170,950,009
Grand Total	960,143	$ 170,950,009

39. We have provided these values as an indicative measure. To be clear, this conversion was purely a desktop calculation exercise to enable us to provide estimated NZD values to the Court. The conversion rates used do not take into account transaction costs (such as withdrawal fees, and cost of opening an account at another exchange to convert the coin into BTC). In addition, the conversion rates between any cryptocurrency and BTC, and BTC and NZD are constantly subject to change.

40. To give the Court one example of how these values can change, Cryptopia has one Account Holder who holds c.26 billion tokens of Dentacoin, an ERC20 token. These were trading until recently at or around USD $0.0000001 per token. A recent price shift to $0.0001 per token has resulted in that Account Holder now holding over NZD4 million worth of that currency, when previously it was worth less than NZD1. Based on the coin conversion rates used to produce the spreadsheets attached at DIR2 this is now the single largest account balance of all Cryptopia's Account Holders.

Company owned accounts

41.   We have identified that there are 27 company owned accounts. These accounts were identified by discussion with Dave Sanders, a former general manager at Cryptopia, and by manually filtering all accounts with an @cryptopia.co.nz email address. Those accounts are:

(a)   CryptopiaTrade

(b)   SYSTEM_CRYPTOPIA_INCOME

(c)   WithdrawalFees

(d)   ListingFees

(e)   DotcoinSales

(f)   RecoveryFees

(g)   DustBin

(h)   FraudRecovery

(i)   System

(j)   PromotionalGiveaways

(k)   OutgoingExpenses

(l)   RewardBot

(m)   Btc (transferreturns-btc)

(n)   XSNRecovery

(o)   Coinrecovery

(p)   PayopiaIncome

(q)   CEFS_USER

(r)   Lotto

(s)   Mineshaft

(t)   Etn

(u)   CryptopiaMarketing

(v)   coinwalletsAccount

(w)   SYSTEM_USER_TRACER

(x)   Bitcoin

(y)   CryptopiaTestUser

(z)   Poloniex

(aa)   Unit.

42.   The "All Users" tab within the *User Summary 2019-10-18* spreadsheet (an Accounts Spreadsheet) shows that the company owned accounts CryptopiaTrade and SYSTEM_CRYPTOPIA_INCOME have the second and fourth largest account balances based on the conversion process discussed above.

Identifying account holders

43.   A list of all accounts, by username and email address, that have a positive coin balance is **attached** in the User Summary spreadsheet. The User Summary spreadsheet contains the following information on each account holder:

(a)   Username.

(b)   Email.

(c)   Country of the IP address detected by Cryptopia's server for each user, other than users with level 3 verification (explained below). For level 3 verification users the country metric was determined by the information provided by that user when applying for level 3 verification.

(d)   Number of currencies held.

(e)   Estimated total BTC value of the coin balance, calculated through converting all cryptocurrencies into BTC.

(f)   Biggest holding in coin type.

(g)   Biggest holding value in BTC.

(h)   Verification level.

(i)   Account registration date.

(j)   Last log in date.

(k)   Total number of trades.

(l)   Last trade date.

(m)   Last withdrawal date.

(n)   The NZD conversion of (e).

44.   The information that Cryptopia required its users to provide depended on the verification level of the customer. The Customer Support Training Manual **(Manual)** (pages 106 to 112 of DIR3) explains the verification levels.

45.   There are four separate verification levels being level 1, level 2, level 3 and legacy, and the levels affect the amount of trades and withdrawals that a user can make within 24 hours (referred as the daily limit). The daily limits are as follows:

(a)   Level 1 verification had a withdrawal and trade limit of NZD5,000.00 per 24 hours.

(b)   Level 2 verification had a withdrawal and trade limit of NZD50,000.00 per 24 hours.

(c)   Level 3 verification had a withdrawal and trade limit of NZD500,000.00 per 24 hours.

(d)   Legacy customers had no trading limit. Legacy customers were established before the verification process, when Cryptopia did not require its customers to go through an AML process.

46.   All users automatically had level 1 verification once they completed the registration process. Users then had the options to apply to move to verification level 2, or 3.

47.   The registration process required the user to create a username and password, and provide an email address that was not associated with another Cryptopia account. The user was then required to verify its email address (page 104 of DIR3).

48. To become a level 2 verified customer, the following additional information was required:

    (a) The user was required to complete a form with the following information:

        (i) First name.

        (ii) Last name.

        (iii) Birthday.

        (iv) Country.

        (v) City.

        (vi) State.

        (vii) Postcode.

        (viii) Address.

    (b) Identification documents:

        (i) Users were required to upload a photo of an identification document, which was required to be a "*government issued current passport, Driver's License or Identity Card*" that had not expired. Page 15 (page 108 of DIR3) of the Updated Manual states that a "*Government issued identity card*" is required. The identity document was required to display a clear picture of the user, and include the user's full name and date of birth.

        (ii) Users were required to upload an additional photo of themselves holding the identification document. The user's face was required to be visible, along with the user's full name and date of birth.

49. Cryptopia's method of verifying the identification document was to check that the user's full name in the form matched the characters in the identification photographs (page 112 of DIR3). Cryptopia's method for verifying the user's address was to check that the address existed on Google maps.

50. To become level 3 verified a customer was required to email verification@cryptopia.co.nz with more detailed personal information, including:

(a) An additional photo of the user holding the ID that was submitted for level 2 verification with another piece of paper with their handwritten username on it;

(b) Proof of address which is described as "*a utility bill, bank statement/letter, or other government communication*";

(c) A statement as to their source of wealth which is described as "*how they have made enough money to be trading at this level*";

(d) Additional information if the account is owned by a company.

51. The number of account holders at each verification level can be calculated by applying the relevant filter to the Accounts Spreadsheet. I am advised this shows that there are:

(a) 839,804 account holders with level 1 verification;

(b) 48,887 account holders with level 2 verification;

(c) 272 account holders with level 3 verification;

(d) 44,185 account holders with legacy verification; and

(e) 12 account holders with a pending status.

52. There were 44,185 Legacy level Account Holders. As discussed, Legacy customers were established before the verification process. These users had an unlimited trading limit and were not required to provide identification information to Cryptopia for AML purposes, as far as we know at this stage. Their combined holdings are valued at approximately NZD23 million at 24 October 2019.

53. Cryptopia operated a password recovery system for situations when account holders forgot the password to their account. The attached emails dated 19 March 2019 at pages 199 to 201 of DIR3 set out how the password recovery system worked. The user was required to provide three pieces of information about the account, including at least one piece of primary information (information on trades or balances), and two pieces of information on account activity. Instead of the second piece of information on account activity the user could provide "*a valid photo ID, as well as a picture of yourself holding the same photo ID and a handwritten note with today's date and your username, along with another photo of proof of*
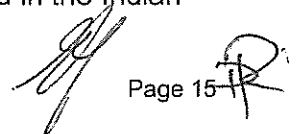
address such as a utility bill". The email sent at 11:56 on 19 March 2019 makes clear that Cryptopia does not hold Account Holders' PINs or passwords. (Pages 199-200 of DIR3)

Additional information available

54. The additional information available for each account is the information listed above at paragraph 43, being information that we have identified from the exchange. This information is included in the User Summary spreadsheet.

55. The User Summary spreadsheet identifies 231 different countries and territories with which customers are associated by reference to IP address. The top ten countries by Account holder numbers are (in descending order by number):

    (a) USA

    (b) Russia;

    (c) UK;

    (d) India;

    (e) Netherlands;

    (f) Germany;

    (g) Japan;

    (h) Canada;

    (i) Brazil; and

    (j) South Korea.

New Zealand has the 26th largest number of Account Holders, with 9,475 accounts.

56. The reliance on the IP address as a basis for identifying the country with which an account was associated is not reliable. This is based on our having identified that the IP address for:

    (a) over 7,000 accounts is shown as the Territory of Ashmore and Cartier Islands, which is an uninhabited external territory of Australia consisting of four low-lying tropical islands. The territory is located in the Indian

Ocean situated on the edge of the continental shelf, about 320 km off the northwest coast of Australia.

(b) Over 5,000 accounts is shown as the Coral Sea Islands Territory, which is an external territory of Australia comprising a group of small and mostly uninhabited tropical islands and reefs in the Coral Sea, northeast of Queensland, Australia. The only inhabited island is Willis Island, which has regular population of four people.

(c) Over 12,000 accounts is unable to be identified by reference to a particular country; and

(d) 29 accounts is shown as the Democratic People's Republic of Korea (also known as North Korea), which we have identified as an error.

57. The aggregate value of holdings associated with the 25,000 accounts referred to in 56 above was over NZD3.2 million as at October 2019 (being 275.5BTC).

Identification of the individual account owners

58. My co-liquidator, Mr Moore, and I have given careful consideration to the limited personal identification information available because, in our view, it raises various issues including AML compliance which I will explain below, as well as issues with what level of identification is sufficient in order to determine who the object of any trust might be. Our considered view is that:

(a) In respect of the majority of accounts, we cannot identify the individual account owner on the information available. For example, the only information held for users with level 1 verification is a user created username and an email address. The User Summary spreadsheet shows the usernames and email address. Many are an alpha-numeric sequence.

(b) If an individual makes a claim in the liquidation on the basis of being an account holder (whether as an unsecured creditor or as a beneficiary of a trust), we will need a reliable method for verifying that account holder's purported account ownership.

(c) If we are unable to reliably verify account ownership, any trust might fail for administrative unworkability.

59. Anonymity is one of the key advantages of cryptocurrency trading, to its users. We anticipate that a number of account owners will choose not to make a claim in the liquidation. We consider that we will not need to take steps to identify those users, however, we seek directions on how to treat any unclaimed holdings belonging to those account holders who choose not to claim in the liquidation.

60. We understand that the terms and conditions give Cryptopia rights to close an account in particular circumstances, including when an account holder refuses to provide information that Cryptopia requires in order to comply with applicable laws and/or AML requirements (I refer to clause 4.4(a)(vi) of the updated terms that were in effect from 7 August 2018 at pages 2 to 17 of DIR1 attached to my earlier affidavit sworn 1 October 2019). We understand that this might have the effect of causing the beneficial interest in the holdings of the closed account to transfer to Cryptopia.

61. We seek directions on whether the terms give us the right to close the account and retain the unclaimed holdings as Company property, and if so, whether we ought to exercise that right and treat the unclaimed holdings as Company property, or whether unclaimed holdings fall to be dealt with in some other way.

AML/CFT verification

62. It is our understanding that we will be required to carry out AML/CFT verification before we can make any distributions to any Account Holders. This will add to the costs of any distributions. The main reason why this exercise is required post-liquidation is that the verification that was carried out before liquidation was not compliant with the legislation, as we understand it. We are looking for a cost-effective and reliable solution for carrying out this exercise. At this stage we have not identified a service provider who can achieve our objectives. Nevertheless, the costs of verification per account could potentially be on average over $50 and possibly higher.

63. To highlight how the cost of distribution is material to whether some Account Holders receive anything out of the liquidation, there are 104,186 Account Holders with an account balance of nil value, and 717,911 Account Holders with an account balance greater than NZD0 and less than NZD100, with the average account balance across that group being NZD12.97. The aggregate value of the accounts in the NZD0-100 band is NZD9.31 million.

64. There are 48,751 Account Holders with an account balance of between NZD100 and NZD200, with the average account balance for this group being NZD141.82. The aggregate value of these accounts is NZD6.9 million.

65. We anticipate that we will need to require any account holder that wishes to make a claim to provide additional identification information in order to comply with our AML/CFT obligations.

Sworn at Christchurch   )

this 8th day of November 2019   )

)   _____
                                                      David Ian Ruscoe

Before me: **Elyse Middleton**
                      Solicitor
                  CHRISTCHURCH

A Solicitor of the High Court of New Zealand

EXHIBIT DIR2

THIS EXHIBIT IS A USB DRIVE THAT CONTAINS TWO EXCEL SPREADSHEETS "User Summary 2019-10-18" and "Coin Summary 2019-10-24".

EXHIBIT NOTE:
This is the exhibit marked **"DIR2"** referred to in the second affidavit of David Ian Ruscoe sworn at Christchurch on   8 November 2019 before me:

Signature:..
A Solicitor of the High Court of New Zealand

~~Elyse Middleton~~
Solicitor
CHRISTCHURCH

Cryptopia Limited Privacy Policy

This is the Privacy Policy for Cryptopia Limited, located at PO Box 1117, Christchurch, 8140, New Zealand. Cryptopia Limited will be referred to as "Cryptopia Limited", "we", "our" and "us" in this Privacy Policy.

The Privacy Policy relates to how we collect, use, share and secure the personal information that you may supply to us. It also describes your choices regarding use, access and correction of your personal information.

We recognise the importance of protecting the privacy of information collected by us, in particular information that is capable of identifying an individual ("personal information").

This Privacy Policy governs the manner in which your personal information will be dealt with. Cryptopia Limited is the entity collecting and holding your personal information in accordance with this Privacy Policy. We reserve the right, at our discretion, to modify or remove portions of this Privacy Policy at any time.

Cryptopia Limited is responsible for the processing of personal data that it receives under the New Zealand Privacy Act 1993, and other applicable international laws.

Please take a moment to read this Privacy Policy carefully. If you have any questions about this Privacy Policy, please contact us at privacypolicy@cryptopia.co.nz. You should review this Privacy Policy periodically so that you are updated on any changes.

Use of Website

By using this website, you agree to the Privacy Policy of Cryptopia Limited, which is set out on this website page. This Privacy Policy is in addition to any other terms and conditions applicable to the website. This website may contain links to other websites not operated or controlled by us, and we do not make any representations about such third party websites.

Collection of Information

We may collect personal information about you through your conduct on our website, via support services, email, telephone, any contact made by you through social media channels and through any other interaction you may have with us.

We collect and hold personal information about, but not limited to:

- users and potential users;
- business associates and potential business associates, and their employees and contractors (where applicable);
- individuals we deal with in the course of providing services to our users;
- suppliers and their employees and contractors;
- employees, prospective employees and contractors; and
- other people who come into contact with us.

1

We collect personal information about you in order for us to provide you with our services, for you to take full advantage of our services, and for us to conduct our business and meet our legal obligations.

Personal information is collected when provided by you, via the website, email, support, phone, social media, or any other interactions you may have with us. For example, we may need to collect such information to provide you with services or to answer or forward any requests or enquiries that you submit to us. Information we collect may include (but is not limited to): names, addresses, contact details, occupations, payment details, employment history, education and qualifications, testimonials, feedback and other information which assists us in conducting our business, providing and marketing our services, and meeting our legal obligations.

We may also obtain information from other sources and combine that with information we collect through our services. For example, we may collect information about you from third parties, including but not limited to social media platforms and publicly available sources.

Registration with the website is voluntary. Registration may include submitting (for instance, but not limited to) your name, email address, address, telephone numbers, and selecting an option to receive updates and promotional material and other information. You may view and edit this information at any time by logging in and going to your account.

We may also collect information about you as permitted by law.

In some cases, if personal information we request is not provided, it might adversely impact our ability to supply you with services or perform our obligations to you.

Any information you provide to us that is not required is voluntary. You are free to choose whether to provide us with the types of personal information requested, but we may not be able to serve you as effectively or offer you Services when you do choose not to share certain information with us.

Collection and Use of Information Collected Automatically

We receive and store certain types of information automatically, such as whenever you interact with the sites or use our services. This information does not necessarily reveal your identity directly but may include information about the specific device you are using, such as the hardware model, device ID, operating system version, web-browser software (such as Firefox, Safari, or Internet Explorer) and your Internet Protocol (IP) address/MAC address/device identifier.

When you visit our website, our web servers gather your IP address to assist with the diagnosis of problems and to enable us to provide the best level of service.

We use cookies on our website to provide you with a better experience. These cookies allow us to increase your security by storing your session ID and are a way of monitoring single user access. This aggregate, non-personal information is collated and provided to us to assist in analysing the usage of the site.

Management of Personal Information

We strive to ensure the security, integrity and privacy of personal information submitted to us, and we regularly review and update our security measures in light of current technologies.

While no data transmission over the Internet can be guaranteed to be totally secure, we will endeavour to take all reasonable steps to ensure the security, on our systems, of the personal information you transmit to us via our online products and services.

In addition, our employees and the contractors who provide services related to our information systems are obliged to respect the confidentiality of any personal information held by us.

Use of Information

Unless we disclose other uses in this Privacy Policy or at the time of collection, personal information about you is used only for the purpose for which it is submitted or for such other secondary purposes that are related to the primary purpose. In general, the purposes for which your personal information is collected, used, held and disclosed are:

   a. to conduct our business;
   b. to provide you with our services and any other services you request;
   c. to market our services to you;
   d. to engage with third parties on your behalf;
   e. to communicate with you;
   f. to help us manage and enhance our services; and
   g. to comply with our legal obligations.

Copies of correspondence sent by you, or from the website that may contain your personal information, are stored as archives for record-keeping and back-up purposes only. All communication from us (including information with regards to new products and services) will provide you with an opportunity to opt out of further communication. You can choose to opt out at any time from receiving marketing communications.

We do not allow the selling of your personal information in any way.

Retention and Disclosure of Information

We take care to allow your personal information to be accessed only by those employees who require it in order to perform their tasks and duties, and to share with third parties who have a legitimate purpose for accessing it.

We may disclose your personal information:

   a. where you have consented;
   b. where disclosure is necessary to achieve the purpose for which the personal information was submitted; or
   c. when the law permits or requires disclosure.

We may also disclose your personal information in special situations where we have reason to believe that doing so is necessary to identify, contact or bring legal action against anyone damaging, injuring,

or interfering with (intentionally or unintentionally) our rights or property, users, or anyone else who could be harmed by such activities.

We may engage third parties to support our operations and/or provide you with services on our behalf. Where we deem it necessary we may disclose personal information held by us to these third parties.

We generally retain personal data for so long as it may be relevant to the purposes for which it was obtained. To dispose of personal data, we may anonymise it, delete it or take other appropriate steps.

Where we no longer require your personal information, we will comply with our legal requirements in respect of that information.

Access to Information

We will endeavour to take all reasonable steps to keep secure any information which we hold about you, and to keep this information accurate and up to date.

The majority of the information that we hold about you will be available for you to review by logging into your online account with us.

Subject to the exceptions set out in the Privacy Act 1993, you may seek access to the personal information that we hold about you. We will require you to verify your identity, and to specify what information you require. A fee may be charged for providing access. If a fee is to be charged, we will advise you of the likely cost in advance.

If, at any time, you discover that information held about you is incorrect, you may contact us to request to have the information corrected in accordance with the Privacy Act 1993.

Links to External Websites

We provide links to websites outside of our websites, as well as to third party websites. These linked sites are not under our control, and we cannot accept responsibility for the conduct of companies linked to our website. Before disclosing your personal information on any other website, we advise you to examine the terms and conditions of using that website and its privacy statement.

Legal bases for processing personal information

The laws in some jurisdictions require companies to tell you about the legal ground they rely on to process, use or disclose your personal data. To the extent those laws apply, our legal grounds are as follows:

      a.   you consent to such processing;
      b.   such processing is required to satisfy our legal obligations;
      c.   such processing is necessary in order to carry out our obligations as part of any contracts we may have with you, or as part of negotiations before entering into a contract with you; or

d. such processing is required in order for us to protect our property and rights, or the safety of Cryptopia Limited, our users, contractors, or other affiliates.

Direct Marketing

If you are a current user, we will only contact you by electronic means (email or SMS) with information regarding any services which are similar or related to those in which you have previously expressed an interest, be that through transaction history or enquiry.

If you are a new user, we will only contact you by electronic means for marketing purposes if you have consented to receive such communications. Direct marketing includes any communications to you regarding advertising or the promotion of products and services. If you do not want to receive marketing communications, at any time and free of charge you may use the opt-out link provided in any communication from us, or contact us at privacypolicy@cryptopia.co.nz.

Individual Rights

We believe that users should be treated equally no matter where they are, and so we are making the following options to control your data available to all users regardless of their location.

You can update certain information by logging into your account with us and accessing your account information and settings. You can also contact us at privacypolicy@cryptopia.co.nz so that we may consider your request under applicable law.

We encourage you to make any individual rights requests through our user support process (https://www.cryptopia.co.nz/usersupport) because this ensures that you have been authenticated already. Otherwise, when we receive an individual rights request via email we may take steps to verify your identity before complying with the request to protect your privacy and security.

Right to withdraw consent. You have the right to withdraw your consent to our processing of your personal information collected on the basis of your consent at any time. Pease note that withdrawing this consent does not affect the lawfulness of processing we may have undertaken prior to the withdrawal of consent. The withdrawal of consent will not affect the lawfulness of processing of information for which consent is not required.

Right of access to and rectification of your personal information. You have the right to request that we provide you with a copy of all personal information pertaining to you that we hold. This information will be provided without undue delay, unless such provision adversely affects the rights and freedoms of other users, contractors or affiliates of Cryptopia Limited. If a fee is to be charged for this service, the full amount will be made known to you in advance. You may also request that we rectify any false personal information pertaining to you that we keep on record. Your right to access and rectification shall only be limited where the expense of providing such access becomes disproportionate to the risks to your privacy, or where the rights of other users, contractors or affiliates may be violated.

Right to erasure. You have the right to request that we erase personal information that pertains to you if that information:

a. is no longer necessary in relation to the purposes for which it was collected;
b. was collected in relation to processing to which you had previously consented, but later withdrew such consent; or
c. was collected in relation to processing activities to which you object, and there are no legitimate overriding grounds for such activities.

If we have made your personal information public and are obliged to erase that information, we will take reasonable steps to inform relevant third parties that are processing your personal information that you have requested the erasure, including all links to, or copies or replications of, your personal information. The above is subject to limitations by relevant data protection laws.

Right to data portability. You have the right to request that we make available any personal information pertaining to you, which we obtained through a contract with you or based on your consent, in a structured, commonly-used and machine-readable format. You may also request that we transfer this information directly to another "controller" where technically feasible, unless the exercise of this right adversely affects the rights and freedoms of others. A "controller" is a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of your personal information.

Right to restrict or object to processing. You have the right to restrict or object to us processing your personal information where one of the following applies:

a. You contest the accuracy of your personal information that we processed. In such instances, we will restrict processing during the period necessary for us to verify the accuracy of your personal information.
b. The processing is unlawful and you oppose the erasure of your personal information and request the restriction of its use instead.
c. We no longer need your personal information for the purposes of the processing, but it is required by you to establish, exercise, or defend legal claims.
d. You have objected to processing, pending the verification whether the legitimate grounds of our processing override your rights.

Restricted personal information shall only be processed with your consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. We will inform you if the restriction is lifted.

Notification of erasure, rectification and restriction. We will communicate any rectification or erasure of your personal information or restriction of processing to each recipient to whom your personal information has been disclosed, if any, unless this proves impossible or involves disproportionate effort. We will inform you about those recipients if you request this information.

Right to object to processing. Where the processing of your personal information is based on consent, contract or legitimate interests you may restrict or object, at any time, to the processing of your personal information as permitted by applicable law. We can continue to process your personal information if it is necessary for the defence of legal claims, or for any other exceptions permitted by applicable law.

Automated individual decision-making, including profiling. You have the right not to be subject to a decision based solely on automated processing of your personal information, including profiling, which produces legal or similarly significant effects on you, save for the exceptions applicable under relevant data protection laws.

Right to lodge a complaint. If you believe that we have infringed your rights, we encourage you to contact us first at dataprotection@cryptopia.co.nz so that we can try to resolve the issue or dispute. You can also complain about our processing of your personal information to the relevant data protection authority. If you are a resident of the European Economic Area, you can complain in the EU member state where you live or work, or in the place where the alleged breach of data protection law has taken place.

You can also complain to the New Zealand Privacy Commissioner.

Postal Address	Office of the Privacy Commissioner, PO Box10094, Wellington New Zealand
Enquiries phone line	+64 800 803 909
Complaints Form	Complete a privacy complaint form

Storage of your personal information. We will try to limit the storage of your personal information to the extent that storage is necessary to serve the purpose(s) for which the personal information was processed, to resolve disputes, enforce our agreements, and as required or permitted by law.

Data Protection Officer. You may reach the Cryptopia Limited Data Protection Officer at dataprotection@cryptopia.co.nz.

Your rights to personal information. Your rights to personal information are not absolute. Access may be denied when:

- Denial of access is required or authorised by law;
- Granting access would have a negative impact on other's privacy;
- To protect our rights and properties; and
- Where the request is deemed frivolous or vexatious.

Problems or Questions

If we become aware of any ongoing concerns or problems with our websites, we will take these issues seriously and work to address these concerns. If you have any further queries relating to our Privacy Policy please contact us in writing at privacypolicy@cryptopia.co.nz.

1. CRYPTOPIA RISK STATEMENT

Date - 20 April 2018

Cryptopia Limited (**Cryptopia** or **we** or **us**) operates an exchange for trading digital assets including cryptocurrencies and tokens (together, **Coins**) at www.cryptopia.co.nz (the **Platform**).

Cryptopia does not permit the trading of Coins which are "financial products" for New Zealand law purposes (also called "securities" outside New Zealand) on the Platform.

Cryptopia is a registered as a financial service provider to operate a money or value transfer service (FSP580928). Cryptopia is not required to hold any licence or other registration in order to provide the Platform in New Zealand.

This risk statement sets out additional information for users of the Platform. Further terms on which we provide the Platform are set out in the **terms and conditions** (available on the Platform here www.cryptopia.co.nz/Home/Terms). By accessing and using our services, and each time the user (**you**) uses our services, you acknowledge having read this risk statement and agreeing to the terms and conditions.

2. Important warning

3. Buying and selling Coins is highly speculative and carries high risk. You may lose some or all of the money or Coins placed on the Platform. You use the Platform at your own risk.
4. You must carefully read all available information, including the risks set out below, and consider your personal financial circumstances before trading on the Platform. If you are unsure about any aspect of trading in Coins, you should seek independent advice before using the Platform.

5. Support requests and complaints

3. We offer a free complaints and IT support service in respect of the Platform. We seek to acknowledge customer requests and complaints within three business days and to resolve (where possible) complaints within 5 to 15 business days.
4. During periods of high trading on the Platform, however, it may take us longer to respond to your request or complaint. This can occur from time to time because of the extreme volatility and sensitivity to market sentiment of Coin markets. For this reason, we do not guarantee our response times. We believe it is better that you understand upfront that there may be delays from time to time.
5. If you are unsatisfied with our resolution of your complaint, you can, without charge, contact our approved dispute resolution scheme provider – Financial Dispute Resolution Service – using the details found on its website: https://fdrs.org.nz/.

6. Risks of using the Platform

8

Market risks

6. Coins can experience extreme price volatility. The exchange price of a Coin may change significantly and you may be unable to transact Coins or money at the anticipated rate or price. Changes in prices may result in large changes in value and/or losses of Coins or money.
7. Past performance is not a reliable indicator or guarantee of future performance. Coin prices go down as well as up.
8. The value of Coins can be affected by many other factors including (but not limited to) future sales or further issues (e.g. airdrops), negative publicity involving the Coin issuer or project, failure to deliver projects or failure of projects to meet expectations, failure of or material damage to the underlying network (including through cyber-attack), fraud or theft by or affecting the Coin issuer or project, competition in the issuer's market, technical failures or setbacks, or general global and economic conditions and sentiments. You must research Coins that you are interested in carefully. Their whitepapers or other offer materials may list further risks which are relevant to holding them.

Processing of transactions

9. There is a risk that transactions cannot be settled or are delayed at settlement, that processing times differ for each transaction, or a transaction may be incorrectly processed. These risks can result from, amongst other issues:
    a. user error when providing transaction details (such as providing an incorrect wallet address or other information);
    b. an error in delivering the consideration for a transaction;
    c. increases in market volume or Platform volume; or
    d. a failure in the Platform processing systems or a failure in an underlying network or software (see further information below at System risk).
10. It may not be possible to reverse a digital currency transaction once processing has commenced.

System risks

11. All Coins, including transactions involving those Coins, rely on the operation of underlying networks and software. As this is developing technology, the networks and software may be subject to technical weaknesses, bugs, system failures, and hacks by external parties. These failures may affect the Platform network and software itself or may relate to a Coin's underlying network and software (including, but not limited to, a weakness in the underlying blockchain). You should understand the operation of the technology underlying a digital currency and the Platform to understand these risks.
12. For example, Coins can be subject to 51% attacks. This refers to an attack on a blockchain by a group of miners controlling more than 50% of the network's mining hash rate, or computing power, or otherwise controlling the blockchain's consensus mechanism in an illegitimate manner. If this happens, the attackers may be able to control new transactions, halt payments or transfer and reverse completed transactions. Cryptopia does not control the blockchain or network for Coins and cannot stop this. If we become aware of an attack, we will assess the best response

on a case-by-case basis, which may include suspending or removing Coins from our exchange.

13. Hackers are sophisticated, and you may also be targeted by 'phishing' attacks or other scams. Phishing includes where third parties masquerade as a legitimate Cryptopia site, social media account, telephone support number or App in order to steal your credentials. You should only access the Cryptopia Web site through its official website (**Cryptopia.co.nz**). Never click on a link or download an App from a third party. We strongly recommend that you enable two factor authentication for all transactions to prevent unauthorised account use. Your Cryptopia passwords should be unique to Cryptopia and should never be stored insecurely on any personal device. If you are a victim of such an attack or scam, the hacker may be able to get you to send them money or Coins inadvertently or they may steal money or Coins.

14. Your ability to use the Platform, buy or sell Coins, or withdraw money, may be affected by these technical failures or attacks.

15. We will make reasonable efforts to notify users where the Platform, or a particular Coin traded on the Platform, has been subject to a technical weakness, bug, system failure, or hack.

16. We may also need to do maintenance or upgrades on the Platform from time to time which could affect your ability to use the Platform, buy or sell Coins, or withdraw money.

Security of private keys and wallets

17. You must be careful when choosing a wallet to store or transmit your private keys relating to your Coins. If your wallet is hacked or another person learns your private key/s, you may lose some or all of your Coins. You should not give your private key or wallet passcode to any other person.

18. If you forget or lose your passcode to your wallet/s, Cryptopia has no ability to provide a back-up or details of your private key or passcode, given the decentralised nature of Coins. This may result in the loss of any Coins stored in that wallet.

19. You should use the highest level of security offered for any wallet that you choose.

Cyber security generally

20. The transmission of information over the internet (including to or from the Platform) is not completely secure or error free. You should stop transacting when it is clear there has been a breach of security or a system failure that poses a risk to security exists (such as malware, ransomware or phishing).

Consumer protection

21. The Platform does not intend to offer or market regulated financial products or securities**.** Therefore, the protections which apply to "regulated offers" (within the meaning in the Financial Markets Conduct Act 2013) or in relation to licensed exchanges under New Zealand law do not apply. General consumer protection law may apply, however, to buying or selling Coins on the Platform, including the services provided by us and, to the extent such consumer laws do apply we do not seek to exclude any of your rights that we cannot by law exclude.

Regulatory risks

22. There is currently no specific regulation of Coins and Coin exchanges in New Zealand, and it is likely that the rules may evolve rapidly. There is also limited guidance on how existing laws and regulations can be applied to Coins and Coin exchanges. New or changing laws and regulations, or interpretations of existing laws and regulations, may adversely impact or significantly change the trading of Coins and the Platform.

23. If we become aware that a Coin which we list is a financial product under New Zealand law, we may de-list it. We may also de-list Coins for other reasons. Delisting may mean that if you hold the Coin there may not be a ready market on which you can sell it, especially if it is not listed on another exchange. You should not assume that any Coin will always be listed by us.

24. Users are responsible for ensuring they comply with all laws regarding the trading of digital currencies applicable in any relevant country for them when using the Platform.

25. Equally, we have no control over whether Coin issuers have complied with laws in any relevant jurisdictions. Any action taken by regulatory authorities or other persons against a Coin issuer or any other person in relation to a Coin may prevent you from selling Coins or otherwise cause a loss in value.

26. Regulatory issues can also cause problems with other important relationships, such as our or your relationship with banks. Many banks currently are shutting accounts which are linked to Coins or dealing in Coins. This has affected our ability to provide certain products.

27. If you are outside of New Zealand you may be subject (or we may become subject) to laws or regulations of other countries which could prevent you from using the Platform or cause us to change the availability of the Platform in your country or how we operate or offer the Platform.

7.   Other information

28. Cryptopia and any person associated with us (including directors, shareholders, employees and any other related parties) may trade and hold digital currencies on our or their own account through the Platform.

29. You need to pay fees for using the Platform. Our trading fees are shown in the trade pair base currency when you place a trade. At time of writing these are set at 0.2% of the trade. This may be subject to change. Withdrawal fees are set per Coin, and clearly shown on the withdraw page. Withdraw fees are adjusted from time to time based on the Coin network fee.

11

Profit and Loss

Cryptopia Limited
For the period 1 January 2018 to 8 August 2018

Trading Income

Staking Income	10,856,908.98
Token Listings	14,605,003.78
Trading fees	26,771,305.38
Total Trading Income	**52,233,218.14**

Gross Profit | 52,233,218.14

Other Income

Exchange revaluation	(19,158,608.95)
Interest Income	8,998.80
Total Other Income	**(19,149,610.15)**

Operating Expenses

ACC	6,982.24
Accounting Fees	1,091.30
Advertising	369.74
Bad Debt	2,000.00
Bank Fees	15,522.64
Cafe Expenses	31,593.53
Charitable Donations	360,000.00
Cleaning	9,889.50
Computer Equipment Expense	27,348.06
Conferences	15,040.09
Consulting	1,285,376.88
Contractor (Infrastructure)	979,987.62
Contractor and sub-contractor payments	2,152,549.80
Depreciation	199,169.21
Entertainment - 100%	10,848.70
Entertainment - 50%	11,334.99
Freight & Courier	10,108.58
Fringe Benefit Tax	22,292.33
General Expenses	106.42
Hosting Costs	2,577,904.84
Income Tax Expense	9,385,927.35
Insurance	3,345.03
Insurance - Health	493.59
Interest Expense	80,313.00
KiwiSaver Employer Contributions	59,431.48
Legal expenses	4,255.89
Light, Power, Heating	8,972.96
Motor Vehicle Expenses	4,770.30
Office Expenses	11,497.17

	1 JAN-8 AUG 2018
Printing & Stationery	3,966.31
Rates	1,853.90
Recruitment Fees	116,833.17
Rent	163,182.60
Repairs and Maintenance	809.24
Salaries	2,295,848.43
Security	49,772.10
Security (Infrastructure)	2,016,844.37
Software Licences & Subscriptions	255,900.74
Sponsorship	466,921.70
Staff Expenses	1,247.86
Staff Gifts	2,618.87
Staff Training	18,334.66
Staff Uniforms	710.39
Subscriptions	4,560.51
Telephone & Internet	28,879.31
Travel - International	103,541.84
Travel - National	33,816.90
Withdrawal Fees Incurred	6,523,637.22
Total Operating Expenses	**29,367,803.36**

Net Profit   3,715,804.63

Balance Sheet

Cryptopia Limited
As at 8 August 2018

	8 AUG 2018

Assets

Bank

Bitcoin	12,870,562.05
Dogecoin	61,147.93
Dotcoin	5,913,906.03
Litecoin	424,731.19
Localbitcoins Wallet	297,147.48
NBS - Cheque Account	2,553,550.95
NBS - Debit Card Account	24,884.39
NBS - On-Call Savings	2,966,636.18
NZDT	182,394.31
USDT	1,167,713.21
Total Bank	**26,462,673.72**

Current Assets

Loan - Resolve Support Services Ltd	287,789.00
Prepayments	465,838.38
Withholding tax paid	0.11
Total Current Assets	**753,627.49**

Fixed Assets

Computer Equipment	809,543.70
Leasehold Improvements	337,448.07
Less Accum Depn - M/V	(10,339.12)
Less Accumulated Depreciation on Computer Equipment	(208,646.75)
Less Accumulated Depreciation on Leasehold Improvements	(23,548.50)
Less Accumulated Depreciation on Office Equipment	(10,735.96)
Motor Vehicle	61,726.09
Office Equipment	246,407.31
Total Fixed Assets	**1,201,854.84**

Total Assets	**28,418,156.05**

Liabilities

Current Liabilities

Accounts Payable	978,043.25
GST	(978,921.70)
Holiday Pay Provision	115,684.55
Income Tax	6,583,414.45
Rounding	0.03
Unpaid Expense Claims	651.53
Total Current Liabilities	**6,698,872.11**

Non-current Liabilities

Drawings – Adam	(2,417,662.40)

	8 AUG 2018
Drawings - Intranel	(1,976,984.34)
Drawings - R P Wood	(83,033.34)
Drawings - Rob	(2,203,777.87)
Net Dividend - Adam	2,440,587.19
Net Dividend - Intranel	1,976,984.36
Net Dividend - Rob	2,199,395.11
Net Dividend - Rose-anna	83,033.34
Total Non-current Liabilities	**18,542.05**
Total Liabilities	**6,717,414.16**

Net Assets

21,700,741.89

Equity

Current Year Earnings	4,842,101.11
Dividend	(7,200,000.00)
Retained Earnings	24,058,640.78
Total Equity	**21,700,741.89**

Cryptopia Limited: Deposits

Please note: no fees were made from deposits. Also, every deposit is entirely dependent on where you are sending the coins from, be it a personal wallet, or another exchange. The only part that Cryptopia would be involved in with deposits, would be generating the actual deposit address and letting the user know which address they should send it to, to get it into their Cryptopia account.

