

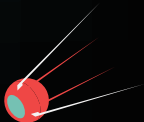
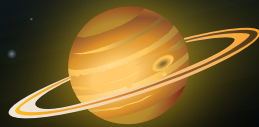
Practical Guide to Crypto

Investment 2018

Australian Edition V 2.0



James F & Jack H



Practical Guide to Crypto In 2018

HELPING THE EARLY ADOPTERS

- INTRODUCING NECESSARY CRYPTO CONCEPTS
- TAX, AML/CTF & REGULATORY COMPLIANCE (AUSTRALIA)
- PERSONAL FINANCE STRUCTURING (AUSTRALIA)
- INVESTMENT STRATEGIES, TRADING & RECORD KEEPING
- ACQUIRING & STORING CRYPTO SECURELY



Many references in this book refer to Australian related matters. Please adapt this information as you see fit for your local laws. I hope you gain value from this document and much of the content is globally relevant.

Disclaimer:

It is of note, that the Authors of this material is not a registered Tax Advisor or Financial Advisor, and does not claim to be a Tax Advisor, or a Financial Advisor. None of this document or its contents should be misconstrued as legitimate Tax Advice or Financial Advice. You should seek Tax Advice or Financial Advice before acting on any endeavours related to this information or cryptographically based assets in general. The views and expressions in this document are strictly for fictional reference only. The Author takes no responsibility to you (the readers') actions, based on what is contained within. By reading further, you agree and are bound by this disclaimer.

There are opinions in this document that should be taken as fiction only. Hence this document should be considered for all legal purposes as fiction.

Although I sincerely hope it helps to inform early adopters.

Because, we rise by lifting others.



Contents

Preface	8
The Future Of Crypto.....	9
Distributed Ledger Technology.....	9
How Distributed Ledger Technology will change our lives.....	9
A new economy is forming.....	10
What to know before you invest.....	11
What Is Crypto?	13
The current dominant blockchains	13
How does it work in practice?	13
Creation of cryptocurrencies and initial Coin Offerings.....	14
Who might create a cryptocurrency and what does it look like?	14
What is an ICO?	14
Coins and tokens in practice	16
Trust in future value by design	17
A word on Participating in ICO's – Be aware on what is being 'sold.'	17
Crypto Regulation Is Coming.....	18
It is time to prepare your holdings and get your house in order.....	18
For those of you that believe that taxation will not affect you.....	19
Tax And Crypto.....	19
Is crypto an asset or a currency?	19
Different ways of investing in crypto require different approaches.....	20
Capital Gains Tax	22
How is CGT calculated?	22
How to tax blockchain fork inheritances, airdrops and other crypto income.....	24
Preventing the annual crypto harvest	24
Tax evasion penalties	25
Tax summary.....	29
Personal Finance Structuring.....	30
Hobbyist/Enthusiast.....	30
Are you an investor, a trader, or hybrid?.....	30



Investing as an Individual	31
Carrying on a "business" in crypto	31
Trading to turn a profit	32
Hybrid trader/investor	33
Keeping Records Of Crypto Endeavours	34
The First-In-First-Out (FIFO) method for calculating Capital Gains Tax	34
Accounting software quirks.....	35
Keeping separate bank accounts for separate activities.....	36
Anti-Money Laundering/Counter-Terrorism Financing And Crypto	37
Overview of the latest AML/CTF regulation.....	37
Regulation of digital currency exchange providers	38
Expansion of powers of AUSTRAC	38
Presumed innocent until proven guilty?	39
Strict liability offences.....	39
Other noted concerns of the bill as it stands in draft form	40
Do You Actually OWN Your Crypto And Can It Be Taken Away?.....	41
Establishing proof of ownership.....	41
Legitimising your crypto holdings.....	42
If starting fresh.....	42
If you have already been in the crypto game a while.....	42
For those with a modest amount of crypto	43
The <\$10,000 exception for personal goods and services.....	43
Where can I spend my crypto?	43
Paying your Bills with your crypto	43
Buying precious metals with crypto	44
Do I have to legitimise my crypto holdings?	44
Thinking about getting creative?	44
I'm just going to hide it where they cannot find it.....	45
Other Possible Avenues Of Unwanted Liability Or Risk.....	47
Divorce or relationship breakdown	47
Child Support payments	47
Bankruptcy	47
A note on borrowing money to buy cryptos	48