Our guide for this was as follows:

Deposits into your Cryptopia account can be made by any of the following methods:

#1. **Depositing cryptocurrency coins** you already hold, such as Bitcoin;
#2. **Depositing your local currency** using a third party cryptocurrency exchange service.

PLEASE NOTE: Depositing fiat $NZD directly from a New Zealand bank account is currently suspended. We are working on a solution to restore this feature ASAP.

#1. How do I deposit cryptocurrency coins, such as Bitcoin into my Cryptopia account?

You can send **any cryptocurrency coin** listed with Cryptopia to your wallet, simply by transferring it to your Cryptopia deposit address. Follow these steps below.

- **Log in** to your Cryptopia account.
- Hover over the **'B'** icon in the top right menu bar and click **'Deposit'**.
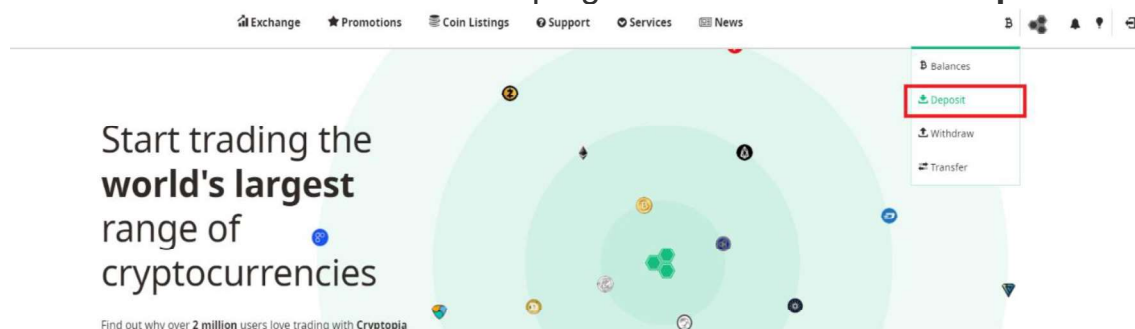
- Select the cryptocurrency coin **you would like to deposit** to your Cryptopia account, e.g. DOT.

Deposit

Please select the currency you would like to deposit to your Cryptopia account.

| Dotcoin(DOT) ▾ |

Next

View Deposit History

PLEASE NOTE: Deposit addresses cannot be generated whilst a wallet is in **maintenance**, **delisting**, or has **no connections** to the network. Deposits will not be received until a wallet is online and resumed connection to its network.

- A **'QR code'** and **'Deposit Address'** will appear on screen for you to use to deposit new cryptocurrency funds.

Dotcoin (DOT)
Please use the address below to deposit new funds.

QR CODE

DEPOSIT ADDRESS

| Back | Done |

WARNING! Please do not mine to your Cryptopia addresses. We do not support transactions from pools like P2Pool etc.

View Deposit History

- Copy the generated **'Deposit Address'** and use it to withdraw the cryptocurrency coins from their location to your Cryptopia account.

PLEASE NOTE: The process for withdrawing your funds will differ depending on the location or platform used to store your cryptocurrency coins. Please, familiarise yourself with that process prior to the execution of your withdrawal.

- Some cryptocurrency coins require an additional **'Payment ID'** (e.g. CryptoNight coins) or **Message** (e.g XEM, BIS), in addition to your **'Deposit Address'**, in order to be received and assigned to your Cryptopia account balance. If an extra field is required for a particular

17

coin, it will be shown on your Deposit page for that coin, together with your '**Deposit Address'.**

PLEASE NOTE: Cryptocurrency coins that require an additional **Payment ID** or **Message** will not be automatically assigned and credited to your Cryptopia account if sent without it.

How do I know if it is a 'CryptoNight' coin?

- Click on the **'Coin Info'** at the top bar.
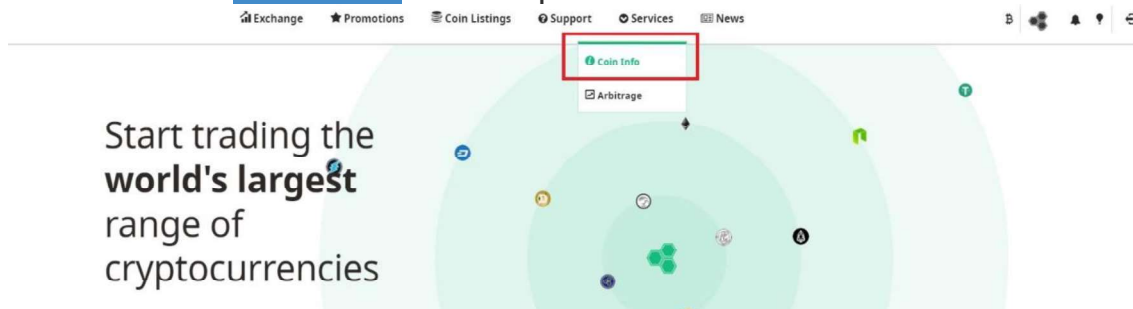
- Type **'CryptoNight'** in the 'Search' box and you will get a full list of 'CryptoNight' coins, which will require an additional **Payment ID** when making a deposit.

PLEASE NOTE: The list of 'CryptoNight' coins may subject to change, check regularly for more updated information.

#2. How do I deposit my local currency into my Cryptopia account (I do not live in NZ)?

If you do not have a New Zealand bank account, the only way to make a deposit using your local currency is by using a cryptocurrency exchange service servicing your domestic country. You should do your research carefully, there are many options available and not all exchange services allow fiat conversion. Choose the right exchange that best meets your requirements and expectations.

PLEASE NOTE: Cryptopia has no affiliation with any third party cryptocurrency exchange service.

Examples of cryptocurrency exchange services include:
- **https://www.coinbase.com/**
- **https://localbitcoins.com/**

Cryptopia Limited: How to buy / sell coins. This works very much like a normal stock exchange.

Please note: This was how Cryptopia made all of it's money, via a 0.2% trade fee incurred with every trade made.

There are four ways to trade on the Cryptopia Exchange:

#1. **Instant Buy** – instantly buy a coin by matching with an existing order. A step by step *example* is detailed below.

#2. **Instant Sell** – instantly sell a coin by matching with an existing order. A step by step *example* is detailed below.

#3. **Open a 'Buy Order'** – create a 'Buy Order' for a coin at a specified price and wait for another trader to match with your order. A step by step *example* is detailed below.

#4. **Open a 'Sell Order'** – create a 'Sell Order' for a coin at a specified price and wait for another trader to match with your order. A step by step *example* is detailed below.

How do I 'Instant Buy' Coins?
- **Log in** to your Cryptopia account.
- Click the **'Exchange'** button in the top left of the menu bar.
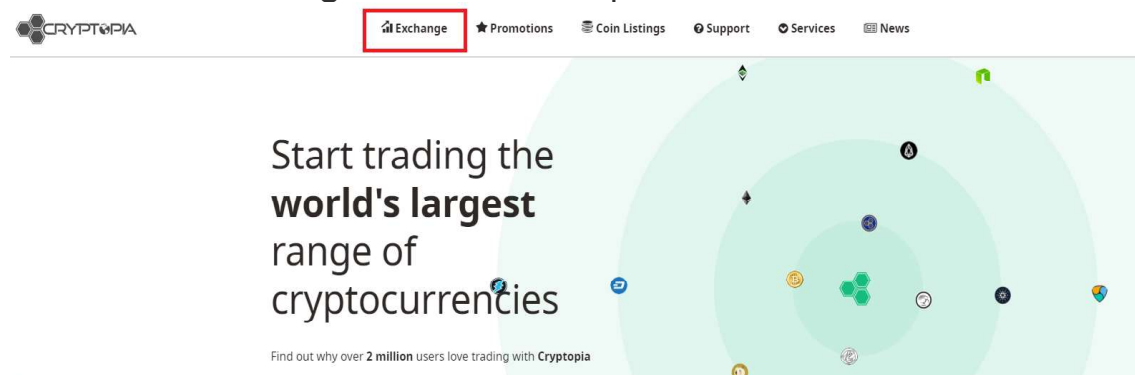
- The left side of the page will show base markets for trading different coins against or trading pairs – BTC (Bitcoin), USDT (US Dollars), NZDT (NZ Dollar Token), LTC (Litecoin) and DOGE (Dogecoin). BTC is displayed as default.

20
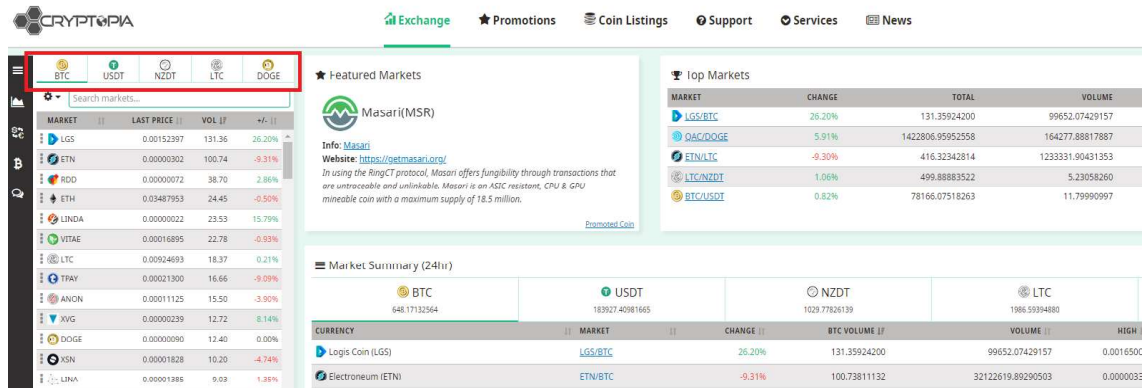
- **Search or filter** the coins available for trade using the 'search markets' field, e.g. type DOT into the Search field to search for Dotcoin. In this example we will be buying DOT in exchange for BTC, or a trading pair of BTC/DOT.

- **Click on the DOT** and the market for this coin will be displayed, showing historical data as well as all the currently available buy and sell DOT orders on the BTC market (DOT/BTC) based on price.
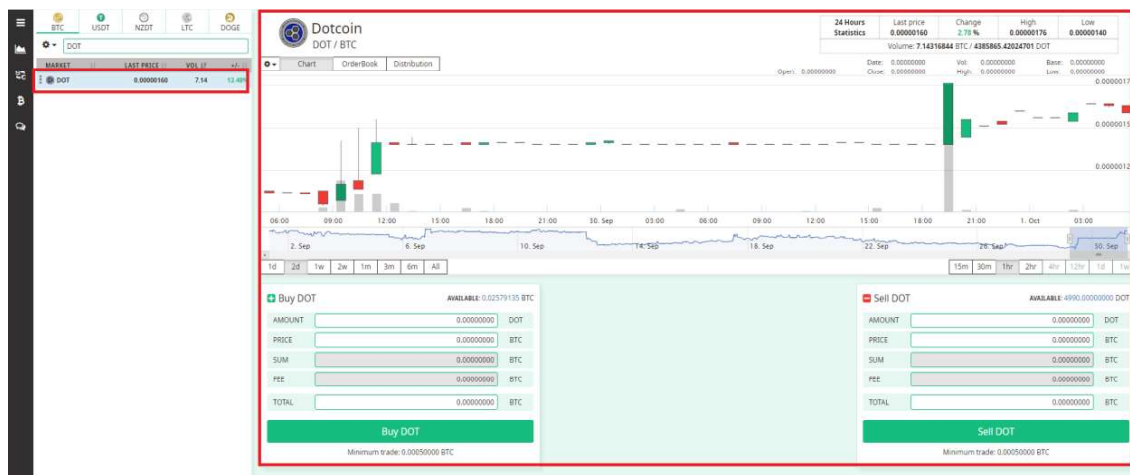
- **Click** on an existing order (as an example, it is circled on the screenshot) you wish to **buy** from the list of current Sell Orders. This will automatically populate the fields ('Amount', 'Price', 'Sum', 'Fee' and 'Total') based on the price already set.

- Click your **'Available'** balance at the top of the box and the order will be adjusted to match your available BTC.

- If you do not want to use your entire balance, you can **manually adjust the 'Total'** to what you want to buy. The other fields will automatically be adjusted.

- Click the **'Buy DOT'** button to complete your order. This will instantly buy DOT coins and credit them to your Cryptopia account using your BTC coins.

Buy DOT		AVAILABLE: 0.02579135 BTC
AMOUNT	200.00000000	DOT
PRICE	0.00005640	BTC
SUM	0.01128000	BTC
FEE	0.00002256	BTC
TOTAL	0.01130256	BTC

Buy DOT

Minimum trade: 0.00050000 BTC

- If there are **insufficient funds** in your account, a 'Trade Notification' will be displayed showing Insufficient BTC funds.

How do I 'Instant Sell' Coins?

- **Log in** to your Cryptopia account.
- Click the **'Exchange'** button in the top left of the menu bar and select Markets from the drop down menu.

24

- The left side of the page will show **base markets for trading different coins against –** BTC (Bitocin), USDT (US Dollars), NZDT (NZ Dollar Token), LTC (Litecoin) and DOGE (Dogecoin). BTC is displayed as default.

- **Search or filter** the coins available for trade using the 'search markets' field, e.g. type DOT into the Search field to search for Dotcoin. In this example we will be selling DOT in exchange for BTC.

- **Click on the DOT** line and the market for this coin will be displayed, showing historical data as well as all the currently available buy and sell DOT orders on the BTC market (DOT/BTC) based on price.

25

- **Click** on an existing order (as an example, it is circled on the screenshot) **you would like to sell** from the list of current Buy orders. This will automatically populate the fields ('Amount', 'Price', 'Sum', 'Fee' and 'Total') based on the price already set.

- **Click your 'Available'** balance at the top of the box and the order will be adjusted to match your available BTC.

- If you do not want to use your entire balance, you can **manually adjust the 'Total'** to what you want to sell. The other fields will automatically be adjusted.

- Click the **'Sell DOT'** button to complete your order. This will instantly sell your DOT coins and credit the BTC coins to your Cryptopia wallet.

- If there are **insufficient funds** in your account a **'Trade Notification'** will be displayed showing Insufficient DOT funds.

How do I Open a 'Buy Order'?

- **Log in** to your Cryptopia account.
- Click the **'Exchange'** button in the top left of the menu bar and select Markets from the drop down menu.

- The left side of the page will show **base markets for trading different coins against –** BTC (Bitocin), USDT (US Dollars), NZDT (NZ Dollar Token), LTC (Litecoin) and DOGE (Dogecoin). BTC is displayed as default.

- Search or filter the coins available for trade using the **'Search Markets'** field, e.g. type DOT into the Search field to search for Dotcoin. In this example we will be buying DOT in exchange for BTC.

- **Click on the DOT** line and the market for this coin will be displayed, showing historical data.

- In the **'Buy DOT'** box input the amount of the coin **you wish to buy** – (in the '**Amount'** row) and how much you want to pay per coin you are buying **–** (in the **'Price'** row).

- The **'Sum'**, **'Fee'** and **'Total'** will then be automatically calculated.

PLEASE NOTE: The '**Total**' must be greater than the '**Minimum Trade**' amount.

- Click the '**Buy Dot**' button and wait for another trader to match with your order.

- To cancel your order, readjust your price, or simply make your coins available again, go to your **'Open Trades'** page, **click on** the order you wish to cancel and **click 'Cancel'.**

Open Orders   Search: [   ]

#	MARKET	TYPE	RATE	AMOUNT	TOTAL	REMAINING	FEE	TIMESTAMP	CANCEL ALL
1270665152	DOT/BTC	Sell	16.00000000	10.00000000	160.000000	10.00000000	0.32000000	3/08/2018 11:10:52 AM	✕

Showing 1 to 1 of 1 entries   Prev 1 Next

How do I Open a 'Sell Order'?

- **Log in** to your Cryptopia account.
- Click the **'Exchange'** button in the top left of the menu bar and select Markets from the drop down menu.

- The left side of the page will show base markets for trading different coins against – BTC (Bitocin), USDT (US Dollars), NZDT (NZ Dollar Token, LTC (Litecoin) and DOGE (Dogecoin). BTC is displayed as default.
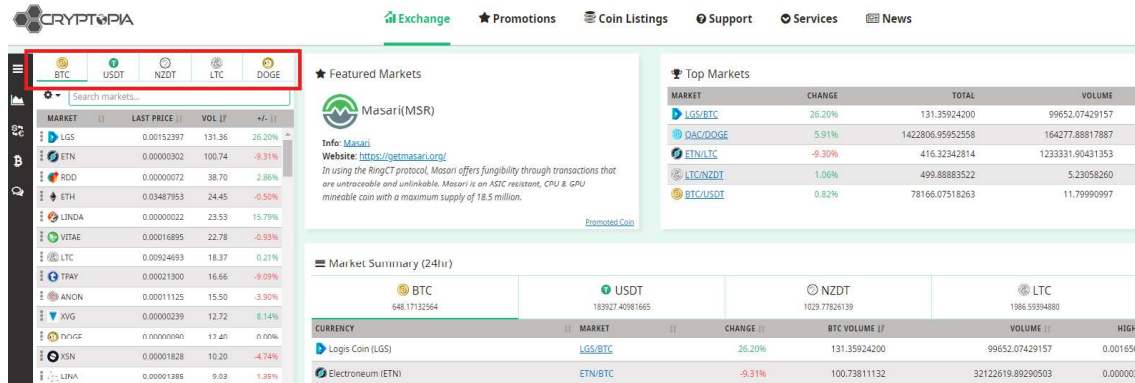
- **Search or filter** the coins available for trade using the 'search markets' field, e.g. type DOT into the Search field to search for Dotcoin. In this example we will be selling DOT in exchange for BTC.

- **Click on the DOT** line and the market for this coin will be displayed, showing historical data.

- Input the amount of the coin **you wish to sell** in the **'Sell DOT'** box (in the 'Amount' row) and how much you want to receive per coin you are selling (in the 'Price' row).

- The **'Sum'**, **'Fee'** and **'Total'** will then be automatically calculated.

PLEASE NOTE: The '**Total**' must be greater than the '**Minimum Trade**' amount.

- **Click** the '**Sell Dot**' button and wait for another trader to match with your order.

- **To cancel your order,** readjust your price, or simply make your coins available again, go to your **'Open Trades'** page, click on the order you wish to cancel and click 'Cancel'.

IMPORTANT INFORMATION REGARDING WALLET MAINTENANCE

- You can still buy or sell a coin when a wallet is in maintenance **but please be aware you will not be able to withdraw** until that coin wallet is out of maintenance.
- To check if a **wallet is in maintenance** please go to our **'Coin Info'** page. By clicking on a coin in this page, you can see the status update and available information about the reason for maintenance.

Cryptopia Limited: How user transfers worked:

Please note: Internal transfers like this were not recorded on the blockchain.

The '**Transfer**' function on the Cryptopia website is an **instant and fee-free** method to transfer coins from one Cryptopia account or user to another Cryptopia account or user.

PLEASE NOTE: A Transfer **DOES NOT** change one coin into another type and does not send coins to external wallets or other exchange accounts.

How do I make a transfer?

#1. **Log in** to your Cryptopia account.
#2. Hover over the **'B'** icon in the top right menu bar next to your username and click on **'Transfer'** from the drop down menu.
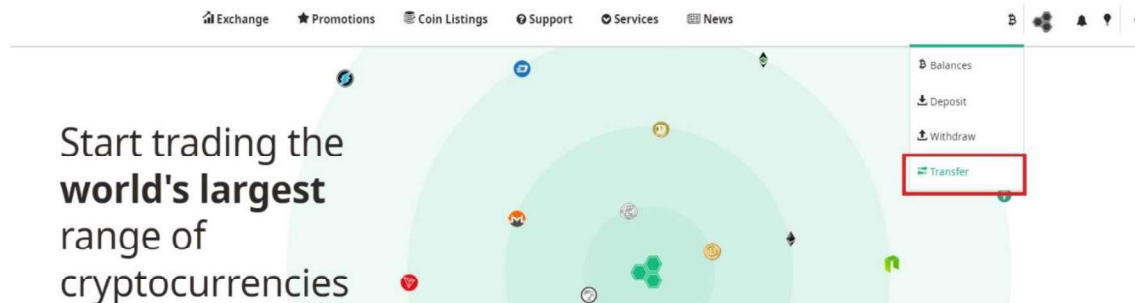
#3. **Select the currency** you would like to transfer to another Cryptopia account or user, e.g. DOT.

⇄ Transfer between Cryptopia users
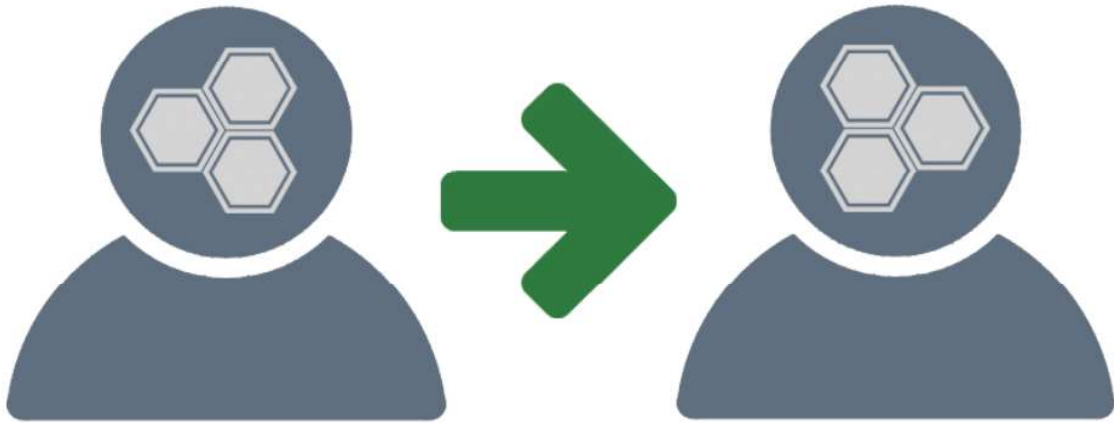
Select currency you would like to transfer to another user's *Cryptopia* account.

Dotcoin(DOT)

⚠ If you want to send crypto to an account at another site or wallet, use the ⬆ withdraw page
⚠ If you want to convert one currency to another, use the exchange to trade between currency pairs.

Next ❯

↺ View Transfer History

#4. Click the **'Next'** button.

⇄ Transfer between Cryptopia users
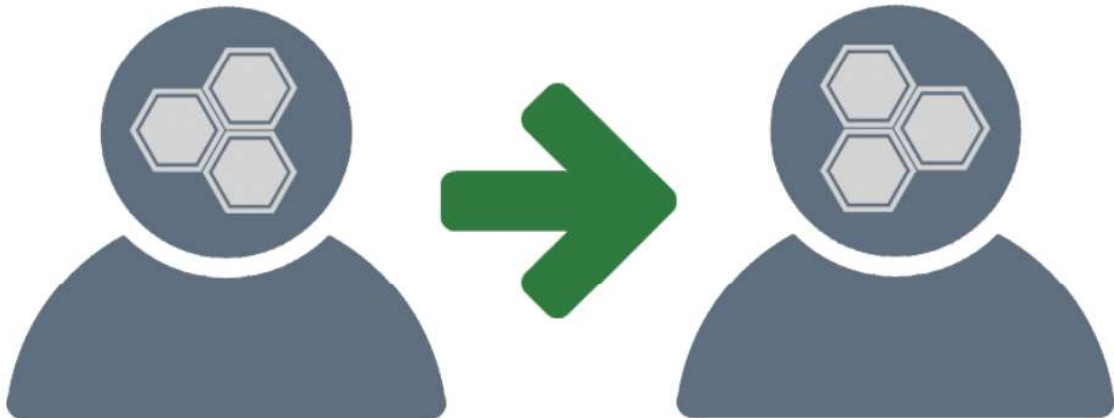
Select currency you would like to transfer to another user's *Cryptopia* account.

Dotcoin(DOT)

⚠ If you want to send crypto to an account at another site or wallet, use the ⬆ withdraw page
⚠ If you want to convert one currency to another, use the exchange to trade between currency pairs.

Next ❯

↺ View Transfer History

37

#5. In the **'Search'** box enter the exact Cryptopia username you want to transfer your coins to and click the **'Verify User'** button.

#6. Check that the verified Cryptopia username **is who you want to transfer to.**

#7. Type the amount you want to transfer in the **'Amount'** field. If you want to transfer your **entire balance**, click on your balance and this will fill the **'Amount'** field with your entire balance.

Transfer DOT to another user

You have used 47.02 of your 500,000.00 NZD daily limit.

SEARCH

✔User Verified

BALANCE
4990.00000000 DOT

AMOUNT
4000

Fee: 0.00000000 DOT
Net: 4000.00000000 DOT ($60.38 NZD)

PLEASE ENTER YOUR CRYPTOPIA AUTHENTICATOR CODE.

Cancel   Next ❯

↺View Transfer History

OR

Transfer DOT to another user

You have used 47.02 of your 500,000.00 NZD daily limit.

SEARCH

✔User Verified

BALANCE
4990.00000000 DOT

AMOUNT
4990.00000000

Fee: 0.00000000 DOT
Net: 4990.00000000 DOT ($75.32 NZD)

PLEASE ENTER YOUR CRYPTOPIA AUTHENTICATOR CODE.

Cancel   Next ❯

↺View Transfer History

#8. Click the **'Send Email Code'** button to sent a unique dynamic 2FA Email Code to your registered Two Factor email address. You will be presented with the following notification **'Email successfully sent to your registered two factor email address'.**

#9. You will receive the **'Transfer Two Factor Confirmation'** email with **unique dynamic 6 digit code.**

PLEASE NOTE: This email will allow you to double check that your account is secured from unauthorized access. *If you did not initiate* this transfer, *we recommend locking your account* and following our article on **'What do I do if I think my account has been compromised?'.**

#10. Enter your **unique dynamic 2FA Email Code** which has been sent to your registered email and click on the **'Next'** button to complete the instant transfer.

Transfer **DOT** to another user

You have used 0.00 of your 5000.00 NZD daily limit.

Email successfully sent to your registered two factor email address.

Search

✔User Verified

Balance
5000.00000000 DOT

Amount

5000.00000000

Fee: 0.00000000 DOT
Net: 5000.00000000 DOT ($148.78 NZD)

Please enter email code.

••••••

Send Email Code

Cancel

Next ❯

↻View Transfer History

#11. To view your previous transfers click on the **'View Transfer History'** button.
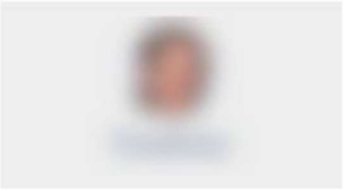
Transfer **DOT** to another user

You have used 0.00 of your 5000.00 NZD daily limit.

Email successfully sent to your registered two factor email address.

Search

✔User Verified

Balance
5000.00000000 DOT

Amount
5000.00000000

Fee: 0.00000000 DOT
Net: 5000.00000000 DOT ($148.78 NZD)

Please enter email code.

••••••   Send Email Code

Cancel   Next ❯

⟳View Transfer History

OR

#12. Go to your **'Transfer History'** through your account. Here you will be able to see who you have sent funds to using the 'Transfer' service and also who has transferred funds to your account.

Karma Points
👍 0

Account	👤
Settings	⚙
Security	🔒
Notifications	💾
Balances	฿
Open Trades	⇄
Karma	👍
Paytopia	⌨
Deposit History	⬇
Withdraw History	⬆
Trade History	↻
Transfer History	⇄
Referral History	🛒

Cryptopia Limited: How to make a withdrawal

Please note: While fees were charged, these were 'network fees' used to carry the transaction across the blockchain in a timely manner. While Cryptopia had set fees in place, sometimes the network fee used could be higher or lower than the fees Cryptopia charged. It's my understanding that any excess fees were held in a 'fees only' type pool and were not used for profit.

Handy youtube video that covers this process here:

https://www.youtube.com/watch?v=mNuqtEDYeig

Our guide for this was as follows:

How do I make a withdrawal?

Please follow the steps below to **withdraw** your cryptocurrency coins. In this example, we will be using BTC for illustration purposes, however the steps for withdrawing are the same for most coins.

#1. **Log in** to your Cryptopia account.
#2. Hover over the **'B'** icon in the top right menu bar next to your username and click on **'Withdraw'** from the drop down menu.
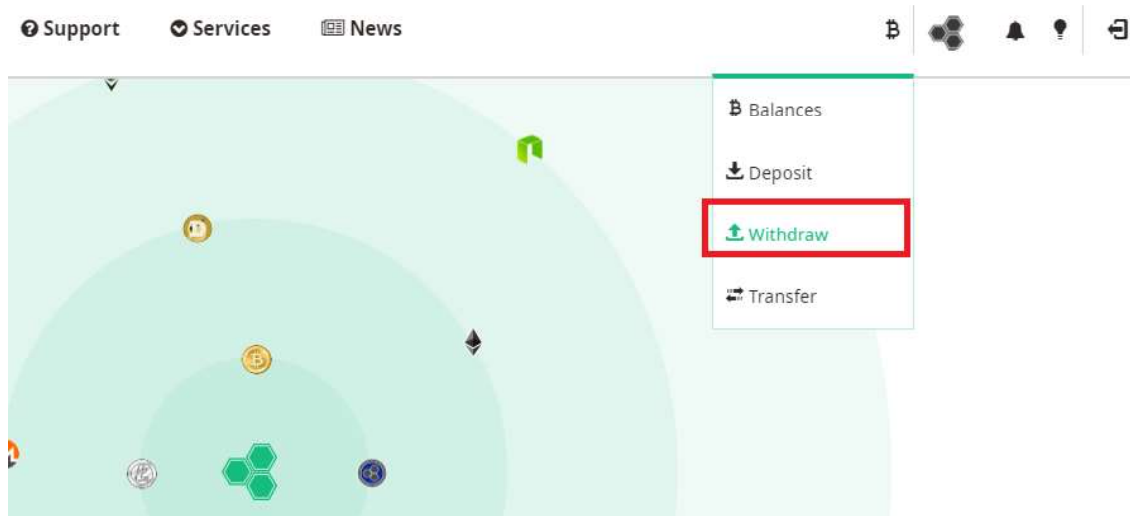
#3. **Select the cryptocurrency** you would like to withdraw from your Cryptopia account from the drop down menu by typing either the ticker or currency name, e.g. BTC.

#4. Click on the **'Next'** button.

#5. The DOT withdrawal window will now appear. **Enter the amount you want to send** in the **'Amount'** field, OR click on the blue hyperlinked numbers of your balance to select your **entire BTC** balance to withdraw.

Bitcoin(BTC)
Please select the address and amount below to withdraw.

You have used $47.02 of your $500,000.00 NZD daily limit.

BALANCE
0.02122685 BTC

AMOUNT
0.00565000

Fee: 0.00050000 BTC
Net: 0.00515000 BTC ($58.20 NZD)

ADDRESS BOOK
Please Select ▾

BITCOIN ADDRESS

PLEASE ENTER THE CODE FROM YOUR EMAIL.

Send Email Code

Cancel | Next

View Withdraw History

OR

Bitcoin(BTC)
Please select the address and amount below to withdraw.

You have used $47.02 of your $500,000.00 NZD daily limit.

BALANCE
0.02122685 BTC

AMOUNT
0.02122685

Fee: 0.00050000 BTC
Net: 0.02072685 BTC ($218.64 NZD)

ADDRESS BOOK
Please Select ▾

BITCOIN ADDRESS

PLEASE ENTER THE CODE FROM YOUR EMAIL.

Send Email Code

Cancel | Next

View Withdraw History

#6. Enter the wallet address you want to send the coins to in the field **'Bitcoin Address'** double checking there are no white leading or trailing spaces, or alternatively select an address from your 'Address Book'.

#7. Click the **'Send Email Code'** button to send the unique and dynamic 6 digit Email Two Factor Authentication Code to your registered 2 Factor Authentication (2FA) email address.

#8. The unique dynamic 6 digit Two Factor Authentication (2FA) Email Code will now be sent to your registered Two Factor email address. Please use this email code to process your withdrawal.

PLEASE NOTE: This email will expire after 24 hours.

PLEASE NOTE: This email will allow you to double check the amount you are withdrawing and the address you are withdrawing to. ***If you did not initiate*** this withdrawal, we recommend locking your account and following our article on **'What do I do if I think my account has been compromised?'.**

#9. Enter the received **'Email Code'** and click on the **'Next'** button.

Bitcoin(BTC)
Please select the address and amount below to withdraw.

You have used $47.02 of your $500,000.00 NZD daily limit.

BALANCE
0.02122685 BTC

AMOUNT
| 0.02122685 |

Fee: 0.00050000 BTC
Net: 0.02072685 BTC ($223.45 NZD)

ADDRESS BOOK
Please Select ▼

BITCOIN ADDRESS

PLEASE ENTER THE CODE FROM YOUR EMAIL.

Send Email Code

Cancel   Next

View Withdraw History

#10. The **'Withdrawal Submitted'** window will now appear. Click **'Done'**.

Withdrawal Submitted

A confirmation email has been sent to
Please click the secure link in the email to authorise this withdrawal.

Address:	
Amount:	0.00456450 BTC
Fee:	0.00050000 BTC
Net Amount:	0.00406450 BTC

Done

View Withdraw History

#11. An email will now be sent to your registered email address. You need to click the '**Confirm Withdrawal**' button in the email to finalise the withdrawal. Your withdrawal will remain as 'unconfirmed' until you click either '**Confirm Withdraw**' or '**Cancel Withdraw**' in your email.

PLEASE NOTE: This email will expire after 24 hours.

PLEASE NOTE: This email will allow you to double check the amount you are withdrawing and the address you are withdrawing to. *If you did not initiate* this withdrawal, we recommend locking your account and following our article on **'What do I do if I think my account has been compromised?'**.

Troubleshooting Withdrawal Issues

- **I am unable to enter a Wallet Address.**
If the **'Address'** field is greyed out and you cannot enter any text, it may be that you have 'Address book withdraw only' ticked on the 'Security' page of your account. See our article **'Why can't I enter a withdraw address?'** for instructions on how to change this setting.
- **I am receiving a 'Invalid Address Error' notification.**

There are two common reasons for this:

#1. You have entered the wallet address **for a different cryptocurrency coin type**. Please double check the address you have entered is correct.

#2. The destination address wallet is running on **a different version than our wallet.** If this is the case, please check the Cryptopia version from our **'Coin Info'** page and, either:

- Contact the support team of the recipient wallet; or
- Update your personal wallet to the latest version. You can do this by heading to that cryptocurrency coin's official website (link found in our CoinInfo page under **'Links'**) and follow the directions on how to download and update to the latest wallet version.

Coin Information

Search: _____

NAME	RATING	ALGO	NETWORK	CONNECTIONS	BLOCK HEIGHT	WALLET STATUS	LISTING STATUS	VERSION
DigiByte (DGB)	★★★☆☆	Scrypt	POW	Connections: 8	7420902	OK	Active	6160500
Emerald Crypto (EMD)	★★★☆☆	Scrypt	POW	Connections: 14	7356119	OK	Active	V0.8.7.7-beta
Lisk (LSK)	★★★☆☆	Other	DPOS	Connections: 10	7198618	OK	Active	
Ethereum Classic (ETC)	★★★☆☆	Dagger	POW	Connections: 8	6669548	OK	Active	Geth/v5.5.0
Corion (COR)	★★★☆☆	None	Asset	Connections: 8	6669547	OK	Active	Geth/v3.1.1 - COR
Ethereum (ETH)	★☆☆☆☆	Ethash	POW	Connections: 6	6442346	OK	Active	Geth/v1.7.3
Unibright Token (UBT)	★★★★★	None	Asset	Connections: 4	6442328	OK	Active	Geth/v1.7.2 - UBT
EZToken (EZT)	★★★★★	None	Asset	Connections: 4	6442328	OK	Active	Geth/v1.7.2 - EZT
Amon (AMN)	★★★★★	None	Asset	Connections: 3	6442328	OK	Active	Geth/v1.7.2 - AMN
TrueUSD (TUSD)	★★★★☆	None	Asset	Connections: 3	6442328	OK	Active	Geth/v1.7.2 - TUSD
Shivers (SHVR)	★★★★☆	None	Asset	Connections: 3	6442328	OK	Active	Geth/v1.7.2 - SHVR
Live Stars Token (LIVE)	★★★★☆	None	Asset	Connections: 3	6442328	OK	Active	Geth/v1.7.2 - LIVE
IVY (IVY)	★★★★☆	None	Asset	Connections: 3	6442328	OK	Active	Geth/v1.7.2 - IVY
GazeCoin (G7F)	★★★★☆	None	POS	Connections: 3	6442328	OK	Active	Geth/v1.7.2 - G7F
Fabric Token (FT)	★★★★★	None	Asset	Connections: 3	6442328	OK	Active	Geth/v1.7.2 - FT
Everus (EVR)	★★★★★	None	Asset	Connections: 4	6442328	OK	Active	Geth/v1.7.2 - EVR
BCShop.io Token (BCS)	★★★★☆	None	Asset	Connections: 3	6442328	OK	Active	Geth/v1.7.2 - BCS
Vice Industry Token (VIT)	★★★☆☆	None	Asset	Connections: 3	6442328	OK	Active	Geth/v1.7.2 - VIT
Soniq (SONIQ)	★★★☆☆	None	Asset	Connections: 3	6442328	OK	Active	Geth/v1.7.2 - SONIQ

- **I am receiving a 'Additional Payment ID' or 'Message' request.**
Some coins require **an additional Payment ID** (e.g. CryptoNight coins) or **Message** (e.g XEM, BIS) as well as your withdrawal address in order to be debited from your Cryptopia account and credited to a non-Cryptopia account. If an extra field is required for a particular coin, it will be shown on your **'Withdraw'** page for that coin, along with your withdrawal address. If you are withdrawing to a personal wallet, simply enter anything as your payment ID.

Read more about what a Payment ID is on our Glossary page **here**.

Electroneum(ETN)
Please select the address and amount below to withdraw.

You have used $47.02 of your $500,000.00 NZD daily limit.

BALANCE
0.00000000 ETN

AMOUNT
200.00

Fee: 5.00 ETN
Net: 195.00 ETN ($6.37 NZD)

Note: ETN supports 2 decimal places.

ADDRESS BOOK
You have no address book entries for Electroneum ▼

ELECTRONEUM ADDRESS
_____

PAYMENTID
_____

PLEASE ENTER THE CODE FROM YOUR EMAIL.
_____ Send Email Code

| Cancel | Next |

View Withdraw History

- **My balance says 0.**

You can check where your balance may be being held in **'Deposit History'** or **'Open Trades'** function of your Cryptopia account.

- **My withdrawal says unconfirmed/my email token has expired.**
  You can resend this email in your **'Withdraw History'**. Alternatively you can cancel it here too.

Cryptopia Limited: How cashing in / out used to work:

Please note: This was a completely free of charge service, Cryptopia did not charge any fees for doing this. **This was also all completely manually processed by humans.**

1.) Customer needed to deposit money into the Cryptopia bank account that was designated for NZDT purchase. Any customer doing this needed to be at the very least, level 2 KYC verified. We would never take anonymous deposits. NZDT was a coin that was made specifically for the purpose of cashing in and out, giving kiwis an easy way to get into Crypto. Customers would deposit money into the specific bank account, with a specific reference number unique to their Cryptopia account, and then their Cryptopia account would be sent the equivalent amount of NZDT. NZDT was always pegged at the value of the NZ dollar, so its value would never fluctuate.

2.) Once the NZDT was deposited to the customers account, they could then trade this on the exchange like a normal coin (see the 'Buying and Selling coins' doc). Cryptopia would take 0.2% of the trade made as trade fees (to clarify, this fee was for any trade made, not just NZDT – this was the source of Cryptopia's income).

3.) When the customer was ready to 'cash out', they would sell what crypto they had for NZDT, and then withdraw the NZDT to the bank account number which was to be credited with the equivalent in $NZD. When the withdrawal was made, we allowed up to 48 hours processing time to then deposit the equivalent amount of New Zealand dollars from the Cryptopia bank account, to the customers bank account that they designated. This was manually handled by a human, twice daily (it's not actually possible to withdraw crypto directly to a bank account).

4.) These were ALL manually processed – we were working on an API to work with ASB however that was still in development when ASB withdrew their support.

In regards to customers using other services Post-ASB, we had a small section on our Knowledgebase about this:

#2. How do I deposit my local currency into my Cryptopia account (I do not live in NZ)?

If you do not have a New Zealand bank account, the only way to make a deposit using your local currency is by using a cryptocurrency exchange service servicing your domestic country. You should do your research carefully, there are many options available and not all exchange services allow fiat conversion. Choose the right exchange that best meets your requirements and expectations.

PLEASE NOTE: Cryptopia has no affiliation with any third party cryptocurrency exchange service.

Examples of cryptocurrency exchange services include:
- **https://www.coinbase.com/**
- **https://localbitcoins.com/**

Cryptopia Customer Service Analyst Manual

Version 1.0

Catherine Teo
CRYPTOPIA

Contents

58

Welcome to Cryptopia Customer Service Team!

Introduction

Who are we?

Cryptopia aims to be more than just another exchange, our focus is on the user experience of the crypocurrencies themselves. In order to make cryptocurrencies more accessible to everyone we provide an auction house and marketplace, several stable nodes on the network, and a support framework for each coin accepted on the site. Each coin accepted on Cryptopia has an established user base and community, as well as proven goods and services that the coin can be exchanged for to provide a consistent experience for the user and avoid hopping around between phad coins and pump and dump coins that won't stand the test of time. Every service provided by Cryptopia is fully integrated, you can mine directly to the exchange, or buy something from the marketplace or auction house with your trade earnings; all funds will be fully integrated and immediately accessible via all current and future Cryptopia services.

History of Cryptopia

- ✓ Been around for 4-5 years
- ✓ Launched as an exchange in 2014
- ✓ Adam Clark and Rob Dawson are our founders.
- ✓ What started out as a hobby, quickly turned into a full time job.
- ✓ 5 months ago, we had ~12 staff (including ones that were contracted), now we are sitting at 75 full time staff.

Intranel relationship:

- Adam used to work at Intranel. When he decided to start Cryptopia, he was told to stay in the building and use the facilities while he was trying to get it off the ground.
- Andy, Dave and Adam (who are the founders of Intranel) also help out full time in Cryptopia.
- Most of Intranel Devs work full time for Cryptopia.

Cryptopia in the Crypto space:

60

- ✓ As an exchange, we are different from most other exchanges as our volumes are generated from crypto to crypto trades. While most other exchanges deal with fiat to crypto exchange.
- ✓ Majority of our listed coins are alt coins.
- ✓ We are globally recognised for listing many alt coins.

Our base markets?

BTC, USDT, NZDT, LTC, DOGE.

https://www.cryptopia.co.nz/Exchange

61

How do I set up an account with Cryptopia?

BELOW ARE STEP BY STEP INSTRUCTIONS TO HELP YOU SET UP AN ACCOUNT WITH CRYPTOPIA.

#1. Click on the '**Register'** button at the top right hand corner.

#2. Create a **Username** for your account and nominate an **Email Address**.

Please take the following into consideration when selecting your Email Address:

- Use a **permanent email address** to which you have a reliable access
- Make sure it is **not connected** to any other Cryptopia account; and
- is **unique** to Cryptopia and **not used** on any other cryptocurrency service, exchange or site. This email address will be used for account verification and registration completion, its secure integrity is important.
- Make sure that your email account as well as information and credentials associated with it, **have not been compromised.** We recommend using available online tools (e.g. **https://haveibeenpwned.com/**) and regularly checking it.

#3. Create a '**Password'** for your account.

Make sure you use a unique password which you do not use for anything else. Cryptopia has strict minimum password requirements for the security of user accounts and these are case sensitive.

PLEASE NOTE: For your password to meet Cryptopia minimum password requirements it must be a minimum of 8 characters long, and include at least one of each of the following:
- 1 Uppercase letter;
- 1 Lowercase letter;
- 1 Special character; and
- 1 number.

Password

****

✖Uppercase ✖Lowercase ✖Number ✖!@#$%^& ✖8 characters

Confirm password

****

#4. Create your own **unique 4-8 digit, Two Factor Authentication (2FA) PinCode**.

PLEASE NOTE: make sure you remember this number as you will need it for login and other user account activities. Once set, this PinCode may be changed on the Security page of your account.

5

62

#5. Click the **'I agree to terms and conditions'** box and **'I'm not a robot'** box and finally the **'Register' button**.

#6. After you complete registration, a **confirmation email** will be sent to your nominated **Email Address**.

#7. Open the email and click on the '**Verify My Email Address'** link in the email. image_censored.jpg 59.09 KB

PLEASE NOTE: This link expires after several hours, so please check for the email and make sure you successfully activate your account soon after registering. These can sometimes go to 'junk', 'spam' or 'promotional' folders so ensure you check all folders.

#8. Your Email Address will now be verified and you will be prompted to log in using firstly your **Email Address**, secondly your case sensitive **Password** and finally your **4-8 digit 2FA PinCode**.
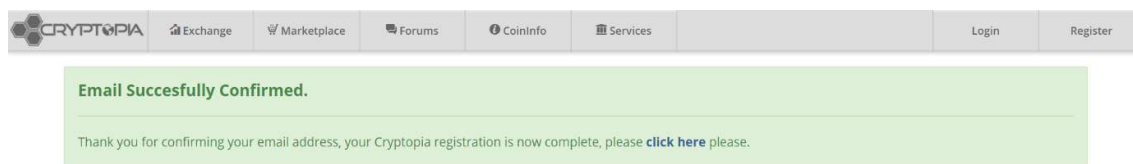
#9. Your account **is now set up** and you are ready to begin trading!

What do I do if I am experiencing registration issues?

- If you can't find the registration email, **it may be filtered into a different alternative folder** within your inbox (i.e. junk, spam or promotional). These folders often do not sync with mobile apps or email clients. We suggest that you log onto your webmail if possible and perform a thorough search.
- We are aware that some ISP email providers and customized domains, reject or defer some of our automated emails. This may either cause **delay**, or you **may not receive** them at all. If you have not received a Cryptopia email you are expecting, you should try and whitelist this email – **noreply@cryptopia.co.nz** with your provider, in addition to contacting Cryptopia Support describing the issue so we can check and confirm if we can assist.
- If the link is not clickable, this is likely due to a compatibility issue with the browser or email client you're using. If possible, try using a different browser or client to view the email, and if you still cannot get it to work, please contact Cryptopia Support and we can manually activate your account.
- If after clicking the link, you get a message on Cryptopia saying "You are not authorized to view this area", this indicates **the link has expired**. If this occurs, please contact Cryptopia Support, and we can manually activate your account.

Do I need to be verified?

Following successful registration of your Cryptopia account, you automatically achieve **LEVEL 1 VERIFICATION**. This happens when you click on the activation email we send to you and you log into your account. For further information about setting up a Cryptopia account, see **'How do I set up an account with Cryptopia'**.

LEVEL 1 VERIFICATION gives you access to all functions and features on Cryptopia.

The only restriction placed on **LEVEL 1 VERIFICATION** is the limit and type of withdrawals and transfers between Cryptopia accounts. This is currently **cryptocurrency only** with the equivalent value of $5000 NZD every 24 hour*.

*PLEASE NOTE: a '24 hour period' means 24 hours from your first withdrawal or transfer, for example, if you make a withdrawal at 4pm on the 8th of Jan, your 24 hour period for that amount runs until 3.59 pm 9th of Jan. The next 24 hour period will commence with your next withdrawal or transfer.

Please go to **'How do I increase my verification level?'** for step by step instructions on how to increase your verification level if necessary.

How do I increase my Verification level?

How do I increase my Verification Level to LEVEL 2?

If you're willing to increase the Level 1 Verification daily limit imposed on withdrawals and transfers between Cryptopia accounts, you need to apply for Level 2 Verification.

LEVEL 2 VERIFICATION LIMIT is currently the equivalent of $50,000 NZD per 24 hours*.

*PLEASE NOTE: a '24 hour period' means 24 hours from your first withdrawal or transfer. For example, if you make a withdrawal at 4pm on the 8th of Jan, your 24 hour period runs until 3.59 pm 9th of Jan. The next 24 hour period will commence with your next withdrawal or transfer.

Applications for Level 2 Verification must be made via our website and be compliant with International Anti-Money Laundering Law (AML) provisions. You must be over 18 years of age at the time of application and ensure you hold necessary identification documentation.

TO APPLY FOR AN INCREASED VERIFICATION LEVEL, PLEASE FOLLOW THE STEPS OUTLINED BELOW:

#1. Log into your Cryptopia account

#2. Go to 'Balances'

#3. Click on the 'Daily Limit' link above the balances of all your coins.

			You have used 0.02 of your 50000.00 NZD daily limit.		
Actions	Currency	Available	Total	Open Orders	Est. BTC	Favorite
⬇ ⬆ — 🏠	Bitcoin(BTC)	0.05654040	0.05654040	0.00000000	0.05654040	⭐

![Cryptopia logo]

#4. Submit Verification for Level2.

User Verification

Verification Level1

Users verified by email have a daily withdrawal limit of $5000.00 NZD

Email
[_____]

Verification Level2
Incomplete

Users that have provided evidence of their identification have daily limit of $50000.00 NZD

FirstName   LastName
[_____]   [_____]

Birthday   Gender
[_____]   [Unknown   ▼]

Country   City
[Afghanistan   ▼]   [_____]

State   Postcode
[_____]   [_____]

Address
[_____]

Photo of Identification   Photo holding identification
[Choose File] No file chosen   [Choose File] No file chosen
                Example   Example

ID CARD
name
for Cryptopia purposes only

☐ I accept to the Terms and Conditions   [Submit]

Verification Level3
Incomplete

Users who need a greater daily withdrawal limit will need to contact the Cryptopia Support team to request Verification Level3, this level of account is required for:

- Personal Accounts with Verification Level 2 requiring a higher daily limit
- Businesses and Corporations

PLEASE NOTE: You will see that your account is already **LEVEL 1 VERIFIED**

#5. Complete **all details** in the form including:
- **First name** (same characters as ID, ex. 李四 is shown on ID, 李四 must also be entered in the registration form; Li Si is not sufficient);
- **Last Name** (same character as ID);
- **Birthday** (DD/MM/YYYY format);
- **Gender**
- **Country**
- **City**
- **State**
- **Postcode**
- **Address** (PO Box or non-specific address is not acceptable).

#6. Upload your **Identification Documentation**. AML Law requires either a Government issued **current** Passport, or Drivers License, or Government issued Identity Card.

PLEASE NOTE: Documentation **must** display your photo, full name and date of birth - if this information is located on the back and front of your Identity Card or Drivers

License we advise you to upload the documentation so that all information is displayed clearly in the **one** image.

PLEASE NOTE: The file size limit for uploads is 4MB. We will not accept any identification that has expired. Please ensure the image is clear and features such as the Identification Documentation text are identifiable.

#7. Upload a clear photo of you holding your uploaded Identification Documentation.

PLEASE NOTE: Please make sure your camera is clean and you are entirely visible in the photo. We cannot accept photos where we cannot see your face. You must hold your identification open to ensure the **photo**, **full name** and **date of birth** are visible.

The file **size limit** for uploads is 4MB. Please ensure the image is clear and features such as the Identification Documentation text are identifiable. Your photos must not be edited in anyway.

#8. Tick the **'I accept the Terms and Conditions'** box.
#9. Click on **'Submit'**.

PLEASE NOTE: Applicant must be at least 18 years of age at the time of application.

What happens now?

Once we have received your Application for Level 2 Verification, our team will review your application. If the application is approved, you will be notified via **email**.

If your application is rejected, you will be notified by email with a reason for the rejection. You will need to address the issue outlined in the email (for example, identification documentation, quality of photo etc) and resubmit your application by following the same process as the above.

How do I increase my Verification level to LEVEL 3?

Cryptopia users who require a $500,000+ NZD daily withdrawal limit will need to contact the Cryptopia Support team to request Verification Level 3 on their account.

Please ensure the subject of your ticket is LEVEL 3 VERIFICATION REQUEST as this will allow for the ticket to be addressed by the right support team member.

Create Support Ticket ✕

Subject
LEVEL 3 VERIFICATION REQUEST

Category
General! ▼

Description

Cancel   Submit

PLEASE NOTE: LEVEL 3 VERIFICATION LIMIT is currently the equivalent of $500,000 NZD per 24 hour period

What is ReCaptcha and why isn't it working?

reCAPTCHA is a free service from Google that helps protect websites from spam and abuse. A "CAPTCHA" is a turing test to tell human and bots apart. It is easy for humans to solve, but hard for "bots" and other malicious software to figure out.
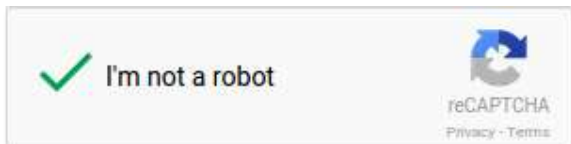
Why is reCAPTCHA not working on my computer?

There may be some instances where certain browsers do not display reCAPTCHA properly. For further information and troubleshooting, please refer to **Google's ReCaptcha support page**.

Why am I not receiving emails from Cryptopia (including verification)

There are a number of reasons why you may not be receiving, or cannot find, automated Cryptopia emails that you might be expecting.

Use these troubleshooting tips to help:

#1. **Is your account activated?**

68

Following registration you will be sent a 'Registration Confirmation' email sent to your nominated Email Address. In order to complete your registration, you will have to click on the account verification link. You will not receive any further emails including password resets, until your account is activated.

#2. **Are you checking the right email inbox?**

Check that you did not register with an alternative email address and have checked the right inbox.

#3. **Have you checked the junk, spam or promotional folders in your inbox?**

It is possible that emails from Cryptopia get filtered into a different folder within your inbox, this may cause issues with synchronization between mobile apps or email cleints. You should log into your email via a web browser if possible, and perform a thorough search for it.

PLEASE NOTE: There are sometimes issues with automated emails sent to email accounts provided by some internet service providers (ISP's). In these cases, our automated emails are often delayed, but should eventually be received in your mailbox.

A small number of ISP providers may completely reject our automated emails as spam. If you are having a consistent issue receiving Cryptopia's automated emails, you should investigate whether you can whitelist our **cryptopia.co.nz** domain from your email account, or request your provider to remove the block on **cryptopia.co.nz**.

If your email provider is not able to help by whitelisting our domain, we recommend using an alternative email service provider and setting up a new account. You can change your email by raising a support ticket and letting our Support team know what email you would like to change to.

Are there any account limits for trading, deposits or withdrawals?

There are currently **no account limits** for trading or deposits to Cryptopia. Limits for withdrawals and transfers between Cryptopia accounts depend on your verification level.

PLEASE NOTE: Due to Anti Money Laundering (AML) regulations, accounts must have a **Level 2 Verification Level** for us to accept deposits or withdrawals of fiat New Zealand Dollars (NZD).

Level 1 Verification – Withdrawal and Transfer Limit

Level 1 verification is achieved during the registration process once you click the link on the Registration Confirmation email sent to your registered email address. Every Cryptopia account has access to all functions and features on Cryptopia once the account is activated at Level 1.

Level 1 verified accounts have **a withdrawal and transfer limit of $5,000 NZD** equivalent of value per 24 hour period*.

Level 2 Verification – Withdrawal and Transfer Limit

You can increase the withdrawal and transfer limit on your account by upgrading it to Level 2 verification. See our article on increasing account verification to Level 2 or 3 **'How do I increase my verification level?'** .

Level 2 verified accounts have **a withdrawal and transfer limit of $50,000 NZD** equivalent of value per 24 hour period*.

Level 3 Verification - Withdrawal and Transfer Limit

You can request a further increase on the withdrawal and transfer limit on your account by upgrading it to Level 3 verification. See our article on increasing account verification to Level 2 or 3 **'How do I increase my verification level?'**.

Level 3 verified accounts have **a withdrawal and transfer limit of $500,000 NZD** equivalent of value per 24 hour period*.

PLEASE NOTE: *A '24 hour period' means 24 hours from your first withdrawal or transfer. *For example, if you make a withdrawal at 4pm on the 8th of Jan, your 24 hour period runs until 3.59pm 9th of Jan for that amount. The next 24 hour period will commence with your next withdrawal or transfer.*

Are there any specific requirements for ID documents?

The only time you need to provide ID documentation is if you choose to apply for **Level Two Verification**. You will be required to upload identification documentation when you apply. See articles **Do I need to be Verified?** and **How do I increase my verification level?** for more information.

Cryptopia's ID requirements are outlined below:

#1. **Upload a photo** of your identification document.

#2. **Law requires** your identification document to be either **a government issued current** passport, Drivers License or Identity Card.

#3. This document must display a **clear picture of you**, and include your **full name** and **date of birth** (If this information is found on two sides of your ID, please upload both sides into one document).

#4. The **file size limit** for uploads is 4MB.

#5. We **will not accept** any identification that has **expired.**

#6. **Upload** a photo of you holding your identification documentation.

#7. Please make sure your **camera lens is clean** and your face is **entirely visible** in the photo.

#8. We cannot accept photos where we cannot see your face. You must hold your identification open to ensure your **photo**, **full name** and **date of birth** are visible.

#9. Please note that **we cannot accept edited photos**.

PLEASE NOTE: We cross check your submitted information with your uploaded ID. This means whatever characters your full name is on your ID, this needs to be the same characters that you submit in the form.

What is ReCaptcha and why isn't it working?

reCAPTCHA is a free service from Google that helps protect websites from spam and abuse. A "CAPTCHA" is a turing test to tell human and bots apart. It is easy for humans to solve, but hard for "bots" and other malicious software to figure out.
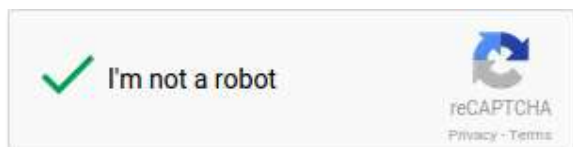
Why is reCAPTCHA not working on my computer?

There may be some instances where certain browsers do not display reCAPTCHA properly. For further information and troubleshooting, please refer to **Google's ReCaptcha support page**.

What fees does Cryptopia charge and how do I see them?

Cryptopia charges **fees** on Trades and Withdrawals are on our Exchange.

Trading Fees

- Cryptopia charges a **0.2% fee for every trade** on our Exchange.

- The fee is automatically calculated and displayed in the **'Fee'** field after you have entered an 'Amount' and 'Price'.

Amount	13017.44337412	DOT
Price	0.00000276	BTC
Sum	0.03592814	BTC
Fee	0.00007186	BTC
Total	0.03600000	BTC

Buy DOT

Minimum trade: 0.00050000 BTC

- The 'Total' field **includes the fee** which is shown before you confirm the order.

Amount	13017.44337412	DOT
Price	0.00000276	BTC
Sum	0.03592814	BTC
Fee	0.00007186	BTC
Total	0.03600000	BTC
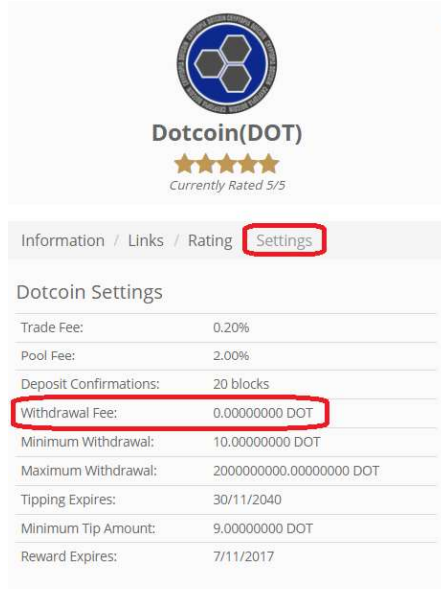
Buy DOT

Minimum trade: 0.00050000 BTC

PLEASE NOTE: Further information on how to trade on Cryptopia can be found in our article **'How do I trade? (for beginners)'**

Withdrawal Fees

- Each cryptocurrency coin listed on Cryptopia has **different fee** for Withdrawals.
- These fees **are static** amounts for each transaction, not percentages of the value of your withdrawal, e.g. you will pay the same withdrawal fee whether you're withdrawing .01 BTC or 1 BTC in a single transaction.
- You can view our Withdrawal Fees on the **Coininfo page**, under **'Settings'** for each cryptocurrency coin.

- Withdrawal fees are based on the **individual Blockchain transaction** cost for that coin. This blockchain transaction cost goes towards paying the miners undertaking confirmations and network running costs.
- Cryptopia reviews the 'Withdrawal Fees' on coins periodically, after assessing the average cost of a single transaction on the Blockchain and considering transaction speed optimisation.

PLEASE NOTE: For detailed information on how to withdraw your coins please see our article **How do I make a withdrawal?**' article. For further information on Blockchain Confirmations, please refer to our article **What are Blockchain Confirmations**?

How do I reset my password?

There are two options if you wish to reset the Password on your account. Below is a step by step guide.

For your account safety we confirm that Cryptopia staff can never view a user's Password so please do not ask us or tell us what your Password is.
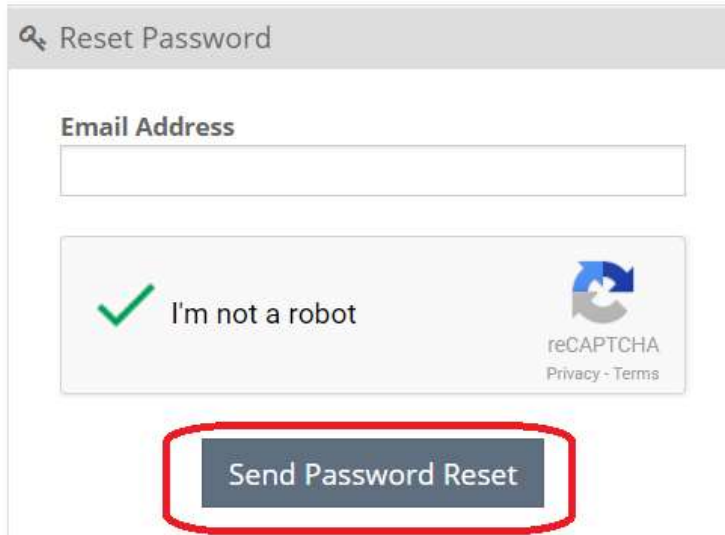
Cryptopia has strict Minimum Password Requirements for the security of user accounts and these are case sensitive.

PLEASE NOTE: For your Password to meet Cryptopia Minimum Password Requirements it must be a minimum of 8 characters long, and include at least one of each of the following:

- 1 Uppercase letter;
- 1 Lowercase letter;
- 1 Special character; and
- 1 number.

OPTION 1 - CAN'T LOG IN

CRYPTOPIA

#1. Go to https://www.cryptopia.co.nz/Login/

#2. Click on the '**Forgot your Password**' at the bottom of the sccreen.

#3. Enter YOUR Email Address and tick the '**I am not a robot**' box.

#4. Click '**Send Password Reset**' button.

CRYPTOPIA

#5. You will be sent an email with a link to reset your Password.

CRYPTOPIA   Password Reset

Hi ▮▮▮▮▮▮▮▮▮▮▮,

A password reset was requested from the IP Address: ▮▮▮▮▮▮▮

Reset My Password

Lock My Account   **Cryptopia Support**

#6. Click on the 'Reset My Password' button in that email.

#7. Enter YOUR Email address and YOUR new Password when prompted. You will be asked to confirm that new Password. Please note our Minimum Password Requirements detailed above.

#8. Press **'Click Here'** and you will be redirected to login using your new Password.

#9. Your Password is reset!

PLEASE NOTE: The **'Reset My Password'** link in the email expires within 15 minutes so please click on the link in the email as soon as you receive it.

OPTION 2 - ALREADY LOGGED IN

You can also reset your Password from your Account Security page if you are already logged in. Below is a step by step guide.

#1. Go to **'Security'** page.

#2. Under **Account Security**, go to **Change Password**.

#3. Enter your current Password.

#4. Enter your new Password, noting our Minimum Password Requirements detailed above.

#5. Confirm your new Password.

#6. Click on 'Change Password' button.

#7. Your Password is now changed!

#8. You will be logged out, and you will need this Password to log back in.

<u>What is a cryptocurrency wallet?</u>

A Cryptocurrency Wallet is software or service used for representing cryptocurrency transactions and securing ownership of them.

Each Wallet is associated with a **Public Key,** which is used as an address for managing and assigning cryptocurrency transactions sent over a blockchain. This Public Key is commonly the address you will specify whenever you send a cryptocurrency transaction from one place to another.

Each Wallet also securely stores a **Private Key,** which is a key that secures ownership of the cryptocurrency balance associated with the Public Key address.

There are various types of cryptocurrency wallets which are used and managed in different ways. Exchange services like Cryptopia manage and maintain Wallets, and provide you with the functionality to send and receive transactions as well as securely hold the balances assigned to your account.

We manage and maintain a Wallet for each cryptocurrency coin, and using this Wallet allow users to generate an address which is associated to each respective account on our database. You can only generate one address per coin and this address will never change.

Types of Cryptocurrency Wallets

Each cryptocurrency coin requires it's own specific Wallet as each operates on its own specific blockchain. To view the software available to set up your own Personal Wallet for a specific cryptocurrency coin, head to the **CoinInfo** page and **select** the 'Links' heading. The first link will be the website for that coin and there you will find the types of wallets that are on offer for different platforms. Outlined below are the common types of Wallets.

#1. Personal Wallets

Personal Wallets are recommended for your **own storage of cryptocurrency coins**, as this gives you complete control over the wallet and the Public and Private keys associated with it.

#2. Online web based Wallets

Online wallets are typically hosted online and accessed from a web browser. These are generally simple to access and use, but may be limited in functionality.

Due to being hosted and managed by a third party, and always being online, they are not necessarily as secure as other wallet types and may be targets for exploiting your cryptocurrency coins.

#3. Desktop Wallets

Desktop Wallets are accessed on a desktop/laptop computer and utilise its operating system, e.g. desktop computer using a Windows operating system.

They are generally **easy to use**, but require some setup and maintenance, and can be kept online or offline depending on your needs.

Desktop Wallets have the **benefit of storing your Private Key on a local platform,** instead of online as a Web Wallet. The security of your cryptocurrency is dependent on the security of the device running them, as well as your general online security practices.

#4. Mobile Wallets

Mobile wallets have some similarities to both Desktop and Web/Online wallets. They are designed to be run specifically from a mobile device, with easy access and convenience in mind.

PLEASE NOTE: phones and other devices often have their own security flaws, such as being easily stolen or accessed by unauthorised parties.

#5. Hardware Wallets

These are hardware dongles specifically designed for secure, long-term storage of a cryptocurrency, and are generally one of the most secure ways to keep your holdings safe.

#6. Paper Wallets

Paper Wallets are physical printouts containing the Public and Private keys associated with your cryptocurrency holdings. They require a little more effort and knowledge to manage, but can provide higher levels of security against online attacks as your Private Key is not stored or accessible anywhere online.

Is Cryptopia safe?

Cryptopia actively strives to ensure the **security**, **integrity** and **privacy** of personal information submitted to us, including regular review and compliance of our security measures in line with current technology. Unfortunately, no data transmission over the internet can be guaranteed to be totally secure.

We will take all reasonable steps to protect the personal information you may transmit to us or we collect from our online products and services. Once submitted, we take all reasonable steps to maintaining its security on our systems.

Additionally, our employees and contractors who provide services related to our information systems, are also obliged to maintain **confidentiality** and **security** of any personal information held by us.

We recommend users regularly review our **Terms & Conditions** and our **Privacy Policy** to ensure that you are familiar with these policies. We reserve the right to change these policies from time to time.

PLEASE NOTE: There are additional measures that you can take to ensure your personal details and accounts are kept safe such as **Two Factor Authentication** and being aware of the common scam tactics used in the industry, six of which are detailed below.

Common scam tactics

#1. Phishing websites

Phishing is a common technique for acquiring a user's personal or account data. Scammers set up fake websites that resemble reputable business sites in order to get you to enter your account or personal information.

The site may look very legitimate (and often look almost identical to official websites) but they will always have a slightly different domain name/URL. Before entering any of your personal details into the website, ensure you have reviewed the below:

What should I look out for?

Every time you log into your account, we recommend double checking that you are visiting the **correct URL,** which you can find below.

https://www.cryptopia.co.nz

PLEASE NOTE: Be aware of URLs that end in **.com, .ws, .cx**

- Check that the URL address starts with **https://**

- Check the **Site Certificate** to see whether a website is safe to visit. If you are using Google Chrome, you can check the security status to the left of the web address (a green lock is an indicator that the website is secure). If you are using a different browser, please look how to view the Site Certificate in the settings of your browser.
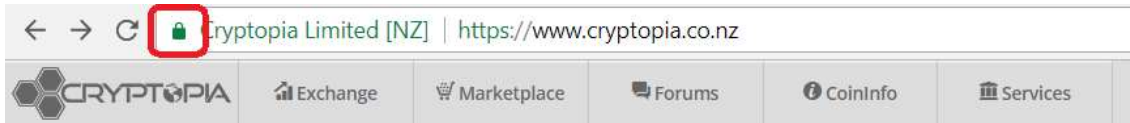
- When typing **Cryptopia** into a search engine (ie Google) or any link sent to you from an external source or website, please double check the **URL is legitimate.**

- When clicking on **Google Ads**, ensure that you check the **URL is legitimate** as phishing sites have been known to place fake advertisements.