Centrelink.....	48
A mention of discretionary trust structures.....	50
Buying crypto for family members, friends or other parties.....	50
Investing In Crypto Via A Self-Managed Super Fund.....	51
Diversification.....	51
Justifying your portfolio allocation.....	51
Look Before You Leap!.....	53
Know what you are aiming to achieve from your investment in crypto.....	53
A note to Millennials about their Lambo... ..	53
A note on the importance of passive income.....	53
Tax Efficiency Strategies For Investors.....	55
A mention on the benefits of white-knuckling (AKA: HODLing).....	55
The never-ending pack of Tim-Tams.....	55
A different form of passive income.....	56
The Salty Taxman.....	57
Diversification.....	58
Strategic buying and portfolio expansion.....	58
Strategic selling and portfolio contraction.....	59
Confidence based buying.....	60
Due Diligence.....	60
Continually betting on the same horse to win the race.....	61
Tax Efficiency Strategies For Traders.....	62
The benefits of keeping good records when making income from trading crypto.....	62
How trading crypto is taxed.....	62
Proof is key to avoid over-taxation.....	62
Cautions.....	64
Trading.....	64
Mining and cloud mining investments.....	66
Emotions can make or break you.....	66
Security (Technical).....	68
Software Wallets.....	68
Hardware Cryptocurrency Wallet.....	68
Your SEED Phrase.....	69



Only use a PC you are confident is secure	70
Do not hold funds or crypto on exchanges	70
Use only hardware wallets for permanent storage	70
Effectively hiding your income or donations which you get in the form of crypto	70
A note on privacy coins	71
Not exposing your crypto holdings	71
How to do it	71
Additional security and privacy tips:	72
Discretion	73
Simple method for securely storing your all-important seed phrase	73
The ultimate method for securely storing your all-important seed phrase	74
Kidnappings, \$5 wrenches, and the only way to guarantee against them.....	77
Other Tips.....	78
Don't send your Tokens to an exchange that does not support them.....	78
Encrypt your USB Drives	78
Do not use cloud providers for storage	78
Bitcoin or Altcoins?	79
Two Factor Authentication	79
Airdrops are not always your friend.....	79
Cryptocurrency Dictionary.....	80
Acquiring Crypto	89
Getting started... ..	89
Example personal financial structure layout	89
The process.....	91
Exchange selection.....	91
Account creation	92
Depositing funds	92
Purchasing crypto.....	92
Acquiring ERC20Tokens and other crypto through Shapeshift	94
Acquiring ERC20Tokens and other crypto through the Exodus Wallet	94
Acquiring ERC20Tokens and other crypto through other exchanges	94
Acquiring ERC20Tokens from EtherDelta	94
Warnings	94



EtherDelta Ledger Wallet Plugin	95
EtherDelta Staging Wallet	95
Getting to EtherDelta	96
Creating a new Ethereum Wallet for use as an EtherDelta Staging Wallet	96
Depositing funds into the EtherDelta Staging Wallet	97
Depositing funds from the Staging Wallet into EtherDelta	98
Purchasing your desired ERC20Tokens	99
Sending funds from your EtherDelta Staging Wallet to your Hardware Wallet "Vault"	102
Guide To Keepings Records With CoinTracking.info	106
Setting up an account at cointracking.info	106
Importing your crypto data	106
Connecting to your exchange API to import your exchange data	106
Importing and monitoring your various blockchain addresses	107
How to record certain Events	107
Network Transaction Fees	107
Exchange Fees	107
Spend crypto for item valued at < \$10,000AUD	108
Spend crypto for item valued at > \$10,000AUD	108
Convert crypto to fiat in any way	108
Rollover crypto assets during a divorce related Property Settlement	109
Sell or exchange crypto purchased at ICO price with bonus, but not spend it	109
Cash purchases and sells (i.e. Localbitcoins.com, or P2P trade)	109
Thinking In Crypto Or Fiat Terms (End Note)	111



Preface

The herd is coming. Many early adopters and eager investors will storm out to get their foot into the crypto rush of 2018. This document aims to minimise the losses of the uninitiated.

This document should help form a practical guide to those entering the crypto landscape in 2018. Many people cannot afford expensive lawyers, consultants and accountants. Every human being stepping into the crypto world is eagerly advised to conduct copious amounts of research and self-education to understand this technology which is not going away any time soon.