- When clicking on any email that looks like it has been legitimately sent from Cryptopia, check the **sent address**. Scammers often send emails with links that look real but actually redirect you to a fake site. Further information on spoof emails is detailed in point **#5** below.

#2. Fake Applications (Apps) on Google Play and Apple Store

Currently Cryptopia **DOES NOT** have a mobile app. **NEVER DOWNLOAD** any app

79

fromany appstore**.** Any release of a Cryptopia App will be announced from official sources such as our **News Page** and **Twitter**.

What should I look out for?

- Never download any Application from either Google Play or Apple that claims to be a Cryptopia Application (app).

WARNING: some apps seem extremely convincing and professional but **please do not download** or **input any personal information** into any third party application.

#3. Fake support numbers

What should I look out for?

Some sites have been known to list a 'support' number for Cryptopia. These numbers are not legitimate support numbersas **WE DO NOT CURRENTLY OFFER SUPPORT VIA PHONE**. Scammers regularly set up these numbers and when users phone, they are hoping to obtain your personal account details to access your account.
- **Never phone** any number that claims to offer Cryptopia support.
- **Never disclose** any of your personal information to a support person over the phone who claims to be a member of the Cryptopia support team.

#4. Fake phone call from 'Cryptopia'

Be aware that no Cryptopia support staff will ever contact you via the phone. If you receive a call from someone claiming to work for Cryptopia support, we recommend you **hang up straight away** and **block** the caller from your device.

What should I look out for?

- **Never give your personal details** to anyone (especially if they have phoned you and claim to be from Cryptopia support).
- Cryptopia support will only ever send emails from addresses ending with **@cryptopia.co.nz** (watch out for slight typographical changes like cryptopja.co.nz).
- Cryptopia support **will never ask** for your password or your two factor authentication code.
- Cryptopia **will never request** that you grant us remote access to your computer.

#5. Spoof emails

Please be aware that we have had reports of **fake emails** being sent out to users.

What should I look out for?

- Cryptopia **will never ask** for a payment that does **not** go through **Paytopia**.
- Cryptopia **will never ask** you to send payment to a specific address.
- Cryptopia staff **will never ask** you for your password or two factor authentication details

#6. Fake Twitter accounts

It is always a great idea to keep up to date with Cryptopia via Twitter. However, always be sure you are on the official Cryptopia twitter account. Copy accounts will duplicate everything they can to seem like the real deal, however always double check the Twitter handle is **@Cryptopia_NZ.**

What should I look out for?

Cryptopia will never ask for a payment that does **not** go through **Paytopia**.

- It is a good idea to bookmark our official Twitter page, or access it through our website.
- We have **only one Twitter account**, anything else is a spoof.
- Always check the Twitter handle is **@Cryptopia_NZ.**

How do I know if I am communicating with a real Cryptopia staff member?

- Through support tickets lodged via **here**,
- Through **@cryptopia.co.nz** email addresses (although beware scammers may send emails that look like they come from **@cryptopia.co.nz)**.
- **Never** via phone.
- We **do** have an official **Facebook** and **Twitter** account. We **do not have** a Telegram account currently.

Additional security tips

- We recommend you **change** your Cryptopia **password regularly** and use a password you do not use anywhere else. See article '**How do I reset my password?**'
- **Activate** or **upgrade** your 2FA to a dynamic code, for example **Google Authenticator** or a **Cryptopia Two Factor Authentication Device**. See article '**What is Two Factor Authentication (2FA) and how do I set it up?**'.
- **Regularly check** to see if your email has been compromised. Go to: **https://haveibeenpwned.com/** or **https://hacked-emails.com/verified_leaks**.

24

- **Enable 2FA** on your email account.
- **Regularly change** your email account **password.**
- **Ensure** your Cryptopia account **password** is **different** from your email account password.
- **Create a new email address** that is used **ONLY** for Cryptopia for maximum security.

BE CAREFUL when clicking on third party links from any (and our) website. We provide links to websites outside of our own. These linked sites are not under our control, and we cannot accept responsibility for the conduct of companies linked to our website. Before disclosing your personal information on any other website, we advise you to examine their terms and conditions, privacy statement and Site Certificate.

Transactions

Cryptopia users are able to Deposit, Withdraw and Transfer in and/or within Cryptopia.

Deposits

When depositing into Cryptopia, you need to generate an address for the coin you would like deposit. This address is a unique set of numbers for funds to be allocated to you from Cryptopia's wallets.

At Cryptopia you generate an address once, for each coin, and this then always remains the same. You can generate an address from your 'Balances' page of your 'Deposits' page.

Cryptonights or some cryptocurrency coins require an additional 'Payment ID' (e.g. CryptoNight coins) or Message (e.g XEM, BIS), in addition to your 'Deposit Address', in order to be received and assigned to your Cryptopia account balance. If an extra field is required for a particular coin, it will be shown on your Deposit page for that coin, together with your 'Deposit Address'.

83

Why would a deposit not show in a customers' account?

- Unconfirmed Deposits
- Wallet is in maintenance
- Wallet may have crashed
- The wallet may have no connections
- Cross-chain deposits
- Smart Contracts
- Multisig
- MultiOutput
- Others

Unconfirmed Deposits

Deposits that has not been fully processed by the network stays as unconfirmed. They need to reach the required number of block confirmations before the transaction is completed, allowing the funds to be credited to the users' account.

Sometimes the deposit stays as unconfirmed if we had technical difficulties (i.e our Deposit tracker stops working); wallet does not have connections or the wallet is behind in block height.

Wallet is in maintenance

When a wallet is in maintenance, no deposits or withdrawals, or creating of new addresses can occur. A wallet may be put into maintenance for many reasons. It may be due to technical difficulties experienced with the wallet, a scheduled maintenance for an upgrade, or a coin developer may request for it to be put into maintenance.

Wallet has crashed

When a wallet is showing '0 connections' and '0 block height', this means that the wallet has crashed due to technical difficulties. Customers are still able to create addresses (but not have their deposits or withdrawals go through) if the status of the wallet does not get put into maintenance.

28

Wallet may have no connections

The lack connections is due to the lack of nodes required from the community. These connections are randomly formed by nodes. Nodes are generated by wallets and exists as an IP addresses that power the Peer-to-peer network, allowing transactions to be posted to the network. When there are no connections, Cryptopia will not be able to verify incoming deposits. The status of a wallet has to be set to 'NoConnections' for addresses to not be created.

Cross-chain Deposits

When depositing into Cryptopia, the customers' address needs to be correct. If somebody sends their coins to the wrong address, they lose their coins 99% of the time. When this happens, a cross-chain can occur.
When the user has deposited their coins into another address they have. These transactions can usually be recovered, however, we do charge a 10% as it takes up time and resources to do the recovery.

These often can happen when there has been a fork in the network and the user has made a deposit of the new currency into the old coin address. The transaction goes through because technically, the transaction is running off the same network.

Smart Contracts

A Smart Contract is a computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract.
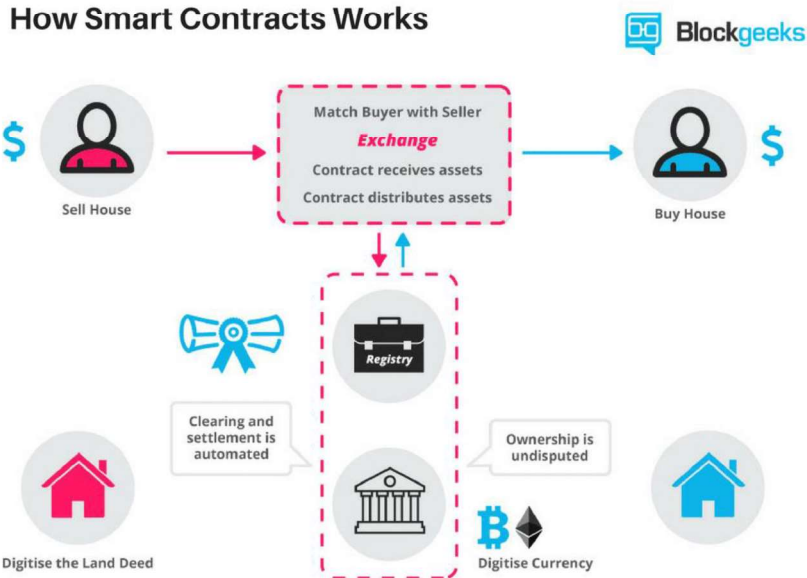
How a Smart Contract transaction looks on the block explorer:
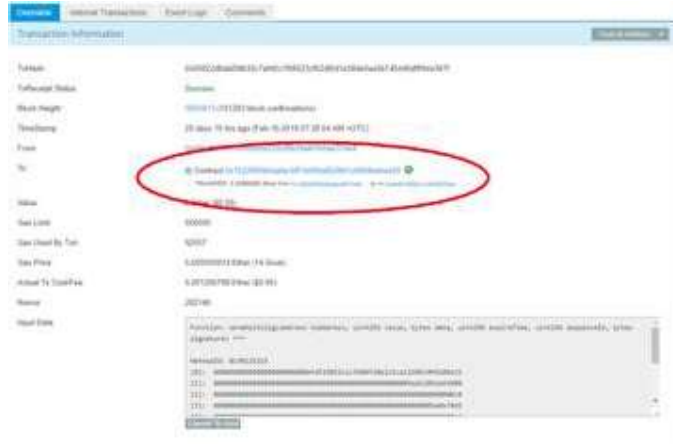
However, this is often confused with a Token transfer (which does not pose a problem to us). The token itself is a Smart Contract but the transaction is not. The key identifier is the token name below the address:

87

Multisig

Multisig transactions require multiple private keys (signatures) to sign a single transaction. Multisignature addresses require another user or users sign a transaction before it can be broadcast onto the block chain. For example: when Alice wants to pay Bob, she sends a transaction to a multisignature address, which requires at least two signatures from the group "Alice, Bob and Trent" to redeem the money. If Alice and Bob disagree on who should get the money (Alice wants a refund, whilst Bob believes he fulfilled his obligations and demands the payment), they can appeal to Trent. Trent grants his signature to Alice or Bob, so one of them can redeem the funds.

Multioutput

A multiple output transaction is exactly what is sounds like - several outputs take place within the same transaction. Our system does not support more than one deposit from a single transaction ID (hash), which is why a multiple output transaction is likely to fail.

If there are multiple deposits attached to one hash, our system can only recognize the first

31

deposit. This is common when sending directly from a pool or third party. This is often done to avoid having to pay fees across multiple transactions.

Others

Invalid Deposits

At the time of writing, invalid deposits only occur in XEM deposits, due to a monitoring service checking all transactions after 534 million US dollars worth of XEMs were stolen due to a hack attack on Coincheck, one of Japan's largest cryptocurrency exchanges.

35820113	XEM	1000.00000000	Invalid	86b7c708ba3e3bad2ca6cc8f10997626835c0b5e55cb613cc5e44f3b8e83bdbd	9

DBET - Token v1

Customers may have deposited DBET tokens that have not been updated to the latest version. Cryptopia currently does not support version 1 DBET coins and due to this, we will have to manually recover customers' funds. Customers will need respond to their ticket with a valid ETH address for us to send the coins back to you.

Upon receiving the coins, customers can update them according to these instructions: https://www.decent.bet/token/info

Valid Transaction IDs

Customers have to provide us with a valid transaction ID for us to investigate any missing deposits. If we do not have a valid transaction ID or if is not showing on the block explorer, the sending wallet/exchange may not have posted the transaction the the network. Customers will have to contact their sending wallet/exchange for more information.

```
                    User submits a ticket
                    asking where is their
                         deposit
                            │
                            ▼
                     Have a transaction
                           ID?
              ┌─────────────┴─────────────┐
              ▼                           ▼
            Yes                          No
              │                           │
              ▼                           ▼
     Is this in their account      Ask for a valid
        in Admintopia?             transaction ID
        ┌─────────┴─────────┐
        ▼                   ▼
 ┌──────────────┐    ┌──────────────┐
 │If the        │    │    No        │
 │transaction   │    └──────┬───────┘
 │has reached   │           │
 │way more      │    Yes. Customer needs
 │confirmations │    to wait for it to be
 │on the block  │◄──   confirmed
 │explorer, send│           │
 │it to App     │           ▼
 │Supp.         │    Is the transaction ID
 └──────────────┘    in the block explorer?
                  ┌───────────┴───────────┐
                  ▼                       ▼
                 Yes                     No
                  │                       │
                  ▼                       ▼
          Sent to the correct      Sending
              address?             wallet/exchange has    Inform customer to
          ┌───────┴───────┐       not published this in ►  contact sending
          ▼               ▼        the network            wallet/exchange
         Yes             No
          │               │
          ▼               ▼
      Cryptonight?    Crosschain/wrong
          │              wallet
    ┌─────┴─────┐           │
    ▼           ▼           │
   Yes    No = It is a      │
    │      missing          │
    │      deposit.         │
    ▼           │           │
Identify        │           │
payment ID?     └───────┐   │
 ┌──────┴──────┐        ▼   │
 ▼             ▼   Send to Application ◄─┘
No payment  Payment ID  Support
ID =        present =       ▲
Customer    Missing         │
has made a  deposit. ───────┘
mistake
 │
 ▼
Ask if customer would
like to pay 10% of
transaction to recover
coin
 │
 ▼
Put in 'In progress
and Hold queue'.
```

91

Withdrawals

Cryptopia users are able to withdraw funds stored in the exchange.

CRYPTOPIA CUSTOMER SERVICE ANALYST MANUAL

Version 2.0

OCTOBER 7, 2018
CRYPTOPIA

Contents

96

Welcome to Cryptopia Customer Service Team!

Introduction

Cryptopia Limited was started in 2014 by Rob Dawson and Adam Clark as a Cryptocurrency Exchange. Based in New Zealand, the Cryptopia Exchange has over 2 million global users and the world's largest range of cryptocurrencies. Our focus is our passionate community of users and we aim to offer them world class service including a fast, secure exchange experience.

Ethically run and compliant with New Zealand regulations, our users experience premier support and fast response times, plus early access to new and innovative coins that have passed our stringent ethical, legal and technical requirements. The Exchange is simple to use, fast and secure. Users can deposit, trade or withdraw all of our 584 listed coins. With access to dynamic charts, live coin information, world class service and the largest range of coins, Cryptopia offers users the best global transparent exchange platform to trade cryptocurrencies.

Cryptopia's ultimate mission is to enable the widespread adoption of cryptocurrencies to give people back control of their money through faster, cheaper and more efficient financial services. We aim to utilise Blockchain technology to open the Fintech sector to innovation and are working on a number of products and services to make this a reality.

History of Cryptopia

- ✓ Been around for 4-5 years
- ✓ Launched as an exchange in 2014
- ✓ Adam Clark and Rob Dawson are our founders.
- ✓ What started out as a hobby, quickly turned into a full-time job.
- ✓ At the start of 2017, we had ~12 staff (including contractors), now we are sitting at 100 full time staff.

Intranel relationship:

- Adam used to work at Intranel. When he decided to start Cryptopia, he was told to stay in the building and use the facilities while he was trying to get it off the ground.
- Andy, Dave and Adam (who are the founders of Intranel) also help out full time in Cryptopia.
- Most of Intranel Devs work full time for Cryptopia.

Cryptopia in the Crypto space:

- ✓ As an exchange, we are different from most other exchanges as our volumes are generated from crypto to crypto trades. While most other exchanges deal with fiat to crypto exchange.
- ✓ Majority of our listed coins are alt coins.
- ✓ We are globally recognised for listing many alt coins.

Our base markets

BTC, USDT, NZDT, LTC, and DOGE.

https://www.cryptopia.co.nz/Exchange

Our Customer Relationship Management Tools

https://www.admintopia.co.nz/

https://supportcryptopia.service-now.com/login.do

Our Customer Service Tool Kit

https://cryptopia.atlassian.net/wiki/spaces/SUP/overview

- **Templates:**
  https://cryptopia.atlassian.net/wiki/spaces/SUP/pages/127172618/Support+Templates

- **Renaming of Tickets for Triaging tickets into App Support:**
  https://cryptopia.atlassian.net/wiki/spaces/SUP/pages/230817831/Triage

- **Phishing Scams info:**
  https://cryptopia.atlassian.net/wiki/spaces/SUP/pages/330563587/Phishing+Scams

- **Jira:**
  https://jira.cryptopia.co.nz/

- **Promapp:**
  https://go.promapp.com/cryptopia

Help Centre for Users

https://support.cryptopia.co.nz/csm

100

Our Values

Communicative

We aim to understand the environment around users and proactively build an excellent experience for both users and staff. We do this by clearly addressing and discussing processes internally, hoping that this will reflect externally with our approach to customers.

"Never assuming what others know."

Comprehensive

Being comprehensive ensures that we take the time to see the whole story and intricacies that it entails. We aim to take the extra effort to learn the technology we use and apply that information to be as effective and helpful as possible.

"If some pieces of the story are missing, we will endeavour to find the missing piece."

Compassionate

We aim to be compassionate by going out of our way to understand where others are coming from – this includes co-workers and all users. We want to be empathetic and approach situations from multiple viewpoints.

"We are all on the same boat sailing towards the same goal."

--

WE SHOULD NOT WORK WITHOUT COMPASSION,

WE MUST USE IT LIKE IT'S GOING OUT OF FASHION,

WE'RE ALL ON A BOAT,

WE MUST STAY AFLOAT,

WE ACHIEVE THIS WITH COMPUTERS AND PASSION.

~ CRYPTOPIA SUPPORT TEAM 2018

Objectives and KPIs (WIP)

1. Cryptopia to consistently deliver World Class Service
2. Consistent messaging and Brand tone
3. Auto-responses in all channels to set customer expectations
4. First response within <mark>24 hours</mark>

FAQs

Let's dive into it and get started!

How does a user set up an account with Cryptopia?

BELOW ARE STEP BY STEP INSTRUCTIONS TO HELP USERS SET UP AN ACCOUNT WITH CRYPTOPIA.

#1. The user clicks on the '**Register'** button at the top right-hand corner.

#2. The user then creates a **Username** for the account and nominate an **Email Address**.

Users should take the following into consideration when selecting their Email Address:

- Use a **permanent email address** to which the user has reliable access
- Make sure it is **not connected** to any other Cryptopia account; and
- Is **unique** to Cryptopia and **not used** on any other cryptocurrency service, exchange or site. This email address will be used for account verification and registration completion, its security is very important.
- Make sure that the email account as well as information and credentials associated with it **have not been compromised.** We recommend using available online tools (e.g. **https://haveibeenpwned.com/**) and regularly checking it.

#3. The user creates a '**Password'** for their account (see figure 1).

The user should use a unique password which they do not use for anything else. Cryptopia has strict minimum password requirements for the security of user accounts and these are case sensitive.

PLEASE NOTE: For a password to meet Cryptopia minimum password requirements it must be a minimum of 8 characters long, and include at least one of each of the following:
- 1 Uppercase letter;
- 1 Lowercase letter;
- 1 Special character; and
- 1 number.

Figure 1 – Creating a Password

#4. The user clicks the 'I agree to the Terms & conditions' box and 'I'm not a robot' box and finally the 'Create Account' button.

#5. After the user complete registration, a confirmation email will be sent to their nominated Email Address.

Confirmation Email Sent.

An email has been sent to ▢▢▢▢▢▢▢, please click the activation link in the email to complete your registration process.

#6. After the user completes registration, a **confirmation email** (see figure 2) will be sent to their nominated **Email Address**.

Figure 2- Account Registration Confirmation Email

#7. The user must then open the email and click on the '**Verify My Email Address**' link in the email.

PLEASE NOTE: This link expires after several hours, users must check for the email and make sure they successfully activate their account soon after registering. These can sometimes go to 'junk', 'spam' or 'promotional' folders so the user must ensure they check all folders.

#8. The user's Email Address will now be verified, and they will be prompted to log in using their **Email Address** (see figure 3), their case sensitive **Password** and their **4-8 digit 2FA code**.
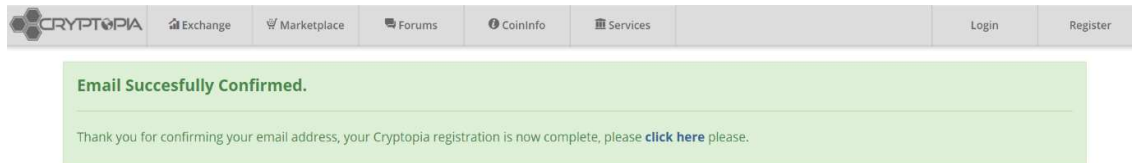
Figure 3 – Email Address verified

#9. The user's account **is now set up** and they are ready to begin trading!

What should a user do if they are experiencing registration issues?

- If a user can't find the registration email, **it may have been filtered into a different alternative folder** within their inbox (i.e. junk, spam or promotional). These folders often do not sync with mobile apps or email clients. We suggest that users log onto their webmail if possible and perform a thorough search.
- We are aware that some ISP email providers and customized domains reject or defer some of our automated emails. This may either cause **delay**, or the user **may not receive** them at all. If the user has not received a Cryptopia email they are expecting, they should try and whitelist this email – **noreply@cryptopia.co.nz** with their provider, in addition to contacting Cryptopia Support describing the issue so we can check and confirm if we can assist.
- If the link is not clickable, this is likely due to a compatibility issue with the browser or email client the user is using. If possible, they should try using a different browser or client to view the email, and if they still cannot get it to

12

work, they should contact Cryptopia Support and we can manually activate their account.

- If after clicking the link, the user gets a message on Cryptopia saying "You are not authorized to view this area", this indicates **the link has expired**. If this occurs, the user should contact Cryptopia Support and we can manually activate the account.

Does a user need to be verified?

Following successful registration of the user's Cryptopia account, they automatically achieve **LEVEL 1 VERIFICATION**. This happens when they click on the activation email we send to them and they log into their account. For further information about setting up a Cryptopia account, see **'How does a user set up an account with Cryptopia'**.

==**LEVEL 1 VERIFICATION** gives a user access to all functions and features on Cryptopia.==

The only restriction placed on **LEVEL 1 VERIFICATION** is the limit and type of withdrawals and transfers between Cryptopia accounts. This is currently **cryptocurrency only** with the equivalent value of $5000 NZD every 24 hours*.

*PLEASE NOTE: A '24 hour period' means 24 hours from a user's first withdrawal or transfer, for example, if a user makes a withdrawal at 4pm on the 8th of Jan, their 24 hour period for that amount runs until 3.59 pm 9th of Jan. The next 24 hour period will commence with their next withdrawal or transfer.

==Please go to **'How does a user increase their verification level?'** for step by step instructions on how to increase an account's verification level if necessary.==

How does a user increase their Verification level?

If a user wishes to increase the Level 1 Verification daily limit imposed on withdrawals and transfers between Cryptopia accounts, they will need to apply for Level 2 Verification.

THE LEVEL 2 VERIFICATION LIMIT is currently the equivalent of $50,000 NZD per 24 hours*.

*PLEASE NOTE: A '24 hour period' means 24 hours from a user's first withdrawal or transfer, for example, if a user makes a withdrawal at 4pm on the 8th of Jan, their 24 hour period for that amount runs until 3.59 pm 9th of Jan. The next 24 hour period will commence with their next withdrawal or transfer.

Applications for Level 2 Verification must be made via our website and be compliant with International Anti-Money Laundering Law (AML) provisions. The applicant must be over 18 years of age at the time of application and ensure they hold necessary identification documentation.

TO APPLY FOR AN INCREASED VERIFICATION LEVEL, USERS MUST FOLLOW THE STEPS OUTLINED BELOW:

13

#1. Log into their Cryptopia account

#2. Go to 'Balances'

#3. Click on the 'Daily Limit' link above the balances of all their coins (see Highlight in Figure 4).

Figure 4 – Balances page. 'Daily Limit' link at top of page, above balances.

#4. Submit Verification for Level2 (As shown in Figure 5).

User Verification

Verification Level 1   Complete

Users verified by email have a daily withdrawal limit of $5,000.00 NZD

EMAIL

emily.chamberlain@cryptopia.co.nz

Verification Level 2   Incomplete

Users that have provided evidence of their identification have daily limit of $50,000.00 NZD

COUNTRY

[▼]   Next

Verification Level 3   Incomplete

If you need to update any of the submitted details, please contact Cryptopia Support.

- Personal Accounts with Verification Level 2 requiring a higher daily limit
- Businesses and Corporations

Figure 5 – Details to be filled in L2 Verification boxes

PLEASE NOTE: The user will see that their account is already **LEVEL 1 VERIFIED**

#5. Users must complete **all details** in the form including:
- **First name** (same characters as ID, ex. 李四 is shown on ID, 李四 must also be entered in the registration form; Li Si is not sufficient);
- **Last Name** (same character as ID);
- **Birthday** (DD/MM/YYYY format) or select from calendar;
- **Country**
- **City**
- **State**
- **Postcode**
- **Address** (PO Box or non-specific address is not acceptable).

#6. The user must upload their **Identification Documentation**. AML Law requires either a Government issued **current** Passport, or Driver's License, or Government issued Identity Card.

PLEASE NOTE: Documentation **must** display a photo, full name and date of birth - if this information is located on the back and front of the user's Identity Card or Driver's License the applicant must upload the documentation so that all information is displayed clearly in the **one** image.
PLEASE NOTE: The file size limit for uploads is 4MB. We will not accept any identification that has expired. Users must ensure the image is clear and features such as the Identification Documentation text are identifiable. These photos must not be edited in anyway.

#7. The user must upload a clear photo of themself holding their uploaded Identification Documentation.
PLEASE NOTE: The user should make sure their camera is clean and they are entirely visible in the photo. We cannot accept photos where we cannot see the user's face. The user must hold their identification open to ensure the **photo**, **full name** and **date of birth** are visible.

#8. The user must tick the **'I accept the Terms and Conditions'** box.
#9. The user must click on **'Submit'**.

PLEASE NOTE: Applicant must be at least 18 years of age at the time of application.

What happens now?

Once we have received the user's Application for Level 2 Verification, our team will review the application. If the application is approved, the user will be notified via **email**.

If the application is rejected, the user will be notified by email with a reason for the rejection. The user will need to address the issue outlined in the email (for example, identification documentation, quality of photo etc.) and resubmit their application by following the same process as the above.

How does a user increase their Verification level to LEVEL 3?

If a user wishes to achieve Level 3 verification they have to provide the following to verification@cryptopia.co.nz:

- Cryptopia username
- An additional photo of user holding the ID that was submitted for Level 2 with another piece of paper which has their handwritten Cryptopia username on it
- Proof of their address such as a utility bill, bank statement/letter, or other government communication
- A statement as to their "Source of Wealth", in other words how they have made enough money to be trading at this level
- If the account is intended as a company account, the user will also need to provide proof of a link between them and the company, such as a bank statement in the company name addressed to them, or a link to a public government register that shows them as a director of the company.
- If they are not the company director, we will also require a handwritten statement from the director approving them to trading on the company's behalf.

All of the above details need to be emailed to verification@cryptopia.co.nz.

In addition, 2FA (Two Factor Authentication) must be enabled on their Cryptopia account for us to proceed, specifically we need some form of OTP (one time password) such as Authentication Application (e.g. Google Authenticator or Authy) or our Cryptopia Authenticator Device.

If their application is rejected, they will be notified by email with a reason for the rejection. They will need to address the issue outlined in the email and resubmit their application by following the same process as the above.

PLEASE NOTE: LEVEL 3 VERIFICATION LIMIT is currently the equivalent of $500,000 NZD per 24 hour period

What is ReCaptcha?

reCAPTCHA is a free service from Google that helps protect websites from spam and abuse. A "CAPTCHA" is a Turing test to tell human and bots apart (see figure 6). It is easy for humans to solve, but hard for "bots" and other malicious software to figure out.
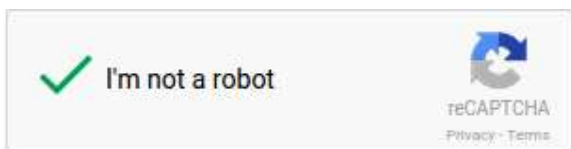
Figure 6 – ReCAPTCHA success

Why is reCAPTCHA not working on a user's computer?

There may be some instances where certain browsers do not display reCAPTCHA properly. For further information and troubleshooting, users should refer to Google's ReCaptcha support page.

Why is a user not receiving emails from Cryptopia (including verification)?

There are several reasons why users may not be receiving, or cannot find, automated Cryptopia emails that they might be expecting.

Users should use these troubleshooting tips to help:

#1. **Is their account activated?**

Following registration the user will be sent a 'Registration Confirmation' email sent to their nominated Email Address. To complete their registration, they will have to click on the account verification link. The user will not receive any further emails, including password resets, until their account is activated.

#2. **Is the user checking the right email inbox?**

The user should check that they did not register with an alternative email address and have checked the right inbox.

#3. **Has the user checked the junk, spam or promotional folders in their inbox?**

It is possible that emails from Cryptopia get filtered into a different folder within the user's inbox, which may cause issues with synchronisation between mobile apps or email clients. Users should log into their email via a web browser if possible, and perform a thorough search for it.

PLEASE NOTE: There are sometimes issues with automated emails sent to email accounts provided by some internet service providers (ISP's). In these cases, our automated emails are often delayed, but should eventually be received in the user's mailbox.

A small number of ISP providers may completely reject our automated emails as spam. If a user is having a consistent issue receiving Cryptopia's automated emails, they should investigate whether they can whitelist our cryptopia.co.nz domain from their email account, or request their provider to remove the block on cryptopia.co.nz.

If the user's email provider is not able to help by whitelisting our domain, we recommend using an alternative email service provider and setting up a new account. Users can change their registered email by raising a support ticket and letting our Support team know what email they would like to change to.

Are there any account limits for trading, deposits or withdrawals?

There are currently **no account limits** for trading or deposits to Cryptopia. Limits for withdrawals and transfers between Cryptopia accounts depend on the user's verification level.

PLEASE NOTE: Due to Anti Money Laundering (AML) regulations, accounts must have a **Level 2 Verification Level** for us to accept deposits or withdrawals of fiat New Zealand Dollars (NZD). (**This service is currently not available**)

Level 1 Verification – Withdrawal and Transfer Limit

Level 1 verification is achieved during the registration process once the user clicks the link on the Registration Confirmation email sent to their registered email address. Every Cryptopia account has access to all functions and features on Cryptopia once the account is activated at Level 1.

Level 1 verified accounts have **a withdrawal and transfer limit of $5,000 NZD** equivalent of value per 24-hour period*.

Level 2 Verification – Withdrawal and Transfer Limit

Users can increase the withdrawal and transfer limit on their account by upgrading it to Level 2 verification. See our article on increasing account verification to Level 2 or 3 **'How does a user increase their verification level?'** .

Level 2 verified accounts have **a withdrawal and transfer limit of $50,000 NZD** equivalent of value per 24-hour period*.

Level 3 Verification - Withdrawal and Transfer Limit

Users can request a further increase on the withdrawal and transfer limit on their account by upgrading it to Level 3 verification. See our article on increasing account verification to Level 2 or 3 **'How does a user increase their verification level?'**.

Level 3 verified accounts have **a withdrawal and transfer limit of $500,000 NZD** equivalent of value per 24-hour period*.

PLEASE NOTE: *A '24-hour period' means 24 hours from the user's first withdrawal or transfer. *For example, if a user makes a withdrawal at 4pm on the 8th of Jan, their 24-hour period runs until 3.59pm 9th of Jan for that amount. The next 24-hour period will commence with their next withdrawal or transfer.*

Are there any specific requirements for ID documents?

The only time a user needs to provide ID documentation is if they choose to apply for **Level Two Verification**. Users will be required to upload identification documentation when they apply. See the articles **Does a user need to be Verified?** and **How does a user increase their verification level?** for more information.

Cryptopia's ID requirements are outlined below:

#1. Users must **upload a photo** of their identification document.

#2. **Law requires** user's identification document to be either **a government issued current** passport, Driver's License or Identity Card.

#3. This document must display a **clear picture of the user**, and include the user's **full name** and **date of birth** (If this information is found on two sides of the user's ID, the user must upload both sides into one document).

#4. The **file size limit** for uploads is 4MB.

#5. We **will not accept** any identification that has **expired.**

#6. The user must **upload** a photo of themself holding their identification documentation.

#7. The user should make sure their **camera lens is clean** and their face is **entirely visible** in the photo.

#8. We cannot accept photos where we cannot see the user's face. The user must hold their identification open to ensure their **photo**, **full name** and **date of birth** are visible.

#9. Please note that **we cannot accept edited photos**.

PLEASE NOTE: We cross check user's submitted information with their uploaded ID. This means whatever characters are used on the user's full name on their ID need to be the same characters that the user submits in the form.

What fees does Cryptopia charge and how does a user see them?

Cryptopia charges **fees** on Trades and Withdrawals on our Exchange.

Trading Fees

- Cryptopia charges a **0.2% fee for every trade** on our Exchange.
- The fee is automatically calculated and displayed in the **'Fee'** field after a user has entered an 'Amount' and 'Price' (see figure 7).

Figure 7 – Trade Table showing 0.2% trade fee

- The 'Total' field **includes the fee** which is shown before a user confirms the order (see figure 8).
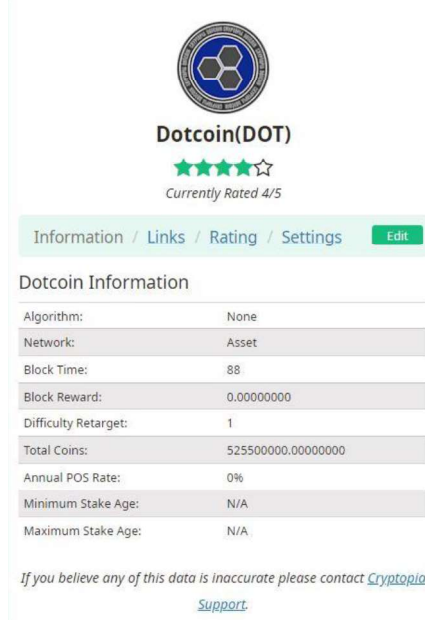
Figure 8 – Trade Table showing 'Total'

PLEASE NOTE: Further information on how to trade on Cryptopia can be found in our article **'How do I trade? (for beginners)'**

Withdrawal Fees

- Each cryptocurrency coin listed on Cryptopia has **different fee** for Withdrawals.
- These fees **are static** amounts for each transaction, not percentages of the value of a user's withdrawal, e.g. a user will pay the same withdrawal fee whether they are withdrawing .01 BTC or 1 BTC in a single transaction.
- Users can view our Withdrawal Fees on the **Coininfo page**, under **'Settings'** for each cryptocurrency coin (see figure 9).

Figure 9 – Settings Tab for DOT in the Coin Info Page

- Withdrawal fees are based on the **individual Blockchain transaction** cost for that coin. This blockchain transaction cost goes towards paying the miners undertaking confirmations and network running costs.
- Cryptopia reviews the 'Withdrawal Fees' on coins periodically, after assessing the average cost of a single transaction on the Blockchain and considering transaction speed optimisation.

PLEASE NOTE: For detailed information on how to withdraw their coins users can refer to our article **How do I make a withdrawal?**'. For further information on Blockchain Confirmations, users can refer to our article **What are Blockchain Confirmations**?

How does a user reset their password?

There are two options if a user wishes to reset the Password on their account. Below is a step by step guide.