This document specifically speculates on safety and certainty of crypto investments. It has a slightly more defined focus on currently existing regulation around the crypto world and speculates on potential future regulation, tax, and other aspects of law enforcement so that potential investors do not get themselves into a mess of potential future liabilities.

Tread carefully.

Jack H

CEO

47.com.au



The Future Of Crypto

Distributed Ledger Technology

Distributed Ledger Technology, herein nicknamed “crypto” is an astounding thing. It leverages what those in computer science know as cryptography, to secure a consistent and immutable ledger of transactional transfer forever – across thousands or more nodes across the planet simultaneously. Hence the term of “Distributed Immutable Ledger” and coined in the term Distributed Ledger Technology (DLT). In its purest form, DLT is the most accurate description of the technology and many can finally see and understand the uses for the technology in our society as the software is now developing into real-world applications. It has the ability to be disruptive to industry and economics on a scale that parallels or surpasses the introduction of Internet Protocol (IP). For those of you who are new to the technology, I would recommend in addition to your own research, at least start with the following video – along with anything else you can search for in the topic.

Blockchain: Massively Simplified | Richie Etwaru | TEDxMorristown

<https://www.youtube.com/watch?v=k53LUZxUF50> (highly recommended)

It is of note that Blockchain is only one, albeit the most popular and common form of Distributed Ledger Technology. The technology will adapt into many forms in the coming decade.

How Distributed Ledger Technology will change our lives

How DLT may change our lives is somewhat convenient and well timed on one hand, and reminiscent of George Orwell's novel “1984” in the other. The technology has the ability to disrupt all industries and will definitively create new industries, just as the internet did.

DLT removes trust from various circumstances but is a double-edged sword. I can see DLT removing a lot of corruption from this world, but that transparency spans down all the way to the individual level, affecting privacy. Eventually, micro-transactions and micro-data points of many now unforeseen areas in our lives will essentially be tracked and traceable, recorded forever on distributed ledgers.

There will be benefits to leveraging this data that help society as a whole, and the cost to privacy is likely to be high. Whether we like it or not, it seems impossible to stop. The real question is that of who has access to the data and for what purposes within society.

Imagine you wake up in the morning, and instead of checking your bank balance to see if you can afford that coffee on the way to work – you find that you currently have 16 different balances of 16 different cryptocurrencies. In total you do have enough to buy the coffee and will probably pay for that coffee utilising one or more of these crypto's simultaneously. There is the crypto you have generated with the solar on the roof of your house. The crypto you generated when you sold your data (from phone, tablet, PC, Amazon Alexa sensors and microphones, etc) to allow marketing companies to follow you and target marketing at you. The crypto you generated by selling your GPS data to the traffic management department of your local city. The crypto you generated for working 1



of your 3 casual/part time jobs. The crypto you got from the government for Universal Basic Income. The crypto you got for renting your car out to strangers last weekend. The list goes on and many of the concepts are foreign to us now, but possible, and many likely in the future.

However, by the time we get to this type of micro-transaction economy, each crypto will have a free market float with accurate value based on supply and demand principles and each crypto will be immediately and instantly transmutable into the desired crypto-currency of which the retailer desires to receive it in. We may even see (although highly unlikely) the International Monetary Fund (IMF) try to form a Special Drawing Rights (SDR) instrument around a basket of crypto's and label it a One World Currency or a similar model of such a function try to be implemented to stem the tide of disruption.

Your data could be on many different blockchains in distributed immutable ledgers across the planet and be recorded forever in what could only be described as the most resilient technological architecture that IT Infrastructure has seen to date.

You couple this with RFID chips whether carried on your person or implantable... and you end up envisioning one of two worlds. Either the world of high convenience, honest monetary principles and less places for corruption to hide. Or as there are some forces on this planet which would unfortunately seek it - you see the biblically referenced Mark of The Beast society and tyranny. It can certainly be said that the duality of people's perceptions during this transition over the coming decade due to the advent of Distributed Ledger Technology – is going to result in many new issues and solutions. Hopefully we can find a way for humanity to evolve society to a higher degree of human wellbeing planet-wide through embracing this technology, without falling into a trap of tyranny. What a time to be alive hey!

The 'glue' of law and justice systems which holds society in a balanced state, is likely to increase in its proficiency of enforcement as the advent of Data Matching by Artificial Intelligence systems in parallel to Distributed Ledger Technologies evolves. The interference of these technologies is also likely to cause societal disenfranchisement of freedoms and the related objections.