For the safety of a user's account we confirm that Cryptopia staff can never view a user's Password so should not ask us or tell us what their Password is.

Cryptopia has strict Minimum Password Requirements for the security of user accounts and these are case sensitive.

PLEASE NOTE: For a user's Password to meet Cryptopia Minimum Password Requirements it must be a minimum of 8 characters long, and include at least one of each of the following:

- 1 Uppercase letter;
- 1 Lowercase letter;
- 1 Special character; and
- 1 number.

OPTION 1 - CAN'T LOG IN

#1. The user must go to https://www.cryptopia.co.nz/Login/

#2. The user must click on the '**Forgot your Password**' at the bottom of the screen.

#3. The user must enter THEIR Email Address and tick the '**I am not a robot**' box. (Note that the reset function does not check to see if an email belongs to a registered user. A user can make a typo or enter the wrong Email Address by mistake. If there is a trailing space, or it does not match the format of name@email.tld, they will see the message "Please enter a valid email address.")

#4. The user must click '**Send Password Reset**' button (see figure 10).
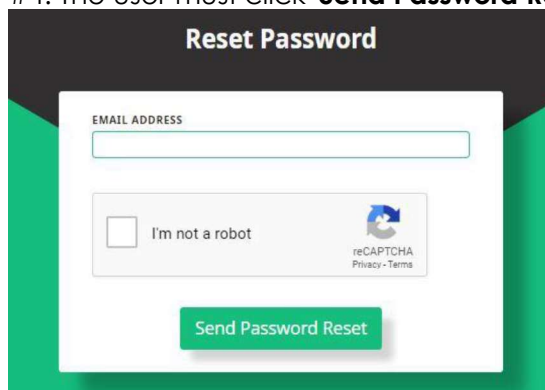
Figure 10 – Reset password view

22

115

#5. The user will be sent an email with a link to reset their Password (see figure 11).

Figure 11 – Reset Password email

#6. The user must click on the 'Reset My Password' button in that email.

#7. The user must enter THEIR Email address and THEIR new Password when prompted. The user will be asked to confirm that new Password. Please note our Minimum Password Requirements detailed above.

#8. The user must press 'Click Here' and they will be redirected to login using their new Password.

#9. The user's Password is reset!

PLEASE NOTE: The **'Reset My Password'** link in the email expires within 15 minutes so the user should click on the link in the email as soon as they receive it.

OPTION 2 - ALREADY LOGGED IN

Users can also reset their Password from their Account Security page if they are already logged in. Below is a step by step guide.

#1. The user must go to **'Security**' page.

#2. Under **Account Security**, the user must go to **Change Password**.

#3. The user must enter their current Password.

#4. The user must enter their new Password, noting our Minimum Password Requirements detailed above.

#5. The user must confirm their new Password.

#6. The user must click on 'Change Password' button.

#7. The user's Password is now changed!

#8. The user will be logged out, and they will need this Password to log back in.

What is a cryptocurrency wallet?

A Cryptocurrency Wallet is software or service used for representing cryptocurrency transactions and securing ownership of them.

Each Wallet is associated with a **Public Key,** which is used as an address for managing and assigning cryptocurrency transactions sent over a blockchain. This Public Key is commonly the address you will specify whenever you send a cryptocurrency transaction from one place to another.

Each Wallet also securely stores a **Private Key,** which is a key that secures ownership of the cryptocurrency balance associated with the Public Key address.

There are various types of cryptocurrency wallets which are used and managed in different ways. Exchange services like Cryptopia manage and maintain Wallets, and provide users with the functionality to send and receive transactions as well as securely hold the balances assigned to their accounts.

We manage and maintain a Wallet for each cryptocurrency coin, and using this Wallet allow users to generate an address which is associated to each respective account on our database. Users can only generate one address per coin and this address will usually never change.

Types of Cryptocurrency Wallets

Each cryptocurrency coin requires its own specific Wallet as each operates on its own specific blockchain. To view the software available to set up your own Personal Wallet for a specific cryptocurrency coin, head to the **Coin Info** page and **select** the 'Links' heading. The first link will be the website for that coin and there you will find the types of wallets that are on offer for different platforms. Outlined below are the common types of Wallets.

#1. Hardware Wallets

Hardware Wallets are recommended for your **own storage of cryptocurrency coins**, as this gives you complete control over the wallet and the Public and Private keys associated with it. These are hardware dongles specifically designed for secure, long-term storage of a cryptocurrency, and are generally one of the most secure ways to keep your Cryptocurrency holdings safe.

24

#2. Online web-based Wallets

Online wallets are typically hosted online and accessed from a web browser. These are generally simple to access and use but may be limited in functionality.

Due to being hosted and managed by a third party, and always being online, they are not necessarily as secure as other wallet types and may be targets for exploiting your cryptocurrency coins.

#3. Desktop Wallets

Desktop Wallets are accessed on a desktop/laptop computer and utilise its operating system, e.g. desktop computer using a Windows operating system.

They are generally **easy to use**, but require some setup and maintenance, and can be kept online or offline depending on your needs.

Desktop Wallets have the **benefit of storing your Private Key on a local platform,** instead of online as a Web Wallet. The security of your cryptocurrency is dependent on the security of the device running them, as well as your general online security practices.

#4. Mobile Wallets

Mobile wallets have some similarities to both Desktop and Web/Online wallets. They are designed to be run specifically from a mobile device, with easy access and convenience in mind.
PLEASE NOTE: phones and other devices often have their own security flaws, such as being easily stolen or accessed by unauthorised parties.

#5. Paper Wallets

Paper Wallets are physical printouts containing the Public and Private keys associated with your cryptocurrency holdings. They require a little more effort and knowledge to manage, but can provide higher levels of security against online attacks as the Private Key is not stored or accessible anywhere online.

Is Cryptopia safe?

Cryptopia actively strives to ensure the **security**, **integrity** and **privacy** of personal information submitted to us, including regular review and compliance of our security measures in line with current technology. Unfortunately, no data transmission over the internet can be guaranteed to be totally secure.

We will take all reasonable steps to protect the personal information users may transmit to us or we collect from our online products and services. Once submitted, we take all reasonable steps to maintaining its security on our systems.

Additionally, our employees and contractors who provide services related to our information systems, are also obliged to maintain **confidentiality** and **security** of any personal information held by us.

We recommend users regularly review our **Terms & Conditions** and our **Privacy Policy** to ensure that you are familiar with these policies. We reserve the right to change these policies from time to time.

PLEASE NOTE: There are additional measures that you can take to ensure your personal details and accounts are kept safe such as **Two Factor Authentication** and being aware of the common scam tactics used in the industry, six of which are detailed below.

Common scam tactics

#1. Phishing websites

Phishing is a common technique for acquiring a user's personal or account data. Scammers set up fake websites that resemble reputable business sites in order to get you to enter your account or personal information.

The site may look very legitimate (and often look almost identical to official websites) but they will always have a slightly different domain name/URL. Before entering any of your personal details into the website, ensure you have reviewed the below:

What should I look out for?

Every time you log into your account, we recommend double checking that you are visiting the **correct URL,** which you can find below.

https://www.cryptopia.co.nz

PLEASE NOTE: Be aware of URLs that end in **.com, .ws, .cx**

- Check that the URL address starts with **https://**

- Check the **Site Certificate** to see whether a website is safe to visit (see figure 12). If you are using Google Chrome, you can check the security status to the left of the web address (a green lock is an indicator that the website is secure). If you are using a different browser, please look how to view the Site Certificate in the settings of your browser.

Figure 12 – Secure website icon

- When typing **Cryptopia** into a search engine (i.e. Google) or any link sent to you from an external source or website, please double check the **URL is legitimate** (see figure 12).

- When clicking on **Google Ads**, ensure that you check the **URL is legitimate** as phishing sites have been known to place fake advertisements (see figure 13).
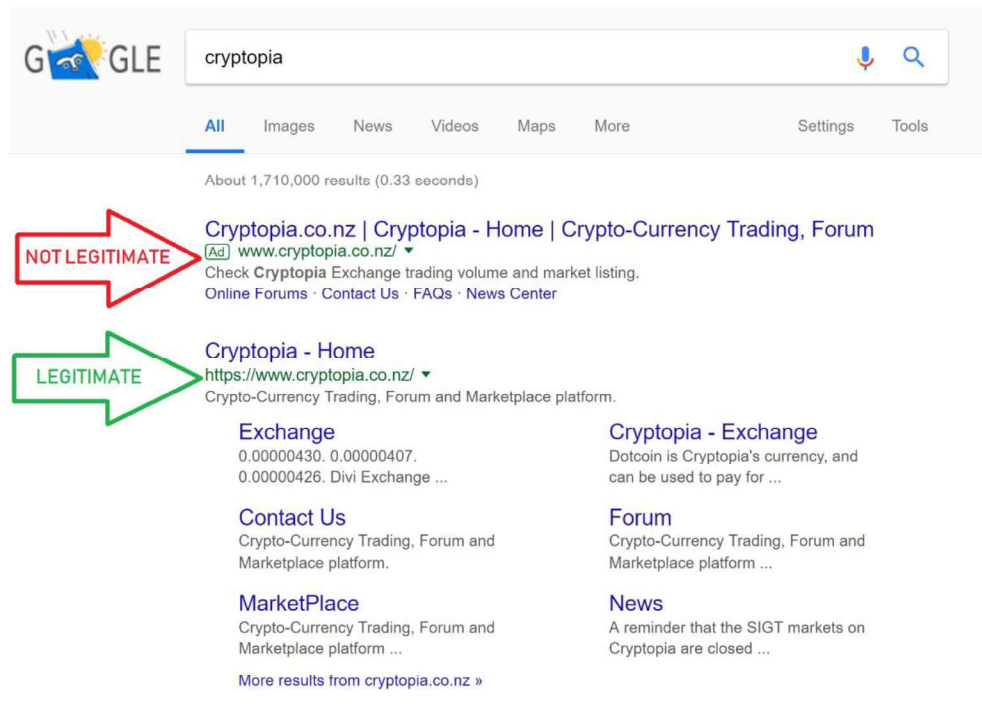
Figure 13 – Google Ads showing phishing websites

- When clicking on any email that looks like it has been legitimately sent from Cryptopia, check the **sent address**. Scammers often send emails with links that look real but actually redirect you to a fake site. Further information on spoof emails is detailed in point **#5** below.

#2. Fake Applications (Apps) on Google Play and Apple Store

Currently Cryptopia **DOES NOT** have a mobile app. **NEVER DOWNLOAD** any app from any App store**.** Any release of a Cryptopia App will be announced from official sources such as our **News Page** and **Twitter**.

What should I look out for?

- Never download any Application from either Google Play or Apple that claims to be an official Cryptopia Application (app).

WARNING: some apps seem extremely convincing and professional but **please do not download** or **input any personal information** into any third-party application.

28

#3. Fake support numbers

What should I look out for?

Some sites have been known to list a 'support' number for Cryptopia. These numbers are not legitimate support numbers as **WE DO NOT CURRENTLY OFFER SUPPORT VIA PHONE**. Scammers regularly set up these numbers and when users phone, they are hoping to obtain your personal account details to access your account.

- **Never phone** any number that claims to offer Cryptopia support.
- **Never disclose** any of your personal information to a support person over the phone who claims to be a member of the Cryptopia support team.

#4. Fake phone call from 'Cryptopia'

Be aware that no Cryptopia support staff will ever contact you via the phone. If you receive a call from someone claiming to work for Cryptopia support, we recommend you **hang up straight away** and **block** the caller from your device.

What should I look out for?

- **Never give your personal details** to anyone (especially if they have phoned you and claim to be from Cryptopia support).
- Cryptopia support will only ever send emails from addresses ending with **@cryptopia.co.nz** (watch out for slight typographical changes like cryptopja.co.nz).
- Cryptopia support **will never ask** for your password or your two-factor authentication code.
- Cryptopia **will never request** that you grant us remote access to your computer.

#5. Spoof emails

Please be aware that we have had reports of **fake emails** being sent out to users.

What should I look out for?

- Cryptopia **will never ask** for a payment that does **not** go through **Coin listings**.
- Cryptopia **will never ask** you to send payment to a specific address.
- Cryptopia staff **will never ask** you for your password or two factor authentication details

#6. Fake Twitter accounts

It is always a great idea to keep up to date with Cryptopia via Twitter. However, always be sure you are on the official Cryptopia twitter account. Fake accounts will duplicate everything they can to seem like the real deal, however always double check the Twitter handle is **@Cryptopia_NZ.**

What should I look out for?

- It is a good idea to bookmark our official Twitter page, or access it through our website.
- We have **only one Twitter account**, anything else is a spoof.
- Always check the Twitter handle is **@Cryptopia_NZ.**

How do I know if I am communicating with a real Cryptopia staff member?

- Through support tickets lodged via **https://support.cryptopia.co.nz/**
- Through **@cryptopia.co.nz** email addresses (although beware scammers may send spoof emails that look like they come from **@cryptopia.co.nz)**.
- **Never** via phone.
- We **do** have official **Facebook** and **Twitter** accounts. We **do not have** a Telegram account currently.

Additional security tips

- We recommend you **change** your Cryptopia **password regularly** and use a password you do not use anywhere else. See article '**How do I reset my password?**'
- **Activate** or **upgrade** your 2FA to a dynamic code, for example **Google Authenticator** or a **Cryptopia Two Factor Authentication Device**. See article **'What is Two Factor Authentication (2FA) and how do I set it up?'**.
- **Regularly check** to see if your email has been compromised. Go to: **https://haveibeenpwned.com/** or **https://hacked-emails.com/verified_leaks**.
- **Enable 2FA** on your email account.
- **Regularly change** your email account **password.**
- **Ensure** your Cryptopia account **password** is **different** from your email account password.
- **Create a new email address** with an email provider that offers 2FA for login, which is used **ONLY** for Cryptopia for maximum security.

BE CAREFUL when clicking on third party links from any (and our) website. We provide links to websites outside of our own. These linked sites are not under our control, and we cannot accept responsibility for the conduct of companies linked to our website. Before disclosing your personal information on any other website, we advise you to examine their terms and conditions, privacy statement and Site Certificate.

ServiceNow

Our Customer Relationship and IT Management Tool

8 standard views

1. My Cases: These are of all cases that need to be followed up (Open or New state);
2. Awaiting Info cases: These are all cases that are awaiting a response from a user;
3. Accounts Team Cases;
4. Compromised Accounts Team Cases;
5. Email Team Cases;
6. Trades Team Cases;
7. Transactions Team Cases;
8. Triage Cases

You will also need to have the following columns (in order):

Case no., Short Description, Contact, Channel, State, Assigned to, Assignment Group, Problem, Created, Updated, Updated By, Tags, follow up.

See the confluence page to set up your filters and columns

Figure 14 – Column view and filters for case views

31

124

Rules

- Always sort ticket queues by oldest 'Created' date.
- Assign the ticket to yourself as soon as you open it.
- Always accept assignment of ticket to change state from New to Open.
- Do not bulk assign a queue of tickets to yourself.
- **Always check for multiple tickets.**
- If a ticket is related to a coin, ensure the 'Coin Name' box has the correct coin entered.
- If you have a case that is time sensitive and is awaiting info from a user, please assign this to someone that is working in the next shift for them to ensure someone has eyes on it, and send them a note on Teams.
- Please un-assign all tickets by the end of work week (or if you're not showing up the next day), unless you have a ticket that requires extended care by yourself. Mark these cases as 'Complex'.
- 2FA reset and email change tickets should be marked for "Follow Up" in 24 hours.
- Tickets enquiring about coin listings should be emailed to listings@cryptopia.co.nz
- Tickets from coin developers should be emailed to coinwallets@cryptopia.co.nz
- Tickets related to marketing should be emailed to marketingteam@cryptopia.co.nz
- Please ensure you have filled in 'Categories, 'Subcategories' and 'Transaction Details' correctly before assigning to App Support, and changed the title to match the format on the 'Triage' page.
- Always propose solution unless it's not a real customer interaction/spam, or is a duplicate ticket. Duplicates and spam tickets can be closed instead of resolved.
- Please resolve all 'Awaiting info' tickets after 48 hours - Please notify the user that their tickets will be resolved as we have not heard from them (they have 2 weeks to reject the resolution and provide us more info).
- Always respond to a ticket before attaching to a problem.
- If an email ticket is sent from an address not registered to Cryptopia, you won't be able to assign a ServiceNow contact, and none of the user's replies to your emails will attach to the ticket. Do not leave these tickets in awaiting info unless you are checking the Support Outlook inbox daily for their reply.
- Reply to email tickets using the email function if the user cannot log in to their account.
- Check each ticket for any attachments from the user.

Transactions

Cryptopia users are able to Deposit, Withdraw and Transfer in and/or within Cryptopia.

Deposits

When depositing into Cryptopia, you need to generate an address for the coin you would like deposit. This address is a unique set of numbers for funds to be allocated to you from Cryptopia's wallets.

At Cryptopia for each coin you generate an address once, and this then always remains the same. You can generate an address from your 'Balances' page of your 'Deposits' page (see figure 15).

Figure 15 – Address creation from 'Balances' page.

Figure 16 – Addresses can be created when selecting 'Deposit' in dropdown bar

33

126

CryptoNights

Cryptonights and other privacy coins require an additional 'Payment ID' (CryptoNight coins) or Message (XEM, BIS), in addition to your 'Deposit Address', in order to be received and deposited to your Cryptopia account. If an extra field is required for a particular coin, it will be shown on your Deposit page for that coin, together with your 'Deposit Address'. https://www.cryptopia.co.nz/DepositHistory

Figure 17 – Examples of CryptoNight coins

We do not accept encrypted payment IDs, as we cannot see which user's account to allocate the funds to.
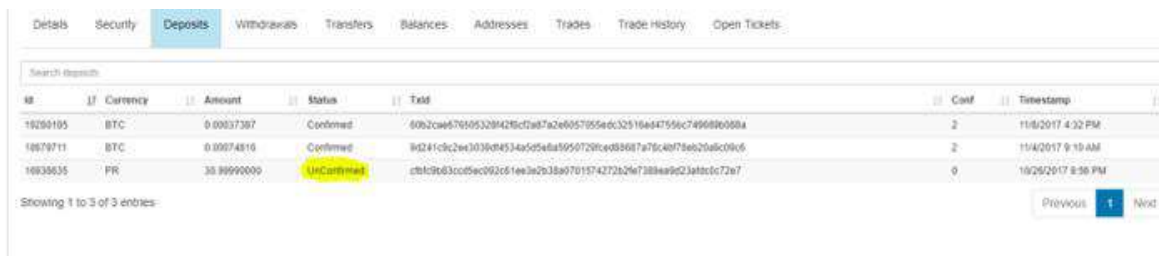
- Unconfirmed Deposits
- Wallet is in maintenance/delisting
- Wallet may have crashed
- The wallet may have no connections
- Cross-chain deposits
- No Payment/Message ID/Encrypted
- Smart Contracts
- Multisig
- Multi-Output
- Others

Unconfirmed Deposits

Deposits that do not have the required amount of confirmations on the blockchain (set by Cryptopia) remain unconfirmed. They need to reach the required number of block confirmations before the transaction is completed, allowing the funds to be credited to the user's account. This number can be as low as 2 (Bitcoin) or as high as 1440 (CoffeeCoin). The number is dependent on the speed and security of the network.

Sometimes the deposit remains unconfirmed if we have had technical difficulties (i.e. our Deposit tracker stops working), the wallet does not have connections, or the wallet is behind in block height (see figure 18).

Figure 18 – Unconfirmed deposit as shown in user's deposits page in Admintopia

35

Wallet is in maintenance

When a wallet is in maintenance, no deposits or withdrawals, or creation of new addresses can occur (see figure 19). The markets for that coin may also be paused. A wallet may be put into maintenance for many reasons. It may be due to technical difficulties experienced with the wallet, a scheduled maintenance for an upgrade, or a coin developer may request for their coin to be put into maintenance.

Figure 19 – Wallet in maintenance status message

Wallet has crashed

When a wallet is showing '0 connections' and '0 block height', this means that the wallet may have crashed due to technical difficulties (see figure 20). Customers are still able to create addresses (but not have their deposits or withdrawals go through) if the status of the wallet does not get put into maintenance.

Figure 20 – Wallet showing 0 connections and 0 block height

Wallet may have no connections

The lack of connections is due to the lack of nodes required from the community (see figure 21). These connections are randomly formed by nodes. Nodes are generated by wallets and exists as an IP addresses that power the Peer-to-peer network, allowing transactions to be posted to the network. When there are no connections, Cryptopia will not be able to verify incoming deposits. The status of a wallet has to be set to 'No Connections' for addresses to not be created.

NZed (NZDT)	★★★★★	None	Asset	Connections: 0	0	Offline ⓘ	Active	
ContractNet (CNET)	★★★½☆	Ethash	POW	Connections: 0	236498	OK	Active	Geth/v5.0.0
Feathercoin (FTC)	★★★★★	NeoScrypt	POW	Connections: 0	0	OK	Active	

Figure 21 – Wallet showing 0 connections.

A coin can lose connections for 2 reasons:

- The Proxtopia for that coin has crashed (most likely when the coin is still active)
- The coin has been slowly dying and nodes are getting switched off and people have stopped mining.

Cross-chain Deposits

When depositing into Cryptopia, the user's address needs to be correct. If somebody sends their coins to the wrong coin's address, they lose their coins 99% of the time. Sometimes they send their coins to a valid Cryptopia address that they own, but they use an address for the incorrect currency. This is a cross-chain deposit. These transactions can usually be recovered, however we charge a 10% recovery fee as it takes up time and resources.

These often happen when there has been a coin swap and the user has made a deposit of the new currency into the old coin address. The transaction goes through because technically, the transaction is running off the same network.

No/Encrypted Payment/Message ID

Payment/Message ID is a transaction attachment that consists of 32 bytes (64 hexadecimal characters) or 8 bytes (in the case of integrated addresses). They are required for CryptoNight transactions, and deposits where the currency has a shared address.

The Payment/Message ID is usually used to identify transactions to merchants and exchanges: Given the intrinsic privacy features built into Cryptonights, where a single public address is usually used for incoming transactions, the Payment/Message ID is especially useful to link incoming payments to user accounts.

From time-to-time users forget to add their Payment/Message ID to their transaction, and this requires App Support to recover these coins. As this process can be time consuming, with a significant resource cost to Cryptopia, we charge 10% of the amount recovered.

When a Message/Payment ID is encrypted, we cannot read it and we will not know who the intended recipient of the funds is. Again, the process for recovering coins with an encrypted Message/Payment ID can be time consuming and the resource cost to Cryptopia can be significant resource cost to Cryptopia, therefore we charge 10% of the amount recovered.

Note: the amount deposited will be shown in full in the history of the user, and the 10% charge will show up in transfers.

Smart Contracts

A Smart Contract is a computer protocol intended to digitally facilitate, verify or enforce the negotiation or performance of a contract (see figure 22).

Figure 22 – How Smart Contracts Works

Figure 23 – Smart contract on the Ethereum Block Explorer

This is often confused with a Token transfer (which does not pose a problem to us). The token itself is a Smart Contract but the transaction is not (see figure 24). The key identifier is the token name below the address:

Figure 24 – Token transfer via a Smart Contract

Multisig

Multisig transactions require multiple private keys (signatures) to sign a single transaction (see figure 25). Multi-signature addresses require another user or users sign a transaction before it can be broadcast onto the block chain. For example: when Alice wants to pay Bob, she sends a transaction to a multi-signature address, which requires at least two signatures from the group "Alice, Bob and Trent" to redeem the money. If Alice and Bob disagree on who should get the money (Alice wants a refund, whilst Bob believes he fulfilled his obligations and demands the payment), they can appeal to Trent. Trent grants his signature to Alice or Bob, so one of them can redeem the funds.

Figure 25 – A multisig transaction on the NEM block explorer

133

Multi-output

A multiple output transaction is exactly what is sounds like - several outputs take place within the same transaction (see figure 26). Our system does not support more than one deposit from a single transaction ID (hash), which is why a multiple output transaction is likely to fail.

If there are multiple deposits attached to one hash, our system can only recognize the first deposit. This is common when sending directly from a pool or third party. This is often done to avoid having to pay fees across multiple transactions.
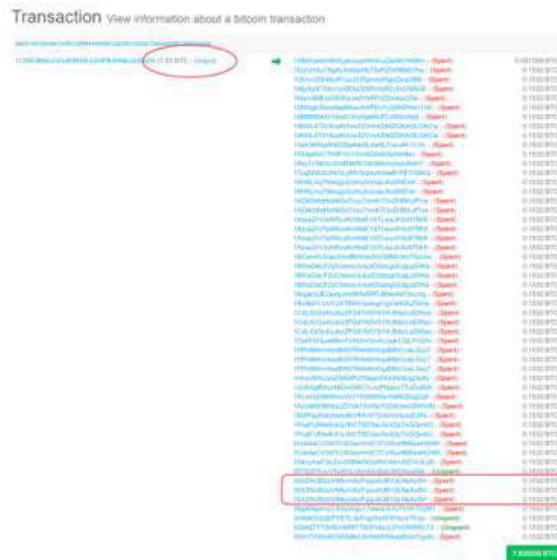
Figure 26 – Multi-output transaction

Others

Invalid Deposits

At the time of writing, invalid deposits only occur in XEM deposits, due to a monitoring service checking all transactions after 534 million USD worth of XEM were stolen due to a hack attack on Coincheck, one of Japan's largest cryptocurrency exchanges.

The XEM stolen funds monitor is now disabled – As XEM couldn't keep up with the speed of payments to make checking viable.

| 35820113 | XEM | 1000.00000000 | Invalid | 86b7c708ba3e3bad2ca6cc8f10997626835c0b5e55cb613cc5e44f3b8e83bdbd | 9 |

ERC20 Tokens

ERC stands for Ethereum Request for Comments. This is an official protocol for proposing improvements to the Ethereum network. '20' is the unique proposal ID number.

ERC20 defines a set of rules which need to be met in order for a token to be accepted and called an 'ERC20 Token'. The standard rules apply to all ERC20 Tokens since these rules are required to interact with each other on the Ethereum network. These tokens are blockchain assets that can have value and can be sent and received, like Bitcoin, Litecoin, Ethereum, or any other cryptocurrency.

The difference between these tokens and a standalone currency like Litecoin is that ERC20 tokens piggyback on the Ethereum network, hosted by Ethereum addresses and sent using Ethereum transactions.

Users often think that Cryptopia accepts all ERC20 tokens but this is not true. We only accept ERC20 tokens that have been listed. In many cases we can recover tokens that have been mistakenly sent to our ERC20 based wallet as a result of user error. As this process can be time consuming with a significant resource cost to Cryptopia, we charge a flat fee of 0.3 ETH which must be paid in advance.

Valid Transaction IDs

Users must provide us with a valid transaction ID for us to investigate any missing deposits. If we do not have a valid transaction ID or if is not showing on the block explorer, the sending wallet/exchange may not have successfully broadcast the transaction id on the network. Customers will have to update their sending wallet or contact the other exchange for more information.

Orphaned Deposit

When a new block is found, and it contains a deposit, X, we write it into our database as Unconfirmed. As new blocks are found that build on top of this block, the number of confirmations rises.

However, the chain can go in multiple directions at any one time: maybe the network becomes split apart and each half doesn't know what the other is working on. Let's say our new deposit was in chain A and it became 3 blocks longer. The other half of the network was faster at finding blocks, so a different set of transactions are confirmed and that head of the chain (B) has 5 blocks on top of the common ancestor block. When the network joins together again, consensus is sought so there is only one chain; usually longest wins, so every transaction in Chain A (including the deposit we saw) is erased from public memory; all transactions in chain A never happened (hence they're "returned" to their wallets- they never left)

This chain splitting process is the reason why some coins required 200+ confirmations: for some less established networks, they split often and are subject to a lot of rewinds, so we insist that at least 200 blocks have built on top of the block containing the deposit. This is to be sure that it's not going to get spontaneously unwound at some point. It's important to appreciate that we operate more like a bank; we don't use the public ledger (block explorer) to track which of our users have coins in their accounts - we just see a deposit of 1 BTC by user x to their address here, we give them a record in our database saying "this user has 1 BTC available" and we let them swap and trade it around (which is purely incrementing and decrementing numbers in our records, no blockchain transactions) and if the user asks for a 1 BTC withdraw, it's some other random BTC we give them back - just like if you deposited $1000 in the bank then a week later took $20 out of the ATM - the note you are given is probably not one you deposited

[This causes users some confusion too: they deposit their 1 BTC and they can see that it has reached "their address" on the blockchain, but a couple of days later we sweep all the transactions into one of our exchange wallets (for operational/performance/security reasons). They may accuse us of stealing their money. In reality, they transferred the BTC to us and we made a promise (inputted a balance of 1 BTC on their Cryptopia account) that upon demand they could have 1 BTC back (it'll come from a different place, and isn't anything to do with the one they deposited) The sweeping process collects tiny fractions of bitcoin dust and consolidates them back into large amounts. It costs more to pay someone in fractions than whole amounts because lots of tiny fragments increase the transaction size. In a real-world analogy, it would cost more to pay for a car using 20 cent coins than if you wrote a cheque for the exact amount because you'd need 25,000 coins to buy a $5,000 car - it's going to take all day to count the change. Handing over a cheque for five grand takes seconds. If you charge for your time (like bitcoin miners do, effectively) then you would have to pay an extra 100 dollars in counting fees. We periodically take all the small bits, add them up, and transfer it to ourselves to consolidate the amounts to a single lump sum.]

It's easier for us to just insist on a number of confirmations that we're confident won't ever get unwound, than it is to constantly monitor the block explorer for orphaned transactions. We'd end up seriously out of pocket if we promised someone we'd pay them a BTC on demand as a result of initially seeing deposit X, without waiting to check if it is not valid. We would essentially have a greater BTC liability than we would have BTC to meet it.

User's wallet is not fully synced to the network

If the user's wallet is not fully synced to the network then the transaction will not be broadcast to the block explorer. The user may also need to update to the latest wallet version. We need the user to provide a valid txid that is on the block explorer to credit their coins to them.

Different coin, same ticker

Some coins use the same ticker which confuses users. For example, we list BatCoin (BAT), but other exchanges list BasicAttentionToken (BAT). If they use compatible blockchains users will sometimes make deposits of a coin that we don't list that shares the same ticker - this is a cross chain deposit which we can recover for the user at a fee of 10%.
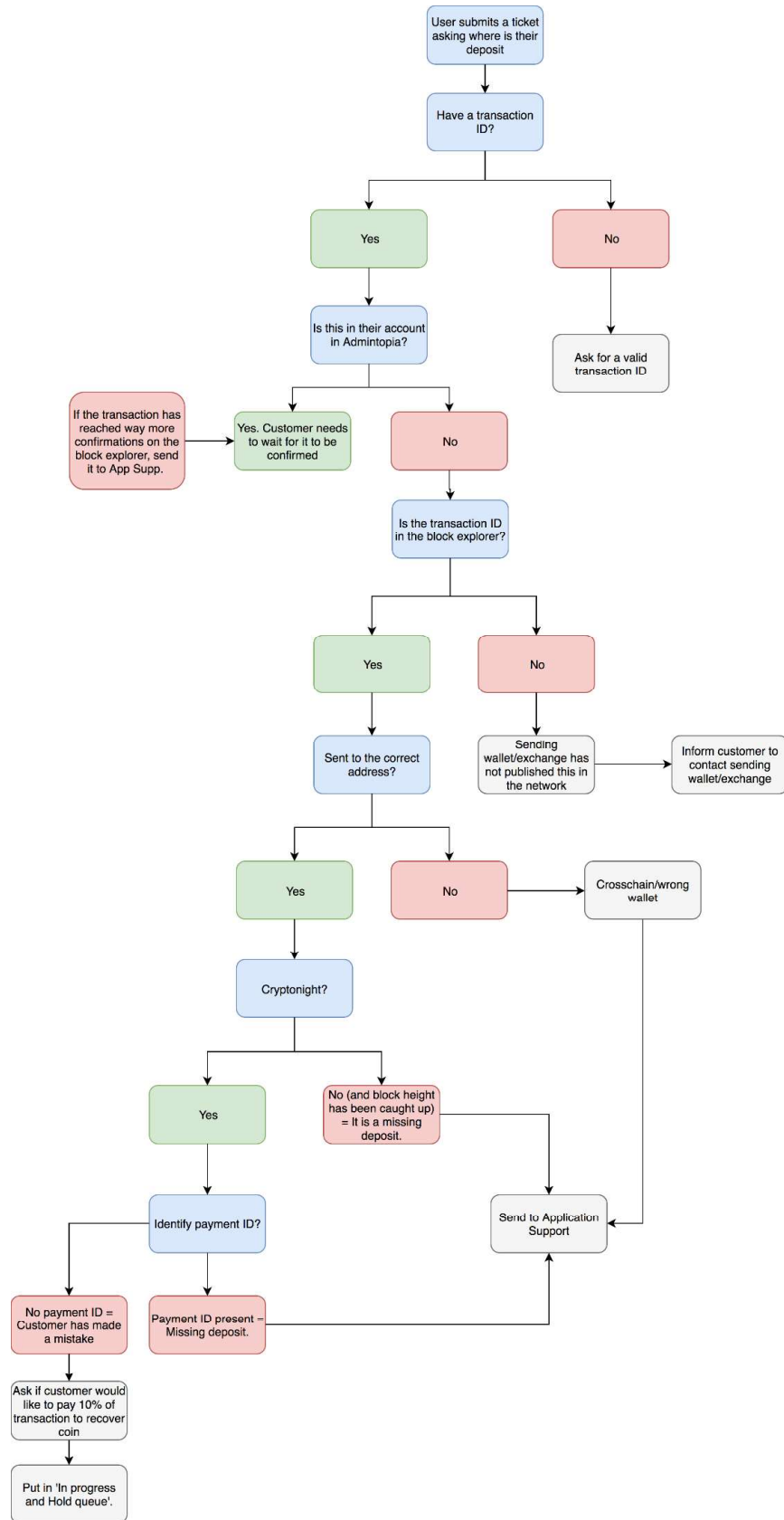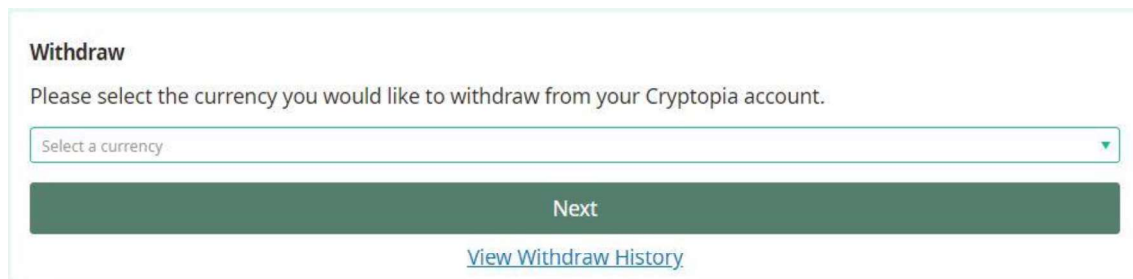
Figure 27 – Diagnosis of a deposit ticket (with the main reasons taken into consideration)

Withdrawals

Cryptopia users are able to withdraw funds stored in the exchange to an external wallet/exchange.