With this stated, I hope the information in this document helps a lot of people from exposing themselves to liabilities related not only to financial loss due to lack of experience or knowledge, but also any tax or anti-money laundering legislative enforcement that will come in the future. Whilst I do believe it will take up to 5 years for governments to catch up in terms of enforcement... The risks associated are best avoided, so be aware and be careful sooner rather than later.

A new economy is forming...

The coming "tokenisation" of our world is likely to result in a new economy being born – and certainly has already begun. Whilst we may perceive Bitcoin as a niche or experimental instrument, it is important to remember that Bitcoin itself was the metaphorical progenitor of a new understanding and birth of this technology and has always described itself as an "experiment". The technology has matured and evolved to allow the tokenisation of almost anything. It is likely to begin with simple things such as commodities like sand, wheat, precious metals, energy, laws, titles of ownership, patents, and far into the future even more ethereal concepts of which we could not yet imagine.

It is likely to be a rough and turbulent time similar to the dot-com boom, whereby the internet allowed economic disruption and tangible advantage to companies embracing the technology. Perhaps over



2018 and 2019 as some of the larger corporations which have been researching and maturing DLT start to release their solutions, their economic value will increase whilst others race to catch up. The Innovators in the space which are already functioning and will be rolling out over 2018 have a tangible level of first-mover advantage and traction, and many may succeed to become the next Amazon's or Google's. On the other hand, most of the current crypto-landscape businesses and their relative tokens will not even make it out of the starting line and at least 90% of the cryptos are likely to fail to thrive or not exist in the coming years.

Likewise, in the coming decade, already established companies not embracing DLT will have to adopt, adapt and evolve or perish. The economic disruption caused by this technology is likely to affect the economic stability and current status quo of the traditional economic landscape significantly. Indirectly, this will also affect the wellbeing, employment and societal balance for individuals during this time. It will be a dynamic time and certainly advantageous to adopt, adapt and evolve ourselves dynamically as individuals in order to benefit from or sustain our own prosperity.

Certainly, "money" is likely to change and has already begun changing. Fiat currency is backed by and relies on the full faith of government – something that is being seen in shorter and shorter supply across the globe recently due to the rise of populism and sporadic social construct movements. A continuation of current trends in relation to fiat currency may likely end up being a contributor of further capital flight from fiat as money, and into crypto as money.

What to know before you invest

When crypto first came along in the form of Bitcoin, it was completely unregulated. Bitcoin's pure architectural resiliency and initial value proposition as a currency attracted many anarchists, purists and enthusiasts from many walks of life. Bitcoin's proffered notion of anonymity also appealed to elements of society for its use as a vehicle for money laundering and to a very small degree was used as such – although the numbers reported are heavily exaggerated.

The basis of being unable to link a specific Wallet Address to a specific person or entity is lessening and traceability is in most cases possible with effort. The technological prowess of law enforcement, as well as the calibre of capabilities of which we now know since the Edward Snowden leaks, coupled with continuous leaks from organisations such as Wikileaks has shown that with effort, traceability is certainly possible and anonymity in most blockchains to an absolute degree of certainty is impossible. There are some Blockchains that currently make the amount of effort required to identify the initiator of a transaction almost completely unfeasible for law enforcement. I believe that these Blockchains (AKA "privacy coins") will continue to exist, and persist, albeit shunned or declared illegal in future or make the use of such subject to penalty... eventually.

The regulation needed to de-anonymise the blockchain through voluntary means in forms of Anti Money Laundering and Know Your Customer (AML/KYC) requirements at the exchange layer and indeed at every other "capture point" possible has already begun being both enforced and adopted by the larger community. Further discussion of such is contained in this document under the Anti-Money Laundering and Counter Terrorism Financing chapter.



The period of being an experimental enthusiast toy, or a potential vehicle for crime is ending. Governments around the world are rolling out the regulation with haste. Many businesses of a very large calibre are almost ready to roll out their use of DLT. A new economy is forming and its velocity trend suggests that it increases beyond comprehension throughout 2018.