Status of Withdrawals: 1. Unconfirmed, 2. Pending, 3. Processing, 4. Complete

Pending - not yet picked up by the processors. Processing, picked up by the processors, and not complete.
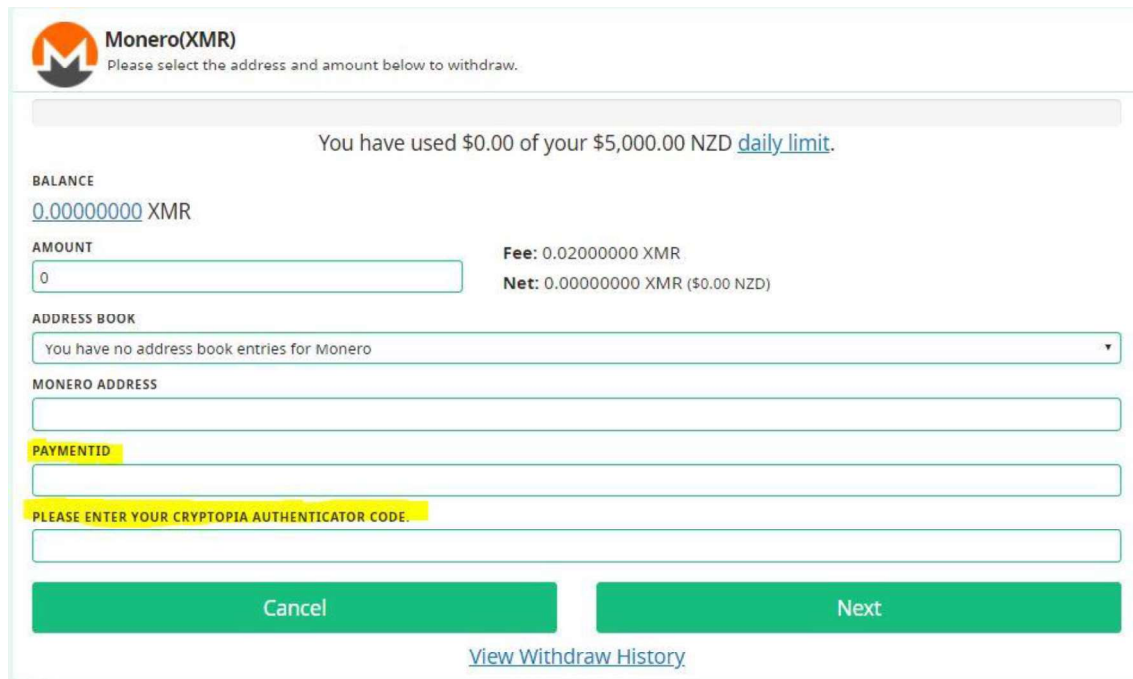
Figure 28 – Selecting a currency for withdrawal

Figure 29 – Cryptonights require payment IDs when depositing into an exchange

Why would a withdrawal not show in a customer's external wallet/account?

- Withdrawal is unconfirmed
- Wallet is in maintenance/has 0 connections
- Withdrawal is stuck in processing
- Withdrawal has not been published to the network
- Others

Withdrawal is unconfirmed

User has not confirmed the transaction via their email and still needs to click 'Confirm Withdraw' link in their email.

	Id	Currency	Amount	Status	Confirmed	TxId	Address	Conf	Timestamp	Init
Details Security Deposits **Withdrawals** Transfers Balances Addresses Trades Trade History Open Tickets										
	1099280	OMG	0.03000000	Unconfirmed			0x366ea033470c6ab6d6eca77c3e...	0	11/9/2017 8:08 AM	UI
	1075143	NZDT	4102.00000000	Complete	11/5/2017 7:49 PM	rkDQD13NdDykfPAiA2mnD9dUPo...	02-1246-0406451-001	0	11/5/2017 7:49 PM	UI
	769146	NZDT	26.00000000	Canceled			0602570264327:daroll	0	9/6/2017 10:08 PM	UI
	593113	BTC	0.01000000	Complete	8/4/2017 8:35 PM	42a0c3b1d60e78ba2ff31caca6982...	1Eu3broZvMT4Jj3L1nKva5vyjE2ec...	0	8/4/2017 8:35 PM	UI
	511048	NZDT	102.00000000	Complete	7/17/2017 3:19 AM	yMoNNRANTxUcdMf7qJaWNjzpe...	02-1246-0406451-001:Rob Smells	0	7/17/2017 3:19 AM	UI

Figure 30 – A user's unconfirmed withdrawal in the withdrawals tab in Admintopia

Withdraw Confirmation

Hi DaRoll,

You have a pending withdraw awaiting confirmation.

IPAddress: **111.69.178.9**
Amount: **0.03000000 OMG**
Address: **0x366ea033470c6ab6d6eca77c3e378f89cfca20ce**

[Confirm Withdraw]   [Cancel Withdraw]

If you did not initiate the above withdraw we recommend you lock your account, this lock will expire after 24 hours and cannot be bypassed by Cryptopia Support:

[Lock My Account]

Email links can expire, and they might need to resend the email, which they can do via their Withdraw History (see figure 31). Users can also cancel their transaction through the same place. https://www.cryptopia.co.nz/WithdrawHistory

Withdraw History

#	Currency	Amount	Fee	Status	TransactionId
3355043	DOT	274.94857142	0.00000000	Unconfirmed	Resend Email Cancel

Figure 31 – Resend withdrawal email

Wallet is in maintenance/has 0 connections

Similar to deposits, withdrawals do not get processed if a wallet goes into maintenance or has 0 connections (see figure 32).

Figure 32 – Wallet in maintenance

Withdrawal is stuck in processing

If everything goes to plan, a withdrawal should go from pending to complete in just a few minutes. If it does not get completed, the withdrawal does not get published to the network and will not be assigned a TxID. These transactions will need to be passed over to App Support to be manually processed.

Figure 33 – A withdrawal in 'Processing' status

Withdrawal has not been published to the network

If the withdrawal has not been published to the network, it will not show up on the external wallet/exchange. These transactions will need to be passed over to App Support to be manually processed.

Others

Orphaned transactions

See explanation for 'Orphaned deposits'.

External Wallet/Exchange issues

Like the issues we may experience when a deposit comes into Cryptopia, other exchanges may also not immediately process deposits. Once the transaction has been published to the network and is visible on the block explorer, there is not much we can do, and the user will need to contact the receiving exchange for assistance.
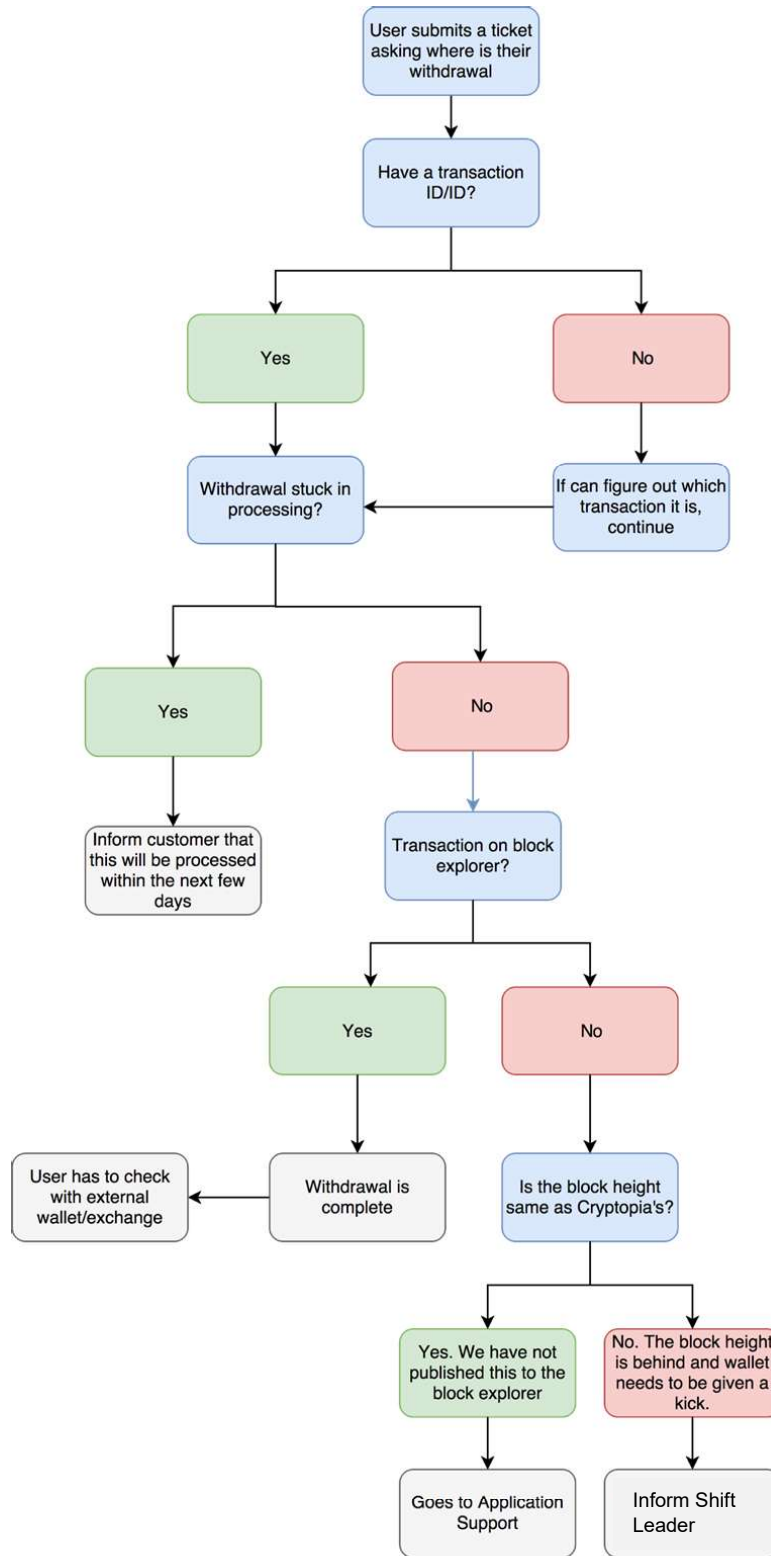
Figure 34 - Diagnosis of a withdrawal ticket (with the main reasons taken into consideration)

Transfers

Transfers are transactions between two Cryptopia users where the funds do not leave our site and the transactions details are not published to the block chain (see figure 35).

There are no transaction fees associated with transfers – users will often not realise that this function exists and use the withdrawal system, which leads to withdrawal issues. For example, if a privacy coin is withdrawn from one Cryptopia user to another, the sending and receiving address will be the same. This confuses our deposit tracker, and it will often miss this.
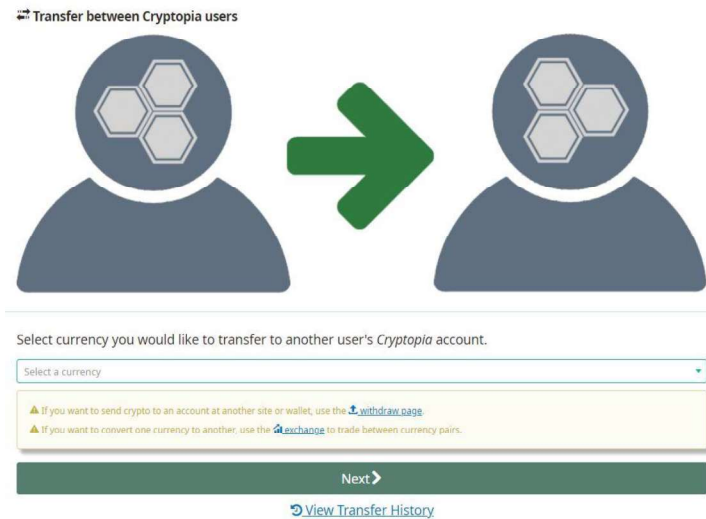
Figure 35 – Transfer function between Cryptopia users
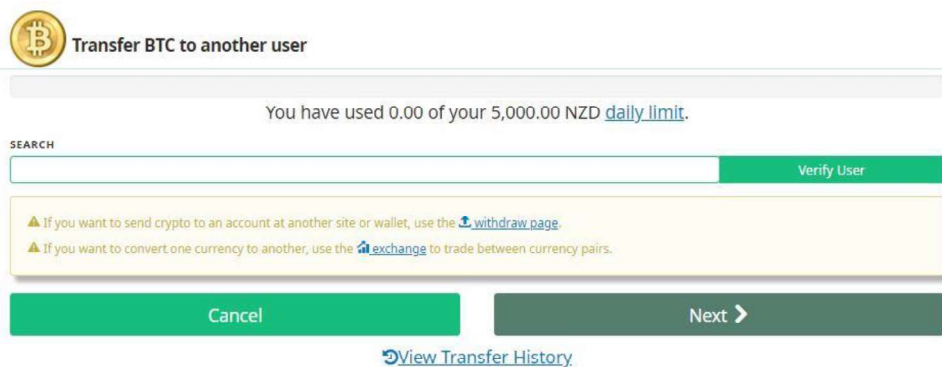
Figure 36 – Transfer function after selecting currency

The Transfer History (see figure 37) lets you see all the transfers associated with your account (both sent and received) - https://www.cryptopia.co.nz/TransferHistory

#	Currency	Amount	Fee	Type	Sender	Receiver	Timestamp
15366823	USDT	0.97716827	0.00000000	CEFS	CEFS_USER	noxccc	1/04/2018 1:25:00 PM
15366822	NZDT	0.02830357	0.00000000	CEFS	CEFS_USER	noxccc	1/04/2018 1:25:00 PM

Figure 37 – User's Transfer History

Trades

On the exchange users can trade or exchange one coin for another by creating a buy or sell order.
Trading happens through the web interface (Cryptopia.co.nz - for humans), and API (for bots), and each day a large volume of cryptocurrencies are exchanged via our platform.

Helping our users learn how to trade and making sure they are able to trade is important because it is our primary source of income.

API
Application Programming Interface

English: It is robot language for professional trading bots.

Types of API
Public: enables users to get public information

CoinInfo (names of coins, maintenance, etc.)

Current market rates & order books, history

Private: enables users to send/receive private information. Requires an API key...

Set buy/sell orders

Withdraw/transfer

It is worth noting that API trades account for 90% of orders on our site, and the 'whales' (big traders with a lot of money) nearly exclusively use the API. Extra consideration should be given to API tickets for this reason.

Refer to hand out for commonly asked questions and answers.

Application Support

Checking information

SQL (Structured Query language)

Talula (remote database log-in)

Figure - App support

App Support (AS) is about fixing mistakes. Not only are we dealing with users' money, we are also dealing with their confidence and sense of security in Cryptopia.

AS has zero tolerance for errors. AS must always recheck any information provided by the CS team. If AS notice any frequent errors they need to be reported to CS Shift leaders. AS will remedy any errors before processing a ticket.

Remote Database Access

Our data base access is remote, access will be provided infrastructure and is secure. Security and focus are key when accessing the DB.

Remember to sign out when done!

Stored procedures

These are like the action templates for AS. They are written in Structured Query Language (SQL) and are used to solve problems.
The Database is made up of tables where all our users' information is stored,

The **Stored Procedures** were written with SQL and stored in the database.

These **Stored Procedures** are the 'templates' used by AS to solve problems.

Actioning **SP**s means you are changing parts of the database.

Every Actioned **SP** is recorded – so nothing goes unnoticed.

The contents of the SP changes depending on
the parameters needed for the Statement.

USE Cryptopia ──────────────────────→ This is the database that we Query.

exec dbo.**AS_CancelIncompleteWithdraw** ───→ This is the Name of the SP
  @ASUsername = '**ThisBeYou**',
  @Username = '**UserUser**',
  @CurrencySymbol = '**CoinCoin**',
  @WithdrawId = **999999**,
  @Address = '**WithdrawalAddress**',
  @Amount = **Float** ──────────────────→ This is the Amount of Coin
  --@TicketId = 9999999

Ticket ID is no longer required
'--' before a line prevents the command to run

Figure – example of a stored procedure

Types of withdrawals App support process:

Stuck in Processing
AS_CancelIncompleteWithdraw

What to check before running SP:

Wallet Status (not in Maintenance & is connected)

TX is not at the Withdrawal address on the block chain.

[Check for Withdraw issues in Admintopia and JIRA if necessary]

Check Query to see if the deposit has attempted to leave the wallet or not: [*0= never ft wallet*]

Processing time is >48 hours

Processing - Already Broadcasted
AS_CompleteProcessingWithdraw

<u>What to check before running SP:</u>
The TXID is not already in the user's withdrawals.

The Coin/token, and time stamp is consistent with the Withdrawal

<u>After running the Stored procedure:</u>
Reply to user with the generated response
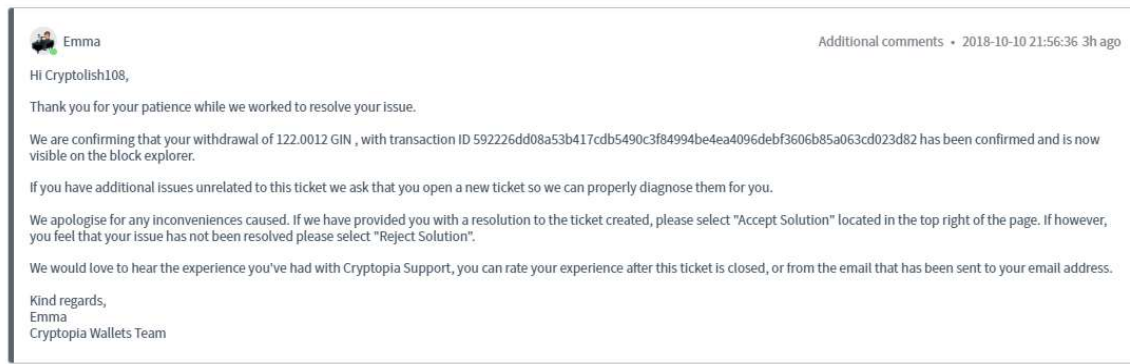
Needs Reprocessing
AS_UpdateWithdrawalStatus

<u>What to check before running SP:</u>

TXID is **not** at the Withdrawal address on the block chain.
Check that the funds have not left the wallet:
(WithdrawalAuditQuery)

Types of deposits App support process:

Cross Chain Deposit
AS_CrossChainRecovery

<u>What to check before running SP:</u>

Information provided is correct with the address the deposit went to.

Not showing in their balances.

Multi Sig/Smart Contracts
AS_InsertDeposit

Contract 0xd4f5bf184bebfd53ac276ec6e091d051d0ed459e ✓

└ TRANSFER 0.5 Ether from 0xd4f5bf184bebfd53ac276... to → 0x5fc189f406d39434348c6...

What to check before running SP:

Check amount and address is correct on the block explorer (see internal Transactions).

Use dbo.AS_InsertDeposit Stored Procedure to credit the user their funds.
Tell a peer you are inserting a deposit

Missing Deposits
Rescan Wallet from X block

Steps to take:

Find the block number or hash for the block you want to scan back to (on the explorer).

Reset last Block hash to this hash in the SP

Show notes that say what you have done (in case something weird happens).

Keep an eye on the wallet after scanning!

Multi-output Deposit
AS_UpdateDepositAmount

Steps to take:

Find the transaction on the block explorer:

Search by address inputs:

Use the *AS_UpdateDepositAmount* Stored procedure.
If it is USDT → BTC remember to add '-USDT' to the end of the TXID

Missing payment ID/message
AS_InsertDepositNoPaymentIdProvided

Coins that need a payment ID (ETN/SUMO etc):
We recover these coins by allocating them to users' accounts, for a 10% fee.

Steps to take:
To check whether the deposit has reached our wallet we need to access the wallet and query it to see if the coins have successfully reached us.

If you are given wallet access you will be shown how to do this.

The risk is that you might accidentally crash the wallet.

Coins that need a Message payment ID (XEM/LYL):
We recover these coins by allocating them to users' accounts, for a 10% fee.
Sometimes we need to ask the user to L2 Verify themselves before inserting the deposit i.e. EOS missing deposits.

Steps to take:
Check the user's account was made after the missing deposit is claimed.

Check the TXID in Admintopia deposit history (across all users) to make sure it has not already been deposited to someone else.

Deposit recovery

We *can* recover ETH tokens that we don't have listed by logging on to the ETH wallet.

We charge 0.3 ETH to recover these tokens.

Account audits

We use the Print Audit mostly for tickets where users complain that their balance is incorrect.

It shows where all the funds of a particular coin type are in their account.

	Title	Result
1	Full BTC Audit Result	
2	Deposit	0.05710212
3	TradeIn	0.04168611
4	TransferIn	0.00000000
5		
6	Withdraw	0.00000000
7	TradeOut	0.09874711
8	TransferOut	0.00000000
9		
10	Total	0.00004112
11		
12	Deposits Unconfirmed	0.00000000
13	Held For Orders	0.00000000
14	Pending Withdraw	0.00000000
15		
16	Available	0.00004112

Jira

Jira is where wallet issues are managed.
Any wallet issues found by a CS agent needs to be escalated to a Shift leader to investigate and potentially create a Jira ticket.

You can search using the 🔍 to find out what is happening with any coin ie.
Searching for ''DOGE'' will find all the DOGE JIRA tickets.

Forks, airdrops, and swaps

What are forks?

Blockchains start at a defined 'Genesis block'. When new blocks are mined they point to a parent block (see figure 38).

The "blockchain" is defined as the longest possible chain of blocks leading to the Genesis block.

Sometimes, multiple miners will mine blocks at the same time, pointing to the same parent block, resulting in a block with multiple children blocks, or a fork (see figure 39). This is 100% normal and expected in the operation of a blockchain. The network typically chooses one side of the fork and other side becomes "Orphaned".

Figure 38 – Blocks on the blockchain pointing towards the parent block/previous block

Figure 39 – Mining blocks at the same time results with multiple children blocks or a fork

What is consensus?

Consensus is a strict set of rules that all nodes on the network follow to determine if a new block is valid.

For example:

- A block must point to a previous valid block (valid due to these rules)
- A block must only contain valid transactions.
    - Transactions must spend coins which previously existed
    - Coins must only be spent once.
    - Transactions must be cryptographically signed by the correct address of the coins.
- A block is allowed to contain one transaction that creates coins out of thin air (the so-called miner reward).
    - This transaction must have a correct miner reward value for that block height
    - It may be sent to any address.
- The block (and all the transactions in it) must be less than 1MB (however this varies across coins and some coins can even vary the block size dramatically).

Nodes check each block (and the transactions inside) as they receive them against these consensus rules and reject any blocks which don't pass as invalid.

Deliberate forks

Sometimes developers need to change these consensus rules in order to implement new features.

These updated consensus rules are supplied in software updates, and are normally implemented so they only apply after a certain block height or date.

There are two types of forks: Soft and Hard forks

What are soft and hard forks?

The difference between a **soft** and **hard** fork lies with how they change consensus. Soft forks **restrict the current set of rules**. New created blocks will abide by more limits.

A soft fork is **backwards-compatible,** and the **miners** are the players that decide whether it is used. The users and merchants can keep using the old rules (old software), but it is recommended that they do the upgrade.

To borrow from a video from Andreas M. Antonopoulos, a soft fork is like a vegetarian restaurant deciding to go vegan. All the customers (vegetarians) can eat the new (vegan) meals without problem.

A **hard fork** occurs when a new feature or set of new features are developed and they **drastically modify block acceptance rules**. After being pushed to a cryptocurrency project, **everybody (miners, users, merchants, etc.) has to upgrade.**

Consensus rules are relaxed or outright changed in such a way that old software sees the newly mined blocks as invalid (see figure 40).

Hard forks are **not backwards-compatible.** People using the old rules/nodes will end up on a different fork of the blockchain that does not include any correct blocks.

To borrow from the same video as before, a hard fork is like a vegetarian restaurant deciding to now include meat with their meals. All the customers (vegetarians) cannot eat the new meals unless they decide to change to meat-eaters.

Some communities go out of their way to only utilise soft forks as a way to preserve backward compatibility.

Many communities, like Ethereum and Monero not only embrace hard forks, but schedule them on a regular basis as the primary method of updating.

90% of coins usually go through a hard fork or use hard forks to update consensus.

95% of the time, the original fork of the chain dies off and is forgotten and coins on that fork become worthless.
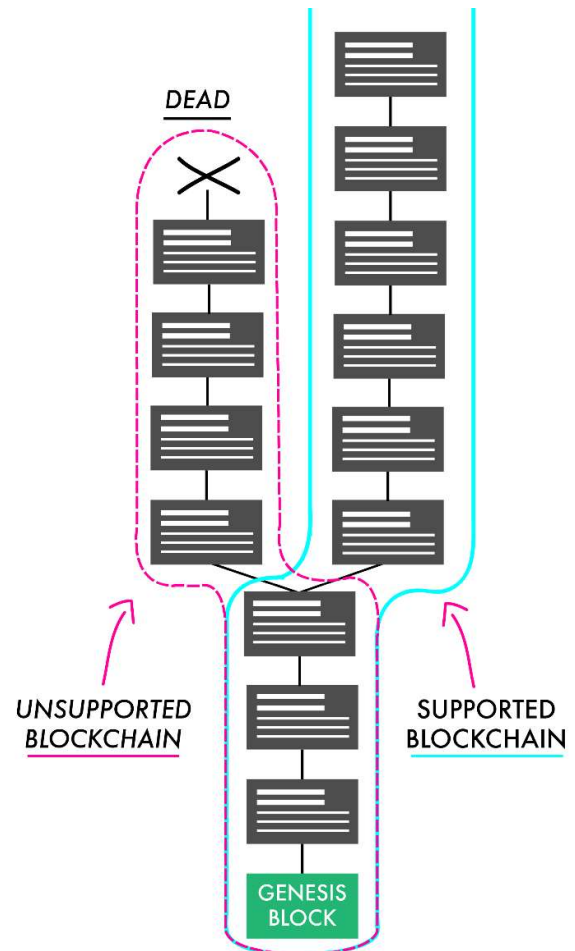
Figure 40 – Forking and the supported blockchain versus unsupported

What happens when both sides of the fork survive?

While hard forks and soft forks are common, as coins go through their normal update procedures, normally only one side of the fork is supported and active.

However, sometimes competing communities make an effort to keep both sides of the fork alive. For example, Bitcoin and Bitcoin Cash; Ethereum and Ethereum Classic; Monero, Monero Classic and Monero V.

In this case, anyone that has held the original currency (in their personal wallet) at the time of fork will have both currencies after the fork.

Going back to our diagram, both sides of the fork survive, both blockchains share a common history, and both chains are 'worth something' (see figure 41).
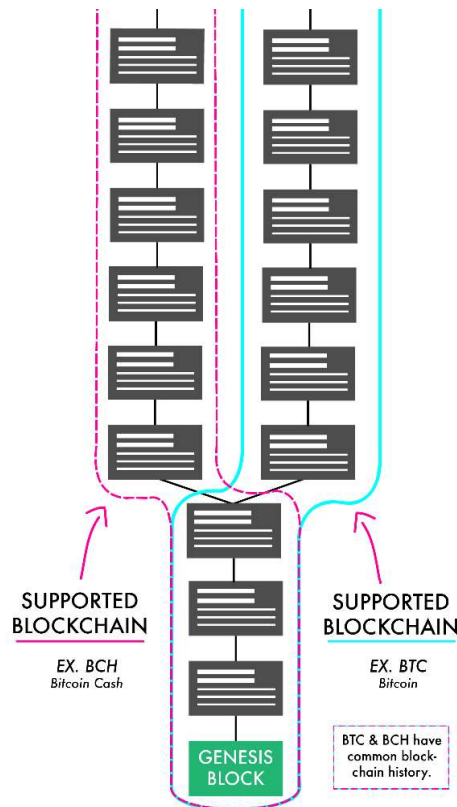
Figure 41 – When both sides of the fork survive, e.g. BTC and BCH

What are airdrops?

Airdrops occur when cryptocurrency users are **given free coins/tokens automatically** due to their holdings of other currencies (or in return for performing certain actions).
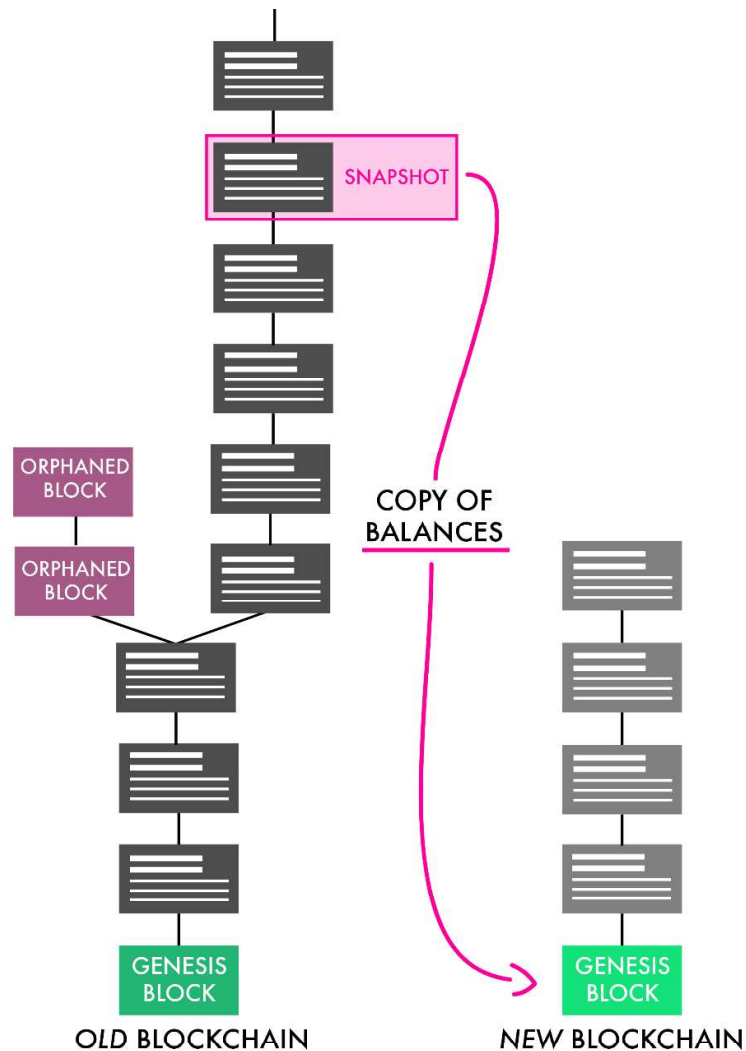
Figure 42 – A snapshot is taken when an airdrop occurs

They are largely used to promote and incentivize use of a cryptocurrency, which is especially valuable in the early stages after a launch.

In their most basic forms, airdrops achieve the same effect as forks where both sides of the chain are supported, anyone who held the original currency at the time of the airdrop will have both the airdropped and original currencies.

However, airdrops use a completely different mechanism where they snapshot the balances of every single address on the original blockchain, and send the appropriate amount of the airdropped currency to each address on the new blockchain (see figure 42).

The original and new blockchains are 100% different, except for the copying of balances.

61

What are coin swaps?

A coin swap is used by developers of a cryptocurrency project when they want to move users from one blockchain to another.

Coin swaps are usually done when the developers behind a project want to port their token to a newer version of the same blockchain. There may be problems with the initial blockchain, or the developers simply want to make a significant change to the software and protocols behind the project.

A swap is opt-in by the **user.** Typically, the user will initiate the swap by sending their old coins to an address, which are then **burned** (destroyed forever) in exchange for coins from the new blockchain - at a consistent, predetermined rate.

Swapping is a permanent process. Once a coin is swapped and burned, it can't be redeemed back on the original blockchain.
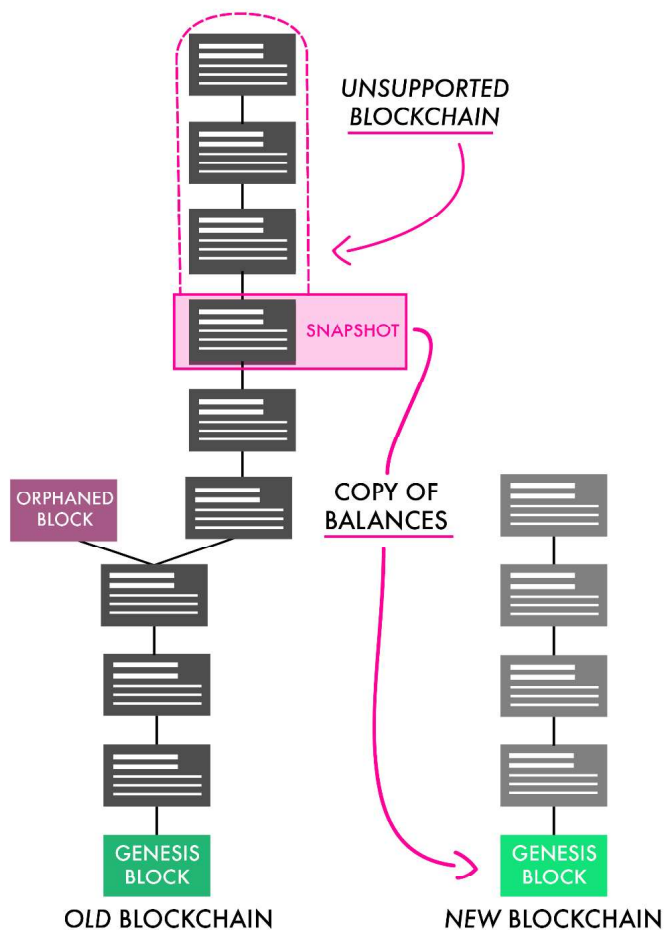
Figure 43 – Coin swaps are similar to airdrop. However the old blockchain is no longer supported.

Coin swaps are essentially the same thing as airdrops, except the old blockchain is no longer supported, and the new blockchain is declared to be "the same currency" (see figure 43).

Unfortunately, coin swaps interfere with Cryptopia's internal systems, as they expect the full transaction history of all deposits to be untouched during upgrades.

We recommend currencies avoid unnecessary coin swaps, and modify the consensus rules of the new codebase until it accepts the old blockchain. Then we can apply this as a simple update for free.

2 coin swaps that Cryptopia has done in the past:

- **Old DOT > New DOT**
- In September 2017, DOT (originally a mineable cryptocurrency) was affected by a 51% attack. We managed to identify and respond to the attack quickly, covering the lost DOT from our own reserves - however after this incident, questioned whether it still made sense for DOT to run on its own network.
- As the use case of DOT was not based around mining or proof of work - and we didn't think anything was lost in moving DOT to a token platform - we decided to perform a swap of the DOT blockchain to a Ubiq asset.
- We credited every holder of old DOT on Cryptopia, with new DOT - in a 1:1 ratio. Then we offered a 30 day window for people to swap their remaining old DOT held in external wallets. The coins were burned instantly after being swapped.

- **PAC Coin > $PAC**
- The development team behind PAC decided that they wanted to reduce the total supply of PAC, in order to reduce the amount of data in the PAC blockchain (allowing faster wallet sync times and making PAC more attractive to exchange listings)
- In order to execute this swap, the PAC foundation asked Cryptopia to help initiate it for our users (as well as creating their own coin swap procedure for PAC holders).
- Following the PAC foundation's direction, we issued a 1000:1 PAC > $PAC swap, assisting in shrinking the total supply from 100 trillion to 100 billion. Although this happened in early 2018, there will always be users who think they have lost their PAC.

Cryptopia does not typically support forks, airdrops, or coin swaps (unless stated otherwise) due to the inherent risks. We recommend that users withdraw their coins from the exchange if they wish to participate in these types of coin events.

Conclusion

Soft fork: a restriction of the block acceptance rules – backwards compatible - everyone using the current coin version are advised to upgrade as soon as possible.

Hard fork: a modification of the block acceptance rules - not backwards compatible - everyone using the current coin version has to upgrade before and after the fork.

Airdrop: when cryptocurrency users are given free coins/tokens automatically due to their holdings of other currencies (or in return for performing certain actions).

Coin swap: A coin swap is an airdrop in exchange for some proof of coins on the other chain (usually a proof of burn). Usually initiated by developers of a cryptocurrency.

Confluence

This is where we keep all our templated responses for answering tickets.
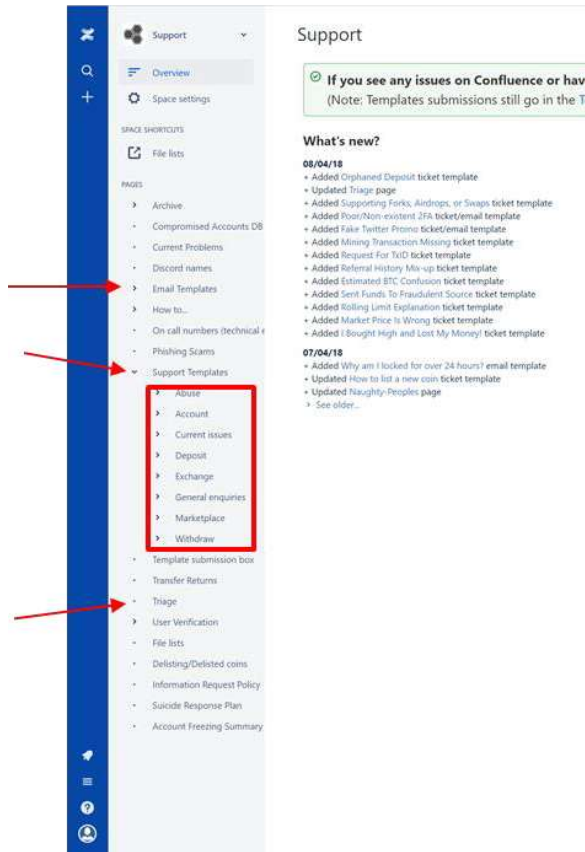
Figure 44 - Confluence

Using confluence templates

Templates can be simply copy and pasted into tickets, however we do need to greet the user and sign off. You may also need to fill in information which is formatted in _**BOLD**_.

Confluence – Triage

When escalating a ticket, we can use the templated responses under Triage.
We must change the ticket short description and include the required admin notes.

Figure 45 – Triage templates

Ticketiquette

We must respond to our users in a way which is formal and inviting. We can do this in the way we format responses, ensuring we are answering the user's question, by reading back over our responses and making sure our responses are consistent.

Basic rules of a response

Start positive – the opening paragraph should engage the user. The opening sentence should show the user you understand their situation.

Middle – Be as informative as possible, and if needed, ask for more information. If you need to give a rejection, make sure you include a reason.

While we do use templates, we should not just copy and paste. Before sending a reply, you need to read over your answer and check that it is relevant to the user. In a ticket with multiple issues, you can combine templates to fully address the situation. In other cases, it is helpful to use short answers to get a point across.

End on a positive note where possible - Asking users a question can make their experience more positive.

- Is there anything else we can help you with?

- Do you have any further questions in regards to this issue?

You can also offer further investigation of a user's issue – they will remember you going the extra mile for them.

Link users to the Help Centre (see figure 46) as required. This is useful in final responses as it gives users another point of reference and is a place they can find answers to many commonly asked questions.
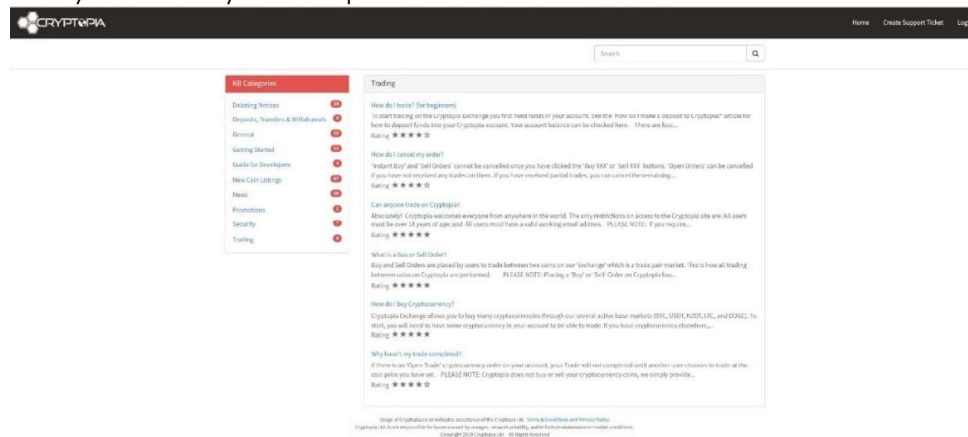
Figure 46 – Help center

159

Include phrases such as "We understand" and "we can assist you" – these are comforting to users.

Tone

You can understand how a user is feeling by interpreting the tone of a ticket. This will help you decide how to approach the user.

Always use formal greetings

Example:

Hi _username_,

Thank you for contacting Cryptopia Support.

Body text

Kind regards,

_your_name_
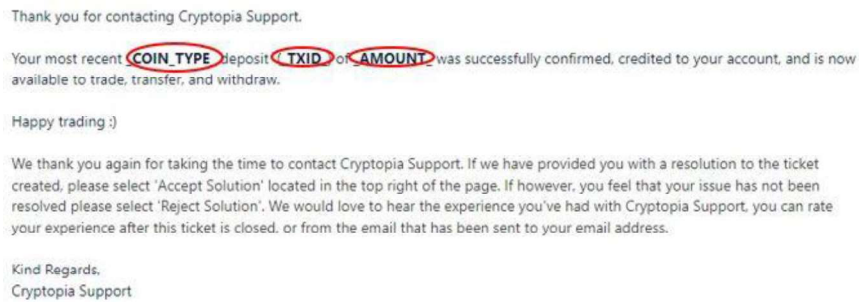
There are formal and casual ways to reply based on the context of the ticket. We can choose to be more "personal" with our users when they are frustrated, especially if you see they have already received a templated response for this issue. Instead of "We" the use of "I" will make the user feel like they are talking specifically to someone.

We should also always address the user with the name they have provided or their user name for example: "Hi _user_name_"

Fill in the blanks:

Check all copy and pasted responses for _blanks_.
Most blanks are shown in this format _word_blank_, these must be filled in before sending any response. Double check all tickets and emails. (see figure 47)

Thank you for contacting Cryptopia Support.

Your most recent **COIN_TYPE** deposit **TXID** of **AMOUNT** was successfully confirmed, credited to your account, and is now available to trade, transfer, and withdraw.

Happy trading :)

We thank you again for taking the time to contact Cryptopia Support. If we have provided you with a resolution to the ticket created, please select 'Accept Solution' located in the top right of the page. If however, you feel that your issue has not been resolved please select 'Reject Solution'. We would love to hear the experience you've had with Cryptopia Support, you can rate your experience after this ticket is closed, or from the email that has been sent to your email address.

Kind Regards,
Cryptopia Support

Figure 47 – Blanks in templates

Response check list:

- Have I answered the user's question/s?
- How would I feel if I got this response?
- Is this a solution or a band aid?
- Has the user accepted the solution?

Resolving complex cases:
Read through the ticket – decide if the issue is sensitive or touchy – if so you may need to make some major changes to templates – give a calm, clear and confident response – converse and raise to shift leaders for advice.

Multifactor Authentication

2FA strength level

Weak – These are static, so never change. They are vulnerable in the event of phishing or doxing.
Meh - Only effective if the email is set up with a strong 2FA. If their email is ever compromised then so is their Cryptopia account.
Strong - You need to physically have the device to access the code.
(see figure 48)

Weak	Meh	Strong
PIN	Email Code	Cryptopia Dongle
Security Question		Google Authenticator
2nd Password		Authy

Figure 48 – 2FA strength level

Types of 2FA

Email Code: the initial default 2FA setting for users' accounts. Users are emailed a code from noreply@cryptopia.co.nz which lasts for 15 minutes, so this is a form of One Time Password. It is more secure if the email address has 2FA set for login as well.

Cryptopia Dongle: must be activated by us. After purchasing the device from users need to contact verifications@cryptopia.co.nz for their device to be activated

Figure 49 – Cryptopia dongle

Google Authenticator/Authy: A third party authentication app which can be set up by the user. (see figure 50)
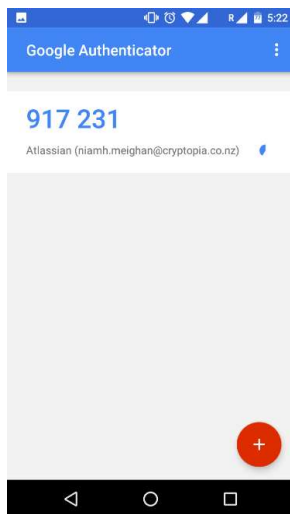
Figure 50 – Google Authenticator

162

Changing 2FA settings

Users can change their account 2FA settings. To change these settings all of their current 2FA needs to removed; this can be done by going to the security page https://www.cryptopia.co.nz/Security

Once the 2FA is removed a new 2FA can be set up.

Users will need to use their current 2FA to change any 2FA settings.
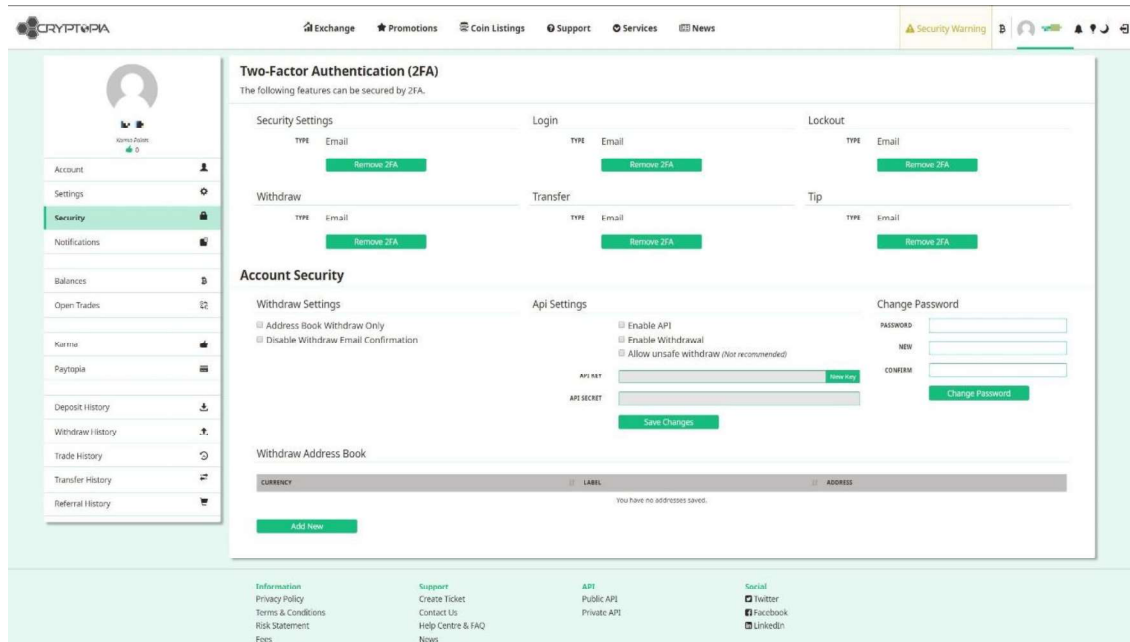
Figure 51 – Security page

Compromised Accounts

Overview

Customers will create tickets in ServiceNow that are usually under the **CSM – Triage** or **CSM – Compromised Accounts** category. Customer Service initially determines whether they have been compromised or if it is another issue, such as not being able to see their balances because they have "Favourites Only" ticked on their balances page. Users have created tickets about their compromised accounts with the following Short Descriptions:

Purchase Bunny Coin	My Account LINDA
missing Bitcoin ? check deposit and account details	lose my all payment
I havent authenticated any transfer. i lost my coins. I dont feel secure . On the same day i also lost my XVG coins Vide Transfer ID 15581770	I did not withdraw
Fraudulent Transfer	My wallet was stolen
some error from your system	Coins transferred without my knowledge

Figure 52 – compromised tickets

Ensure that you have thoroughly read the description, previous Activities, and checked for attachments to the ticket. The user may have updated their ticket with more information.

Figure 53 – Compromised account ticket

Potential compromised account scan

Check IP addresses under the Security tab to check for any abnormal logins. IPs can vary greatly if a user accesses their account from multiple locations, but most users will only login from one or two IPs. (See figure 54)

Figure 54 -Compromised account

Check withdrawals under the withdrawals page for any activity around the time of logins (see figure 55)

Figure 55 – withdrawals page

Check trade history under the Trade History page for any trading activity around the time of the withdrawal, there will often be multiple trades to one coin type in a short time.

Check Transfers under the Transfers tab for any transfers made around the time of any suspicious activity within the account.

Figure 56 – Trade history and Transfers

Naughty Man Transfers

If the user's funds were transferred to another Cryptopia user we may be able to escalate the ticket to Application Support for recovery. Look at the Naughty Person's account, and if any funds remain send the ticket to your Team Leader for further investigation. If there are no funds then fill out the transfer template.

Investigating cases within CSM

Assigning cases

When you assign yourself a case you should review all information in regards to the potential compromised accounts to confirm the account is indeed compromised.

Using Notepad

Notepad ++ is used to record all the data in regards to the compromised account (see figure 57)

Figure 57 – Compromised accounts Note pad file

Promapp link?
https://go.promapp.com/cryptopia/Process/Minimode/Permalink/BggUCe2rNYfHWzJRhugkDa

Ask Josh

Flow charts coming soon…

73

We populate this template with the following information.

Withdrawals

- **Username**: Username associated with account
- **Country of User:** Under Security tab, click "Timestamp" to find the first login, enter their IP into https://www.iplocation.net to find the location.
- **Pwned**: Check their email on www.haveibeenpwned.com. If it comes back positive paste their email in this field, if it comes back negative use "n".
- **Accessed IP**: Under the Security tab, enter the IP address that appears to correspond with the fraudulent activity.
- **Accessed Date:** Enter the Timestamp of the fraudulent IP address.
- **Country**: Search for the fraudulent IP on https://www.iplocation.net/, then enter the country into this field.
- **Traded**: Under the Trade History tab enter the timestamp of the last trade conducted if it corresponds with the fraudulent activity. If no trades exist enter "n" for no.
- **Withdrawn**: From the Withdrawals tab, enter the timestamp for the fraudulent transaction.
- **Blockchain:** From the Withdrawals tab, copy the TxID of the fraudulent transaction, go to the respective block explorer, search the TxID and copy the URL into this field.
- **Address**: Under the Withdrawal tab, enter the address for the fraudulent transaction.
- **Cryptopia Held Address:** On the Currency page - https://www.admintopia.co.nz/Currency - enter the withdrawn coins ticker e.g. BTC, select it in the results and search for your address. If a result is found immediately lock the account, and add them to the Naughty People list.
- **Disabled email:** In the user's account settings under Security, User Security Settings, check to see whether "DisableWithdrawEmailConfirmation" is false or true. If true then enter "Yes" into the field.
- **API:** Under the Security tab, check **IsApiEnabled** is not set to true, if true enter "Yes". If false, check the Trade History tab to see whether there are certain times where trades were conducted consecutively via the API not UI. E.g. if there 3+ trades labelled API around the same time with **NO** other trades within a 5 minute period. If you locate some enter "Was," but if there is no such activity enter "No".

Potential outcomes

```
API Enabled: No

API Enabled: Yes

API Enabled: Was
```

Transfers

- **Username – Pwned – Accessed IP – Accessed Date – Country – Traded – Disabled email – API** are the same as above.
- **Transferred To:** Under the Transfers tab, enter the Naughty Person's username.
- **Transferred Time:** Under the Transfers tab, enter the timestamp associated with the fraudulent transfer.
- **Blockchain:** In the Naughty Person's account, try to match a withdrawal TxID to a time after the fraudulent Transfer was made, as with withdrawals check this on the block explorer and copy the URL.

   Note: There will be situations where there will be multiple logins/withdrawals/trade times. Adjust this template to suit your own needs, such as adding all the times the identified IP/trades/withdrawals were made at your own discretion as this is more of a reference than a proper database and mainly just useful for filling out the template.

Tags

In Service Now we have 4 general tagging stages for compromised accounts.

1. **COMP – First Response**
   This tag is applied to cases that are New/Open that have been given the templated response in Confluence under Support Templates/Accounts/Compromised Account

2. **COMP – Investigated**
   This tag is applied to cases that have had the account investigation done

3. **COMP – Response to Investigation**
   This tag is applied to cases that have re-opened/replied to their case with a response to the prior investigation that was sent.

4. **COMP – Locked Account**
   This is used for any account inquiries regarding a Locked Account that appear to be related to a user becoming Compromised.

Standardised Tags
COMP-First Response | **COMP-Investigated** | **COMP-Response to Investigation** | **COMP – NM Recovery**

Other useful Tags
COMP-Awaiting info | **COMP-Completed** | **COMP-Locked account** | **COMP-Post Enquiry** | **COMP-Replied to** | **COMP-Tricky** | **COMP-Unable to help** | **COMP-Multiple Cases**

Responding to the case

Work notes

In your case under Notes, copy and paste the notepad data into Work Notes. (See figure 59)

```
 1   Username: bonusvoucher
 2   Country of user: Czech Republic
 3   Pwned: burners@seznam.cz
 4   Accessed IP: 50.252.207.114
 5   Accessed Date: 5/13/2018 8:22 PM(UTC)
 6   Country: United States
 7   Traded: 8:32 PM(UTC) to 5/13/2018 10:54 PM(UTC)
 8   Withdrawn: 5/13/2018 8:26 PM(UTC)
 9   Blockchain: https://blockchain.info/tx/0b56fe26d5f60e21576acef74123ca3e9e521ac1e22873b30177ac778a7573bf
10   Address: 3F8UYPbHwRfzogJ1w2HNpy4DRnERRpHGoE
11   Cryptopia Held Address: No
12   Disabled Email: No
13   API Enabled: No
```

Figure 58 – Note pad file

R   Rob

Username: sthetix
Country of user: Indonesia
Pwned: spazioforma@gmail.com
Accessed IP: 202.174.5.2
Accessed Date: 4/20/2018 7:51 AM(UTC)
Country: India
Traded: 4/20/2018 7:51 AM(UTC)
Withdrawn: 4/20/2018 7:52 AM(UTC)
Blockchain: https://verge-blockchain.info/tx/27666233df8ecc681d017beed723e1f283fd19c8976d44bcfebcfa6f7bac1340
Address: DNSMcbZjYknmk3Krt8irGzp4Sb2kN8m8P3
Cryptopia Held Address: No
Disabled Email: Yes
Api Enabled: No

Figure 59 – Service now work notes

Under the "Additional Comments (Customer visible)" field, copy and paste the respective template (withdrawal/transfer) from your word document. Each field marked with an XX in front is a variable field which you copy and paste the data from your work note into.

Within the word document there is also comments associated with certain variables such as:
-Withdrawal Confirmation Disabled
-Pwned?
-API Enabled?
-Logins Same IP

Notes:

There are also other various small adjustments like multiple withdrawals/IPs/API enable/Logins same IP. However, feel free to adjust each one of to suit the case.

We just need to give sufficient proof and try to cover all bases of how their account may have become compromised.

Closing the case

After you've filled in the template, change the tag to **Investigation Sent**, head to **Closure Information** and mark the code as Completed and Close notes to Investigation Sent. If this was a complex case or you believe it requires a few extra details feel free to add these in at your own discretion. After this head to the top of the page and click **Propose Solution**.

AML/CFT Act

Anti-Money Laundering and Countering Financing of Terrorism Act 2009

What is ML/TF?

Money laundering (ML) is any attempt to disguise the source of money or assets derived from criminal activity.

Terrorist financing (TF) is activities that provides financing or financial support to individual terrorists or terrorist groups.

Businesses in New Zealand struggle to believe that their products and services are being used by their customers for ML or TF activity. The truth is that over $1.5 billion dollars are estimated to be laundered through New Zealand financial service providers and other businesses each year. It is very unlikely that your business has not been touched.

The New Zealand government warns that it may only be a matter of time before New Zealand is exposed to terrorist activity.

ML/TF usually has three distinct phases

Placement

Placement is the process of physically placing bulk cash derived from criminal activities into financial service providers or other legitimate business.

The source of the cash can be easily disguised or misrepresented.

This may happen when cash is deposited at a bank's front desk, or when a cash transporter collects cash to transport it to the bank. Any business that deal heavily in cash are heavily exposed to the placement phase.

Layering

Layering is the process of separating the source of cash or asset from its criminal sources, by passing it through a number of transactions.

The purpose of this stage is to make it more difficult for law enforcement to trace the true origin of the cash or asset.

This may happen through the purchasing of material assets with cash, or moving cash or assets through different accounts or owners.

Integration

Integration is the process of combining illegal funds with legally obtained funds in order to provide a legitimate explanation of their ownership.

This often takes place through the banking system so that criminally obtained funds may appear to be normal business earnings

This is the stage in which shell companies, property dealing, and false trade invoices are common.

What are Cryptopia's requirements?

There are three government agencies that supervise the regime in New Zealand:

- Department of Internal Affairs (**DIA**)

- Financial Markets Authority (**FMA**)

- Reserve Bank of New Zealand (**RBNZ**)

Cryptopia will probably be supervised by the DIA, but the regulators are still getting to grips with crypto exchanges.

Formal Guidance

Formal AML/CFT guidance are the minimum requirements that Cryptopia must follow in order to be compliant with the AML/CFT Act.

There are four formal guidance groups that your AML/CFT Compliance Officer must ensure are met:

- Legislation
- Regulations
- Code of Practice
- Guidance Material

Informal Guidance

Informal AML/CFT guidance is information that can guide Cryptopia towards specific, practical interpretation of the AML/CFT Act in New Zealand and your industry's best practice.

There are two groups within informal guidance that your senior managers must ensure are met:

- Supervisor news and resources
- International guidance

Three Key Concepts
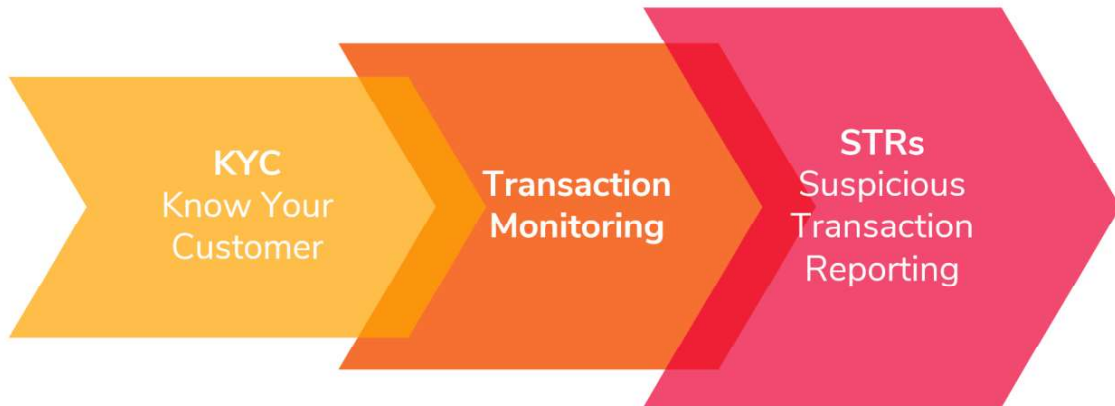
Cryptopia's responsibility is to tell the New Zealand Police if anyone in the business sees something suspicious.

Different parts of the business look for different threats.

Each will be trained in Cryptopia's "<u>k</u>now <u>y</u>our <u>c</u>ustomer" checking, transaction monitoring, and "suspicious <u>a</u>ctivity <u>r</u>eport" responsibilities.
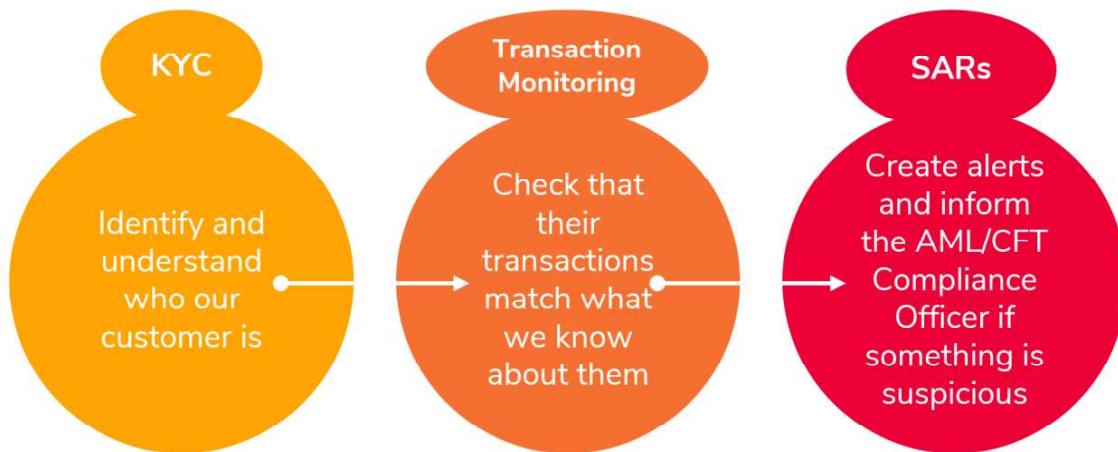
KYC is important

The first chance Cryptopia has to protect itself against ML/TF activity is when a new customer establishes a contract with us. This is why it's so important at this time to:

Verify the identity of relevant people within the customer's business;

Gather information about the nature and purpose of our customer's business and expected transaction needs;

For those who are high risk, verify the source of wealth of a customer, and the source of any funds of an unusual or suspicious transaction.

Once we do KYC, know our customer, and can predict how they will transact with us, spotting signs of ML/TF activity gets easier.

Once we can spot potential signs of ML/TF activity, we can file SARs to the NZ Police and remain AML/CFT compliant.

What's Next?

Talk to Tim Brocket, your AML/CFT Compliance Officer. He has all you need to know about AML/CFT at Cryptopia right now.

Dig into the world of AML/CFT in New Zealand at www.fiducia.co.nz.

Dealing with Account Changes

Moral Compass

These protocols are for security purposes and to ensure we have consistency in our response. What actions we can take depend on whether the user logs in and makes a ticket, or sends us an email (see figure 60).

2FA Reset	Correct Info?	Perform Reset actions	Request more info?
Ticket	n/a	Yes	No info needed for tickets, 24 hr delay before reset
Ticket (New/Blank Account)	n/a	Yes	

Ticket from different account	Yes	No	
Ticket from different account	No	No	No

Emailed from registered address	Yes	Yes	
Emailed from registered address	No	No	Yes
Emailed from registered address (new/blank account)	n/a	Yes	
Emailed from registered address (new account Auth App)	Must say account is empty	Yes	

Emailed from unregistered address	Yes	No	
Emailed from unregistered address	No	No	No

Email	Correct Info?	Perform Reset actions	Request more info?
From ticket	n/a	Yes	
From ticket - diff account	Yes	No	
From ticket - diff account	No	No	

Emailed from registered address	Yes	Open Ticket	
Emailed from registered address	No	No	Open Ticket
Emailed from unregistered address	Yes	No	
Emailed from unregistered address	No	No	No*

Figure 60 – Moral Compass showing the 'Dos and 'Don'ts.

Checklist for 2FA Resets via email

- What verification level is the user?
  - ➔ Level 2 or 3 can provide their ID, use "Level 2 Verified" template

- Is their account activated?
  - ➔ They will not receive our emails if not activated.

- Is their account locked?
  - ➔ Check to see if they are a Naughty Person.

- What form of 2FA is on their login?
  - ➔ User may not have any 2FA on login. Tsk tsk.

- Did they recently upgrade their 2FA?
  - ➔ User may say they are no longer receiving 2FA emails, but they may have just upgraded to AuthApp.

- Are there incorrect password login attempts?
  - ➔ Provide the "Password Resetting" template as well as "Verification for reset".

- Have they logged in after sending the email?
  - ➔ Ask if they still need help with their 2FA.

- Is this a new account with one or two logins, and no balances?
  - ➔ If Auth App, ask them to provide some information, reset if they say account is empty. If Pin Code, reset 2FA and provide Empty Account Pin template reply.

2FA reset via ticket

1. Service Now 2FA reset protocol – reply to user, and mark ticket for follow up in 24 hours.

Emails

1. Only reset through a ticket *(exceptions seen later in document)*
2. Check their new email is not in use.
3. Check whether they have Email Code as 2FA *(this will need to be reset after their email is changed)*
4. ServiceNow reset protocol – reply to ticket and email old address and new address and mark the ticket for follow up in 24 hours.

Incoming Emails

PLEASE CHECK TO SEE IF THE USER IS LOCKED BEFORE 2FA RESETTING.

If a user's address can't be found in an Admintopia search, replace the @emailservice.com with a * for a wildcard search, and make sure there is no space before the start of the email address in the user admin box.

@googlemail.com is the same as @gmail.com. @icloud.com is the same as @me.com – If in doubt, google to see if an address has multiple aliases.

Some users have added the +Cryptopia filter to their address. They will not automatically be assigned a ServiceNow contact, and you won't find them unless you remove the @emailservice.com as above.

Users often have the same username at different email providers. Proactively looking can solve the issue without generating more emails back and forth. If they send an email from an unregistered address and are clearly describing an account that exists registered to the same username at another email provider, you can send them a reminder message to their registered email - "Hello my dude, just wanted to remind you that this is the email address you signed up to Cryptopia with." Do not send this email address to the other email enquiry – never release **ANY** user data.

- Outlook.com email account appears as "outlook_[long series of letters and numbers]@outlook.com" in sender email

If you can figure out the email address from the content of the email, send them this link - https://support.office.com/en-us/article/outlook-com-email-account-appears-as-outlook-long-series-of-letters-and-numbers-outlook-com-in-outlook-for-windows-90ed7938-7f21-4cb5-a69d-a3b79ea4eafd

You can't reply to the outlook_23098unjaspfd@outlook.com address, it will be undeliverable.

- Gmail - You can add '.' to anywhere in the first part of the email address with Gmail and receive emails regardless of the '.', i.e. email address is emailaddress@gmail.com you will receive emails even if they are sent to email.address@gmail.com and vice versa. This means you could sign up to Cryptopia with dots anywhere and not experience problems. Please note that if they email from emailaddress@gmail.com and their registered account is email.address@gmail.com, it is the same email account. A user **cannot** use this feature to register multiple accounts.

Exceptions to resetting an email address through an email.

In Confluence: Email Templates **>** Account Related **>** Account recovery > proven dead email address - READ GENERAL PROCESS

https://cryptopia.atlassian.net/wiki/spaces/SUP/pages/414875910/Account+recovery+-+proven+dead+email+address+-+READ+GENERAL+PROCESS

Email Templates **-** Account Related **-** Not receiving automated emails - Spam Report

https://cryptopia.atlassian.net/wiki/spaces/SUP/pages/442269744/Not+receiving+automated+emails+-+Spam+Report

As we are not able to remove any spam reports a user may have created, we need them to verify their identity then we can update their email address.

Rule: We would rather fix the issue rather than change the user's email address.

If a user is unable to log in, CS must be sure that they have fixed any issue from our end, and that the user has fixed any of their issues.

If they can log in, they can request an email change through a case/ticket.

Investigating an Account

When you get an email, you should always do your due diligence investigating an account.

Check for any other tickets they may have open. Search through their settings, logins, approvals etc.

You want to paint the best and most full picture of what's happening.

Cross Examining information provided

We require at least **THREE** pieces of information.

We at least **ONE** piece of primary information from the user's account. Without this primary information we cannot reset their 2FA:
Trades
Balances

Example: I have 345.00 DOGE or I traded 650.00 ETN for BTC

Additionally, we will need at least **TWO** correct pieces of account activity from the list below.
Deposits
Withdrawals
Wallet address
Payment IDs
Transaction IDs
Login dates
IP address

Registration date

Instead of one of the second pieces of information they can provide a picture of a valid photo ID, as well as a picture holding the same photo ID with a hand written note saying **_RANDOMLY_GENERATED_PHRASE_** along with another photo of a proof of address such as a utility bill.

Bear in mind, everything except for **balances** and **trades** is information that can be found elsewhere (transaction IDs and addresses in other exchanges or personal wallets, withdrawal confirmation emails contain all information in them, etc.) so everything *except* balances and trades **must** be exact.

Trades and balances, the accuracy on these should depend on how long it's been since they've logged in. If it's been months since they've logged in, the margin of error would be bigger.

Trades acceptance criteria:

- Have the trade pair correct
- Whether it was buy or sell
- Date of trade (if a day off, check user's time zone)
- Rate – reasonably close i.e. ± 5% of X
- Amount – reasonably close i.e. ± 5% of X

Balances acceptance criteria:

- Currency must be correct
- i.e. ± 5% of X

If you feel that a user is legitimate, but they don't fit the criteria – you should get a second opinion from your Shift Leader.

Automated emails we send from noreply@cryptopia.co.nz:

- **Cryptopia Two-Factor Unlock** – 2FA reset email after reset gets approved
- **Cryptopia Login Confirmation** – Email Code
- **Cryptopia Withdrawal Confirmation** – click on the email activity and it will show you the withdrawal number
- **Cryptopia Failed Login Attempt –** incorrect password/2FA
- **Cryptopia Account Registration Confirmation –** new account registration email.

Timeouts for Codes and Tokens

EmailCode is ~7.5mins (see figure 61)

Withdrawal Confirmation Email token = 24hrs

Registration code = ~2 days

Password reset = ~24hours

However, **withdrawal confirmation email** tokens are invalidated when you login, logout, reset password, lock account, or unlock account. And the token is valid for its corresponding withdrawal only.

So if a user's token is invalid it is likely due to them performing one of the above actions rather than them reaching the timeout.

Email 2FA codes are generated per-user based on the current time.
They are valid for on average 7.5 minutes from the time of creation.

Valid for 15 Minutes total

Valid in the past   Valid in future

| 3 Min | 3 Min | 3 Min | 3 Min | 3 Min |

Email codes generated here
Always generates same code within this
3 min time window.

Time
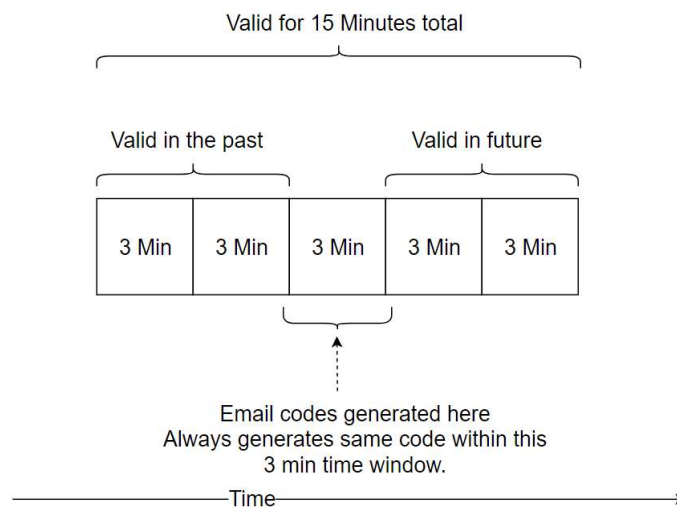
Figure 61 – EmailCode creation and void

180

Inbound Social Media Enquiries

Introduction

Cryptopia receives in-bound messages and direct contact from customers via a number of social media channels. The inbound contacts from users that the Customer Service Team are expected to respond to are:

1. Facebook: Messenger
2. Facebook: Comments in reply to our posts
3. Twitter: Direct Messages
4. Twitter: Replies to our Tweets

Objectives and Key Performance Indicators (KPIs)

5. Cryptopia to consistently deliver World Class Service
6. Consistent messaging and Brand tone
7. Auto-responses in all channels to set customer expectations
8. First response within 48 hours
9. Resolution (for 90% of cases) within 3 days

Brand Tone and Characteristics

Cryptopia's vision is for **digital currencies to be used for anything by everyone**. Our mission is to enable the widespread adoption of digital currencies to give people back control of their money through faster, cheaper and more efficient financial services. We aim to utilize Blockchain technology to open the Fintech sector to innovation.