As an investment landscape it is full of opportunity, especially in a world where traditional investment vehicles are starving for yield. As long as you navigate carefully – VERY carefully, you can take advantage of the opportunity. If you still harbour the traditional crypto mindset of it being a “playground” of sorts, your actions may result in unwanted outcomes as the regulation and clampdown continues to surround the crypto world over the next 5 years. Prepare correctly from the beginning – which is now.



What Is Crypto?

If you are going to involve yourself in the crypto world, there is much to learn, but I will try to cover the basics here.

The current dominant blockchains

The landscape of dominant blockchains is likely to change over time. It is a lot more complex than this, and over time will become an absolute jungle, forming its own ecosystem. But for now, the leading technologies are as follows:



Bitcoin (BTC) was the first Blockchain and does not support "smart contracts (AKA "Tokens") until future software releases such as Rootstock (RSK). Ethereum in its modern-day form (ETH) is the most common smart-contract (tokenizable) blockchain and is used as "gas" to conduct transactions of both itself as a crypto and its "Tokens", which are referred to as "ERC20Tokens". All of its many ERC20Tokens operate on its Blockchain and share the over-arching ETH Wallet Address. Other blockchains also exist and have their own specifics in terms of value and potential. Be mindful of what your Hardware Wallet (Trezor or Ledger Nano S) supports in terms of your capability to securely store these crypto assets before you invest in a specific crypto.

In the overall crypto market at the time of writing there are about 1500+ various cryptos.

How does it work in practice?

Each Blockchain exists simultaneously around the world in a decentralised fashion amongst hundreds and thousands of nodes across the planet. To interact with these blockchains you use a "Wallet". A "Wallet" consists of two things – a **PUBLIC KEY** and a **PRIVATE KEY**.

Each KEY is a simple "string" of characters. And although confusing at first, when you develop and wrap software around the use of these keys and your interaction with the blockchain the usability and use-cases begin to show.

PUBLIC KEY: (Example looks like: "0x117fa382Eb6aA693862c34vb24a63BE5fet9Cvd0")

Think of this PUBLIC KEY as a BSB/Account number... It does not matter if it is seen by other parties as it is only used for receiving the Blockchain units of account in the ledger.

PRIVATE KEY: (Example looks like:

"8a6b6f45336961ff467b356f6c6e652c0aa1a3cb18e7caf018dxceex0x38229")

Think of this PRIVATE KEY as an almighty password which must be guarded immaculately. Anyone that has this key can essentially withdraw or send units of account from the corresponding Wallet (PUBLIC KEY) on the Blockchain.



Here is a picture to try to help you visualise how one would send “Litecoin” from one address to another.

Send payment

ADDRESS

AMOUNT ↑ LTC

FEE

Confirmation time cannot be estimated.
Fee: 0.000136 LTC

Do note that each blockchain has its own standard for the Wallet Addresses. The example of the above Public Key of “0x117fa382Eb6aA693862c34vb24a63BE5fet9Cvd0” is an address for the Ethereum Blockchain. Whilst in the screenshot above, the Address starts with “LQ3B36Yv2~” as that is in line with the standards for the Litecoin Blockchain.

You will come to see that this “Distributed Ledger Technology” in daily use, is essentially just the blockchain with graphical user interfaces wrapped around it.

Creation of cryptocurrencies and initial Coin Offerings

Who might create a cryptocurrency and what does it look like?

So, let's go back a step. There are 1500+ cryptocurrencies and more coming throughout 2018. But how do they come about? Well, this creation and access to cryptocurrencies is perhaps the most radical departure from ‘currency’ as it is presently known and understood by most people. As technology has matured and new business opportunities present themselves, there are a range of circumstances where creating a cryptocurrency might indeed be a completely rational way forward. Almost anyone can make a cryptocurrency — of course, this doesn't mean that they should. It is likely (and has already been seen) that without the cryptocurrency representing something of clear and potentially increasing value to a lot of other people, the currency will be worthless (i.e. no one will trust it has value). The process of presenting a new digital coin or token to a wider user community is known as an ‘Initial Coin Offering’ (ICO), and they have the potential to completely revolutionise business fundraising.

What is an ICO?