One of the ways we want to differentiate ourselves from our competitors is through always offering our users World Class Service by ensuring we:

1. Treat our customers with respect no matter how big their balance is
2. Are a champion for, and to protect, the small guy
3. Are friendly but professional (conversational tone)
4. Are always well-informed
5. Always go the extra mile in support

Brand Voice

When responding to messages in public or in private, it is important to remember the guidelines of our brand tone and how we aim to be perceived on social media. All of our responses should be friendly, professional, consistent, and give the impression that we are capable and **we want to resolve their query.**

First Person Plural Pronouns

Always use first-person plural pronouns (we, our, us) to respond- that is, we don't use "I" when replying on behalf of the company. (E.g. We're very sorry to hear this happened to you.) This is especially tempting to do on social media!

Non-English Messages

If you see that a user's Facebook profile indicates they are a speaker of another language, it is preferable to use simple language. If they appear to have difficulty understanding the language used, make it as simple as possible while still being friendly, but do not use Google Translate.

Dos and Don'ts

Here's a helpful guide as to the dos and don'ts when replying to customer queries received via social:

Characteristic	Description	Do	Don't
Passionate	We're passionate about helping everyone use digital currency for anything.	- Use strong and passionate verbs - Be a champion for the everyman (without singing the downfall of the establishment)	- Be lukewarm, wishy-washy or uncertain - Be passive
Pioneering	We're not afraid to innovate and challenge the status quo.	- Be open to new ideas - Be open and be proud of our new ideas	- Be pushy or rude or domineering - Ever be disrespectful of someone else's opinion - Be a bully
Quirky / Irreverent	We're reliable as hell but we still like to have fun while we're at it.	- Take our product seriously but not ourselves. - Be playful and interesting and informed.	- Be too casual - Be too overly familiar and overstep the professional mark
Authentic	We believe in transparency - not smoke and mirrors. We'll help in whatever way we can.	- Be honest use friendly language (but still professional) - Own our mistakes and apologise Stick to our word	- Be abrupt or rude - Overpromise - Oversell

Figure 62 – Dos and Don'ts for responding to customer queries via social media

Facebook Messenger

Overview & KPIs

We receive Facebook messages from users, coin developers, marketers, journalists, investors, and more. Our KPIs for responding in this channel are:

1. Respond to all messages within 4 hours
2. Provide Help Centre links where appropriate
3. Use templates where appropriate to reply (these will often need to be slightly tailored)
4. Aim to resolve their issue with the first response (encourage them to lodge a support ticket, escalate their support ticket or answer with a Help Centre article)
5. Keep a clean inbox and ensure you 'Mark As Done' for messages that are resolved
6. Escalate support tickets where appropriate (and advise the customer you are doing so)
7. Assign tricky messages to Cat or marketing where required

Auto-Responses

When users open a message with our page, they see the message "Welcome to Cryptopia Messages! We aim to respond to all messages within 4 hours. Visit our Help Centre for more assistance https://support.cryptopia.co.nz/csm".

We also have an automated reply which you will see- this is "Hi [firstname], thanks for your message! We will respond within 4 hours. If your query is support related, please create a support ticket at https://support.cryptopia.co.nz Current support response time is 72 hours."

YOU CAN UPDATE THESE THROUGH THE SETTINGS IF YOU ARE AN ADMIN.

Templates

We have a number of pre-set templates on our Facebook messenger. They all follow the following template, and most all messages sent from our Facebook account should follow this template:

Hi *[firstname]*,
Message (friendly, helpful, comprehensive, etc.)
Thanks,
Cryptopia Team

You can find these templates ('saved replies') here- they automatically input the user's name. You can add relevant templates by clicking 'manage replies' and delete unused ones for ease of access.

Marking as Done or Follow Up

Once you have finished replying to a message, mark them as done (see figure 63). This puts them in a different folder until the customer replies again.

The other options are to mark a message:
- for follow up (the star next to the tick),
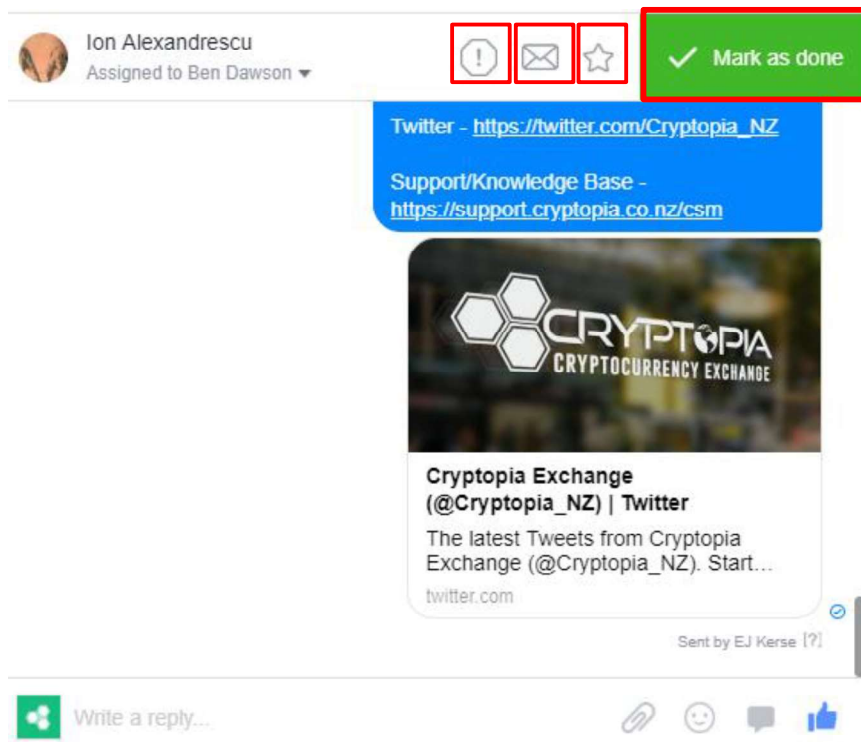- as unread (the envelope),
- as spam (the exclamation mark)

Figure 63 – Marking a message as done

Assigning

This drop box allows you to assign a message to a member of the team (see figure 64) to escalate or forward to marketing if it's a marketing or media enquiry.
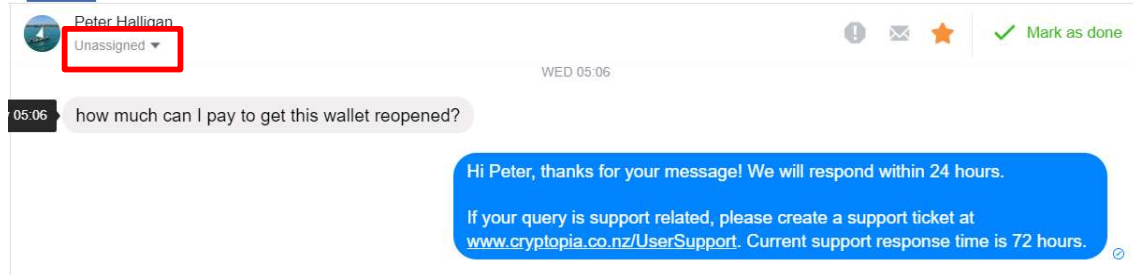
Figure 64 Assigning a message to a member

Josh Yaspan
View Profile

About

⚒ Works at International Fitness Oregon

🎓 Studied at Maric College

🏠 From Los Angeles, California

Labels   Manage Labels

● kate

Add Label

Your Notes   Add Note

Notes help you keep track of your conversations. Only admins can see notes.

Customer information

This section shows whatever information the user allows to be seen publicly (see figure 65).

These labels can be used to categorise users or track current issues, and are visible only to admins. In case these are ever accidently leaked to the public, we'd prefer to use colours to describe users rather than words.

The notes section can be used to track information about a case between staff.

Security

We can only give certain information to users over Facebook messages for privacy and security reasons. Users will sometimes send screenshots of their account balances, transactions or tickets.
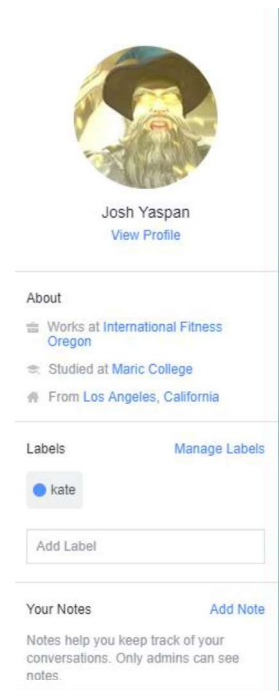
Figure 65 -Labelling customers' current issues

We can we do?

- Tell a user that their ticket has been replied to or escalated
- Explain information that is clear from screenshots or their messages
- Use hypotheticals
- Offer advice on where to get support

What we cannot do:

- Tell someone the contents of a ticket reply
- Tell someone the contents of an account
- Tell someone for sure their account has been compromised
- Give any account information (email, username, locked/unlocked status)

- Offer support
- Give any information on upcoming coin listings
- Correspond with coin developers about the specifics- send them to coinwallets

Users often message when they can't get into their account. Sometimes they have emailed support and sometimes not.

Known FB Messenger Bugs

It's important to note that there are a few glitches that occasionally affect the interface.

- Not being able to see assigned messages
- Messages including our latest post will randomly send to users (possible hootsuite bug) without prompting
- Messages from before a certain date will not appear – in this case, do a hard refresh. Try to keep a note of when your oldest messages are and be aware if they don't show up when you keep scrolling down.
- Follow up star glitches sometimes and won't appear or won't be un-selectable

Remember to check if a user has private messaged us too, but comment anyway to notify them that we're dealing with it.

Abusive Messages

If a user is being abusive, it is ok to ignore their messages. If they are angry about something out of our control, there is little that we can say that will calm them down. You can disengage after providing a reasonable reply.

Facebook Wall Post

Overview & KPIs

When we post on Facebook, we get comments. These comments could be from users, coin developers, marketers, journalists, investors, and scammers! Our KPIs for responding to wall posts are:

1. Respond to the majority of messages (where we can) with the objective of either:
   a. General information queries - provide Help Centre links where appropriate
   b. If the user needs to log a support ticket, ask them to do so
   c. If the user needs more information, as for them to SEND US A MESSAGE VIA MESSENGER. Ultimately we don't want conversations being had on a public forum and sometimes this information can be sensitive.
   d. Answer generic questions that won't encourage a reply
2. Use templates where appropriate to reply (these will often need to be slightly tailored)

Managing replies

It's best to view by Most Recent / Newest (see image below)

Remember to check if a user has private messaged us too, but comment as well to notify them that we're dealing with it.
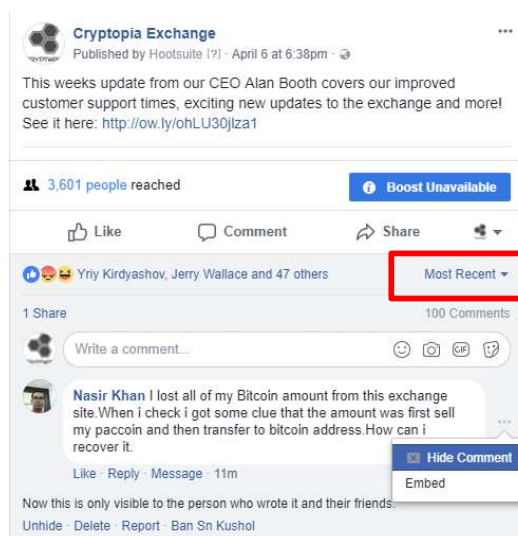
Figure 66 – An example of a Facebook post

You can also monitor new comments on our posts via the comments and more tab on Facebook. This will present a list of the latest comments in the same layout as Messenger conversations. It is helpful for seeing new comments made on very old posts.
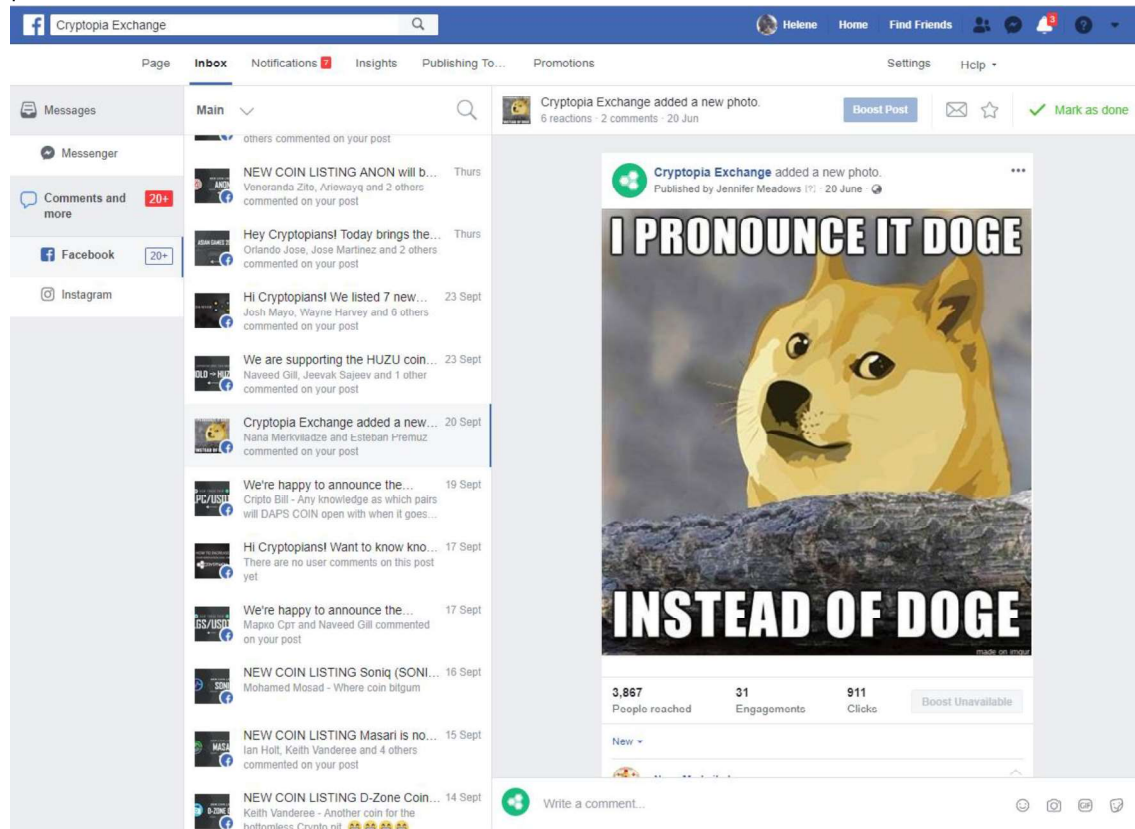
Figure 67 – Comments tab

Hiding Comments/Banning users

When a commenter is abusive, spamming, or includes sensitive information in their comments, we can hide their comments from the public and ban the commenter if necessary. Banning a user from the page means they can no longer message or comment on our page- if a user is being abusive on messenger, it's good to check if they've commented as well. Only do this in extreme cases as this will send them to the phishing pages- see below.

Do not ban a user just for a negative review or being angry.

When replying to comments, double check you are replying as the company page and not with your personal account.

We have disabled the option for users to make a public post on our Facebook page, so users will continue to comment on week- and month-old posts to get our attention- make sure to monitor these.

Phishing Pages

Figure 68 – Phishing pages in Facebook

These phishing pages (see figure 68) respond to messages they are sent mostly requesting money to BTC addresses. Otherwise, they will comment on users' comments or posts with a fake help line pretending to be us- when they do this, it is very hard to see the difference on the post. If you see these, delete them and ban them.

We are working on getting verified so we can report them properly.

Cryptopia the community organisation is not an affiliate nor a phishing scam, just a similarly named organisation.

Extra tips

As this is an instant message platform, users can tend to be more impatient and use strong language, as well as have higher expectations due to the faster response rate. We have templates explaining why we can't help, but after a certain amount of communication, when there isn't anything else to add it is okay to ignore the messages, especially if they are abusive.

Otherwise, take a moment before responding to the message and remember that they aren't criticising you, they are just letting out their frustration. The task here is to manage their expectations – You can't take on their problems or solve every issue via social media.

Twitter

Overview & KPIs

When we post on Twitter, we get replies (see figure 69). These replies could be from users, coin developers, marketers, journalists, investors, or scammers! Our KPIs for responding to replies in Twitter are:

1. Respond to the majority of messages (where we can) with the objective of either:
    a. General information queries - provide Help Centre links where appropriate
    b. If the user needs to log a support ticket, ask them to do so
    c. If the user needs more information, as for them to SEND US A MESSAGE VIA DIRECT MESSAGE. We want to encourage users to never share any of their private information on a public forum.
    d. Answer generic questions that won't encourage a reply
2. Use templates where appropriate to reply (these will often need to be slightly tailored)

We aim to respond to every reply to our tweets.

These are different to retweets and mentions.

On the Twitter interface, they appear under our tweet, which makes it an important place for us to be seen interacting with our users.
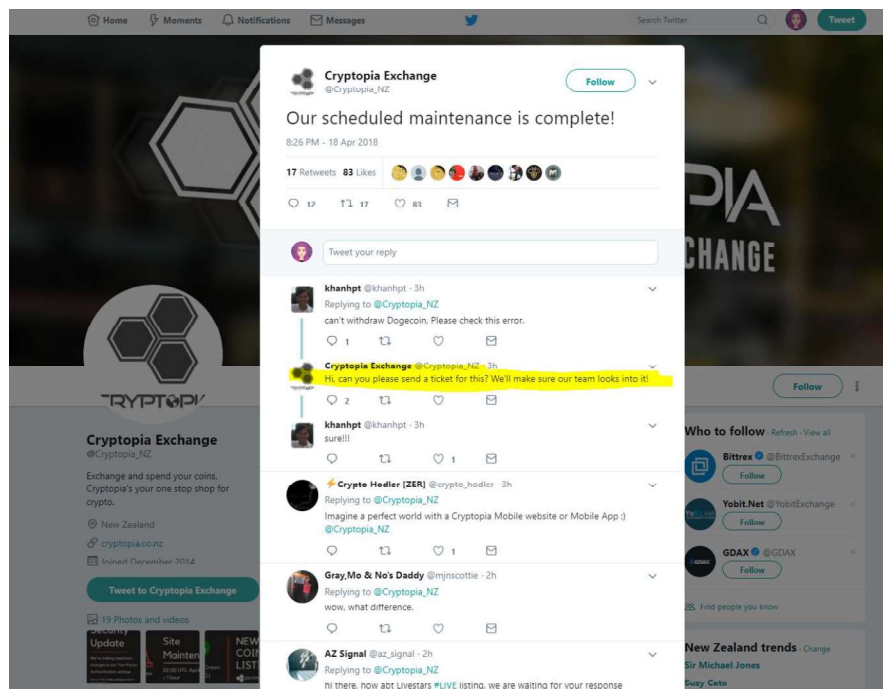
Figure 69 – Picture of twitter

Tweetdeck – set up and how to use

We use Twitter's monitoring platform Tweetdeck to keep track of replies. For this, you will need to create a Twitter account using your @cryptopia.co.nz email address. Make sure you have 2FA enabled (they use SMS by default). You can do this from your Twitter settings.

First- connect your Twitter account to ours:

1. Send your Twitter handle to the Community Coordinator so we can give you access!
2. Accept the invitation by email, which will take you to tweetdeck.twitter.com where you can accept the request in Accounts → Team Invitations.
3. Make sure this confirmation step is enabled, and have it enabled as your default account.
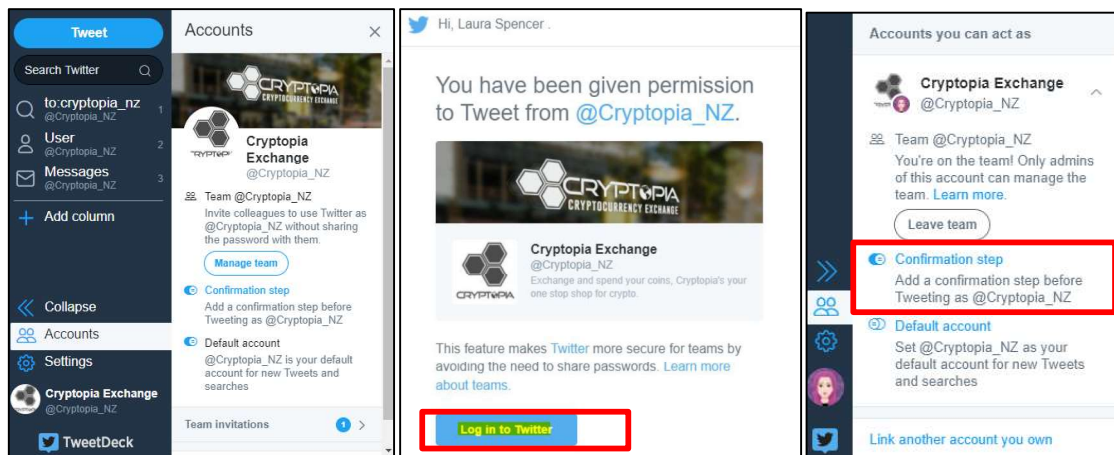
Figure 70 – Tweetdeck set up

Tweetdeck's interface is unique, but it allows you to easily monitor replies to our tweets and send Direct Messages to users. Tweetdeck works in columns.
This is the sidebar:

New tweet

Blue icon is search

The icons here represent columns

Add Column

Expand sidebar
Accounts
Settings

To monitor replies, you will need to add a search column. Click Add Column,

This search query will show all replies to our tweets!

To reply to the user's reply-tweet:

1. Click on any message from the column to view our original tweet:

These next two sections – if Cryptopia is set to your default account (the icon indicates the account being used), you can just reply in the column, if not, click the icon circled in red and use the new tweet column to write the reply from the correct account.

100

The columns you should have set up are

Messages, User @Cryptopia_NZ, @mentions @Cryptopia_NZ, search Cryptopia_NZ, Scheduled

We sometimes receive spam messages in our DMs. We can remove these by flagging the conversation as spam.
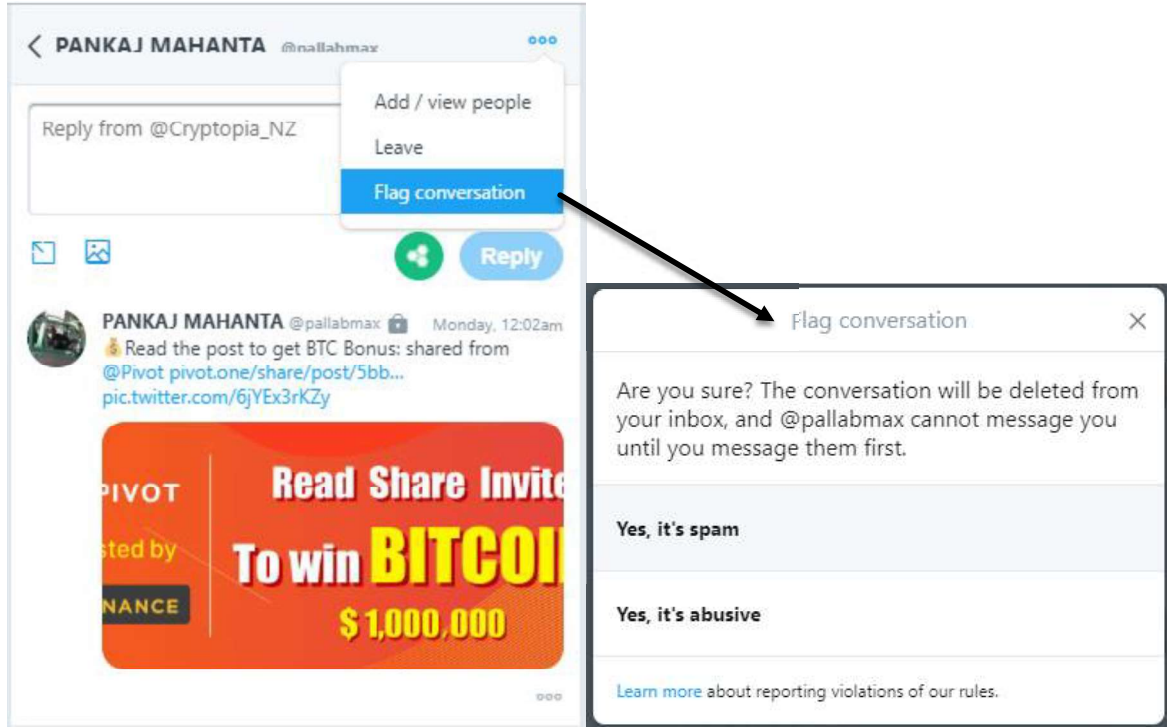
Phishing tweets

Phishing tweets can be identified by checking the user is legit. (see Figure 71)

Figure 71 – phishing tweet

We can report users who are trying to impersonate Cryptopia

Figure 72 – reporting users on twitter

Once you send this report, an email will arrive to the address entered within a minute. Reply with a brief confirmation of your report, which will generally lead to the account being suspended within 24 hours.

After the report is complete the account will generally be suspended within 24 hours.

102

Moderator Guidelines

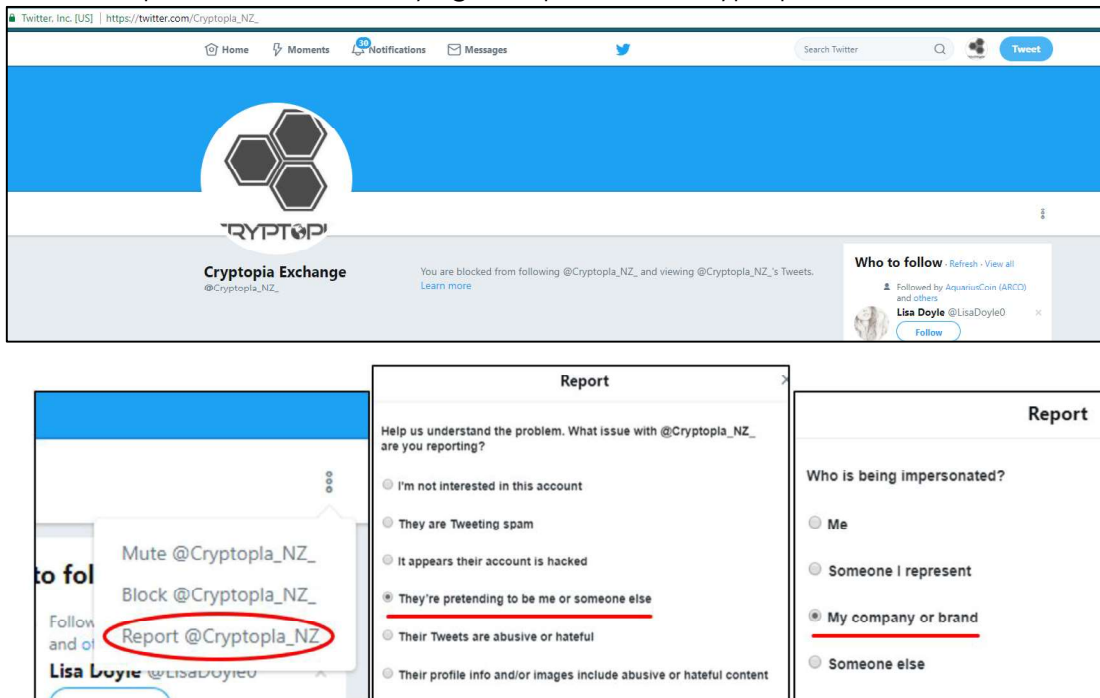Cryptopia has Moderators who voluntarily help to ensure users who frequently use the Trollbox, Discord and a number of social media and community channels get the help required. This document outlines the dos and don'ts for all our moderators.

Dos

- Be reasonable with our users, and use their abilities responsibly
- Moderate the Trollbox
- Ensure all users are following the Trollbox rules.
- Moderators are **not above the rules** and can also be banned.
- Moderators may not ban other Moderators.
- If an Administrator bans a Moderator they must sit out the full duration of the ban and may not unban themselves.
- The first Moderator to respond to a user's question or problem, should be the only Moderator to handle the situation unless they have asked another Moderator to step in or help. This is to avoid miscommunication between users and different Moderators.
- Uphold Cryptopia's Terms and Conditions to the best of their ability
- Help new users to Cryptopia feel welcome
- Answer questions where you can when they are asked in a reasonable capacity, and direct users to raise Support Tickets appropriately.
- Promote Cryptopia's Help Center
- Promote the importance of having good personal security on their Cryptopia account
- Promote the importance of knowing about phishing scams, and how to prevent them
- Report abuse, and fill in all of the required fields with appropriate information when doing so.
- Communicate with each other and Cryptopia Admin staff
- Remove profane or hateful attacks toward individuals or groups of people
- Remove personal information (when reasonably deemed inappropriate or dangerous)
- Remove any and all scam, spam, or any other material from our forums which goes against our Terms and Conditions, and report it appropriately.
- Moderation is essentially a volunteer job, those that fail to remain active or abuse their position will be stripped of the role.
- ****ONLY**** post links to Coin discord groups in a support capacity when required. No unsolicited links to anything otherwise.

103

196

Moderating the Trollbox

Below is a basic outline of what is expected of moderators in the Trollbox. Please ensure that if you are in the Trollbox, you are also online in the Cryptopia Discord.

Make sure you read and understand the Trollbox rules and follow them yourselves.

Banning with warning:

You should always try to give the user warning before you take any sort of action, unless they are a repeat offender.

Make sure you state the rule/s they have broken and post a link to the Trollbox rules in the ban message. Update the 'Chat Bans' channel in Discord with the ban reason, user banned, and duration of the ban.

Trollbox Ban Protocols:

10 minute warning for minor offences – Check rules timeout, 600 seconds
- First Offense: 86400 Seconds (1 Day)
- Second Offense: 864000 Seconds (10 Days)
- Third/Final Offense (or specific bad cases): 999999999 Seconds ("Life")

You can only ban a user without warning for the following reasons:
- Excessive and or deliberate link flooding in Trollbox.
- A user that repeatedly breaks the same rules.

Do Not's

- Ban or request a ban without evidence of a user breaking a specific guideline
- Delete threads or discussions based on personal views or dislikes
- Speak "for" Cryptopia without confirming information about to be released
- Create additional Cryptopia materials, rules, or branded content, without first consulting admin staff or getting approval from management.
- Publish correspondence, images, resources, etc. before obtaining permission from all involved—community members and/or staff
- Post links to Discord groups
- Ask for payment of any form
- Be a douche
- Break any of the rules outlined for our users
- Promote specific coins via their Username OR Profile picture (Discord, Trollbox etc.)
- Promote ANY coin via Discord, Trollbox etc. (Including our own DOT, CEFS) – we must be completely impartial
- Post unsolicited links to discord groups.

Trollbox Rules (WIP)

In order to keep our Trollbox a safe place for our community to chat, share ideas and help one another. We want to create a mutually respectful place where everyone can be heard and that is also free from spam.

1. Logging a Support Ticket about someone not liking you in chat or any similar trivial reasons will result in Trollbox Perma-Ban
2. Logging a Support Ticket about getting Banned or PayBanned will result in Trollbox Perma-Ban
3. Logging a Support Ticket about being on someone's ignore list or tip ignore list will result in Trollbox Perma-Ban
4. Logging a Support Ticket complaining that you only made 0.0000xxxx in tips today will result in Trollbox Perma-Ban
5. Please do not use the Trollbox for support requests
6. Do not beg for tips
7. Do not post only emoticons, instead please contribute to the conversation
8. Do not spam links
9. Do not post referral links
10. Personal issues are to be dealt with in private. Don't pollute the Trollbox with disagreements or other personal agendas/conflicts
11. Respect everyone's right to speak in their native language
12. Do not comment on tips, at all. No "Thank you", "you're awesome", "nice rains" or anything of that nature. No "I missed the tip/rain", no "I'm going to tip soon", nothing. Tips happen all day, every day, your thanks are assumed and commenting on tips is spam.
13. Do not use the tip reasons to advertise
14. Do not use your chat handle to advertise
15. Do not use the Trollbox to advertise
16. All links that could be considered Not Safe For Work must be tagged with [NSFW]
17. No advertising your buy or sell orders, or asking people to buy or sell your coins.
18. No commenting on karma: no asking for it, no offering it, no saying thanks for it.
19. No commenting on the rewards you win.
20. These rules are subject to Moderator/Administrator discretion, please respect the Moderator/Administrator's final decision

CS0106247 - reset google authenticator

From: Cryptopia Support <support@cryptopia.co.nz>

To: support@onlinedirectdealings.com

Date: Tue, 19 Mar 2019 11:56:38 +1100

Thank you for contacting Cryptopia Support.

To maintain the security of your account, we need you to provide some information to verify that you are the account owner before we can reset your 2FA.

We require at least THREE pieces of information about your account.

We need you to describe at least ONE piece of primary information from your account. Please note that without this primary information we cannot reset your 2FA:

Trades
Balances

Example: I have 345.00 DOGE or I traded 650.00 ETN for BTC (Not Estimated Value in BTC)

Additionally, we will need at least TWO correct pieces of account activity from the list below.

Deposits
Withdrawals
Wallet address
Payment IDs
Transaction IDs
Login dates
IP address
Registration date

Instead of one of the second pieces of information you can provide a picture of a valid photo ID, as well as a picture of yourself holding the same photo ID and a hand written note with today's date and your username,along with another photo of a proof of address such as a utility bill.

If you cannot fulfill these requirements we will be unable to reset your 2FA. Please understand we take the security of our users' accounts very seriously and we must be absolutely certain you are the account owner before we can perform a reset for you.

A quick reminder: Never tell anyone (including us) your PIN or password, we do not have access to this information and revealing it will decrease the security of your account.

Kind regards,
Michael

Ref:CRYMSG1413053_Z44q749k6W30g8hH9

CS0106673 - reset email for 2FA

From: Cryptopia Support <support@cryptopia.co.nz>
To: sermonindex@gmail.com
Date: Tue, 19 Mar 2019 11:52:25 +1100

Hi sermonindex,

Thanks for contacting Cryptopia support.

You have a TwoFactor Email Code active on your account.

After you log in to Cryptopia with your email address and password, you will be prompted to enter a TwoFactor Email Code. At this time, an email with the subject "Cryptopia Login Confirmation" will be sent to your registered address, which contains a unique TwoFactor Email Code. Email Codes expire 15 minutes after they are sent, so please use the most recent one received before it expires. A new TwoFactor EmailCode will be sent for each action on your Cryptopia account which has this type of 2FA set.

If you can't find one, it may have been filtered somewhere (ie Junk/Spam, or other folders) which don't get synced with mobile apps or email clients, so you should log into a Webmail session if possible, and perform a thorough search for our email.

If you're still unable to locate this email after all of this, then at this stage the only solution we can offer is to change your registered email address for you. Please let us know if you would like to proceed with an email change and we will be happy to begin the process with you.

Kind regards,
Olivia

Ref:CRYMSG1413041_qLqu2RwxYq9MYIK9K