An ICO is an Initial Coin Offering, which is another way of describing the first sale event of a digital coin or token. Basically, a token or coin is a digital representation of the value of a product or service. When a business or organisation decides to create an ICO, they determine how much funding they need to establish or grow the product or service and then determine the liquidity of this funding by (usually) deciding how many coins will be offered. Most ICO's offer a limited amount of coins that can be



publicly traded around the planet – even if this amount of coins numbers in the hundreds of millions. From these determinations the cost of the coin is set. The business then publicises and advertises the forthcoming ICO (often referred to as a coin sale) and often there are bonuses for people who purchase the coins earlier in a sale. Normally, the business has named the amount of funds it is seeking and this is important to note; most coin purchases are done through 'smart contracts' whereby if a target is not met by a particular date, all funds are returned to buyers automatically, and if fundraising targets are met, the purchase finalised. It's important to note that in most ICOs the number of coins is hardwired into the initial creation of the coin itself, giving some measure of assuredness about the coins usage and possible future value (i.e. basic supply/demand principles).

As the name suggests an ICO is somewhat like an IPO (Initial Public Offering) of a company, in which they register on a stock exchange and their shares are publicly traded. Its important to note that share represent (part) ownership of a business; coins or tokens are best described as usually representing access to a particular service or platform but not ownership of the overarching business. Also different to the share market is the fact that, like the distributed nature of the blockchain, the checks and balances come not from a government regulator but from the blockchain community who seek to verify the bona fides of the new coin offering through research and consideration of detailed plans (a 'white paper') put forward by the development team as well as from other publicly available documents such as press releases, interviews etc. It is here that some general cautionary aspects regarding investing in ICO's need to be outlined:

- There are many stories of people investing in seemingly reputable ICO's which turned out to be scams. Throughout this book you're encouraged to take the time to seriously investigate the underlying principles behind any investment, and doing some due diligence on the ICO team is one of these fundamental principles. Double check the named members-do they exist on LinkedIn? Twitter? Do a Reddit search. Can you follow an employment history of the members? There are known instances of alleged team members having identities stolen to add credibility to projects. Do your research but also understand that one of the unique things about ICO's is that they are exposing potential investors to markets in which they may previously have had very little exposure. For example, Australian investors are likely to not have much experience with eastern Europe and South Korea, two 'crypto' hotspots – this both increases risk but also access to experts in these same countries.
- Look for partnerships- are they real or simply claimed? Saying you will partner with VISA is different to actually having the VISA partnership...many claims are made at present by some of the more unscrupulous operators in this space. Be wary.
- Ask yourself, do I really understand what this business is trying to achieve? This goes to the heart of investor vs. speculator sentiment.
- Use basic security measures like checking the authenticity of websites and never clicking on unsolicited links in emails. These relatively low level frauds still exist for the reason being that they still dupe enough unsuspecting victims.

Check what types of currencies the ICO accepts. Check how long they plan to keep funds in 'escrow.' Compare their proposed costing for their developments. Look for figures or timelines that look unrealistic or not feasible.



· Lastly, understand that most of the ICO's offered through 2017 and 2018 are likely to not exist in five years as a business or service and are in many cases replicating the dotcom boom of the late 1990s. Taking a long term, non-emotive view can help you assess ICO's on their merits and filter out some of the 'noise.'

Currently ICOs are mostly put forward to novel companies that want a quick and easy way to crowd-fund their business (or idea). This is how businesses can nowadays get funded by thousands of completely anonymous coin holders with currencies and technology that wasn't even invented a decade ago. In essence, it's a Kickstarter campaign on steroids, of which no one exactly knows the real value and implications (including legal) yet. This is an important point to reinforce —

investments in ICO's are not well understood by most investors; there is little to no legal recourse in the event an ICO is a scam and Governments around the world are scrambling to both understand and provide guidance and regulation around these ICO events. It is however worth also noting that through 2017, far more money has been raised in ICO's than through venture capital avenues. It seems like 2018 will be the year the sheriff (Government/ATO) steps into the Wild West with regulations and laws governing these areas. Be prepared.

Coins and tokens in practice

Let's say a big or promising company, such as Apple or Amazon or any company providing quality goods and services, decides to make its own cryptocurrency. In creating this cryptocurrency, they assure people that with that cryptocurrency, they will be able to buy Apple products and services. It is likely people will think that this currency has value because of what they can exchange it for. Such a currency is often labelled a 'token' or 'coin' (just like Bitcoin). Using a 'coin' in this way means that the business and the individual are transacting directly with each other rather than through a third party (such as a credit card provider).

So how is having an Apple coin or Apple token different from buying an Apple gift card? It is so in a couple of ways.

1. This Apple coin will not be tied to one currency. You could exchange Apple coin for McDonalds coin, Facebook coin, Bitcoin, or even US Dollars or Euros. This makes it ideal for a digital economy and commerce on a worldwide scale, meaning value is not lost moving money across borders.
2. The coin will (likely) be divisible. You can buy or sell 0.003 Apple coin for example. Or buy Apple products with 0.249 Apple coin.
3. The value of the coin will depend on Apple's relative value compared to other currencies (coins)

So, in this example, how is having an Apple coin different from having Apple shares?

1. Coins are a direct means of payment (value), shares are an indirect means of value, represented in 'part' ownership of the business as represented conventional currencies, subject to government protections and jurisdictions.
2. Coins are in most instances (still) a legal grey zone, whereas shares (being a shareholder) are subject to clear legal terms and conditions with governments possessing clear regulations and penalty regimes



for all participants breaking the law. Currently there is little to no recourse should an ICO prove to be a scam.

In a way, you can think of a coin in this example as a hybrid fusion of Apple gift cards and Apple shares. Imagine McDonalds and Apple both having their own coin, with their own relative value to each other, tradeable on an exchange. That means you could walk into a McDonalds with nothing but Apple coin in your 'digital wallet', quickly swapping your Apple coin for McDonalds coin on the exchange and buy a Big Mac. There was no Euro, Dollar or Yen whatsoever needed to complete that transaction.

Trust in future value by design

Just like any other currency, or shares, coins are usually issued with a limited supply, which is mostly set in stone before the coin is issued. This assures people that the coin will not suddenly be worthless by the issuing entity deciding to produce more coins, in a similar way to central banks when responding to certain economic situations, thus preventing 'hyperinflation.' By putting a hard stop to the 'coin production', trust is created in that no hyperinflation will occur through system changes — in other words, through the creators 'minting' more coins and therein diminishing the value of existing coins because of an increased supply. It does not, of course, guarantee that the coin will be devalued in other ways (such as lack of demand for the product or service, poor business plans, poor management of the overarching business etc. and therefore no value in the coin itself).

A word on Participating in ICO's – Be aware on what is being 'sold.'

So although cryptocurrencies are radically different to current practices in many ways, remember the following as a general rule of thumb— in crypto assets, like any other asset type, you're buying one of two types of asset. The first type is something that has an underlying product or service in which people find useful or desirable and therein will generate usage and (hopefully) value to you as an owner of this asset over time – for example, traditional shares or commercial property. The second type of asset is one which you buy and hold in the hope that over 'x' length of time, somebody else will subsequently buy it off you for more than you paid for it – classic artworks being an example of something which produces no value itself. Throughout this book you're encouraged to think for yourself and will come to (hopefully) understand the significant differences this kind of thinking can have on the ways you wish to be involved in cryptocurrencies.



Crypto Regulation Is Coming

For too long, the machinations of society have ignored DLT in all of its forms. The disruption that it potentially brings is beyond comprehension and indeed, societal disruption on many layers will happen. However, the days of the "wild west" in crypto are closing and a new chapter is forming in its lifecycle.

Authorities ignored cryptos long enough to the point that they could not ban it. They left it too long – long enough to evolve for it to actually prove its true value to humanity. Now they are in for a troubling age of digital disruption akin to the age of when Arpanet evolved into the Internet. Even the mainstay concept of value on our planet, "money", is likely to face significant disruption... although the change has a chance to be smooth – and I hope that is what is achieved. However, the first step in the more-or-less "orderly" adoption (especially over 2018) of this technology across the planet is Regulation!

Governments of different nations are taking different approaches of regulation, trying different strategies, but either way... it's an all or nothing end-game upon completion. Japan now sees it as legal tender, in 2018 Vietnam will also, while other countries have outright banned crypto, but the largest majority simply classify it as another asset in accounting terms. The disruptive nature this will have in terms of tax income and financial governance volatility across the planet is yet to be seen... but the regulation of such is coming.

It is time to prepare your holdings and get your house in order

All money is already inherently digital... but DLT just moves its current system to an immutable, almost invincible ledger. For years, the powers that be have been pushing for a cashless society to try to prevent any "money" being hidden from the hands that collect taxes and keep the glue of society in economic balance.

By watching the developing rollout of regulation around the world, it can be presumed that the next few years will involve ever increasing occurrence of regulation forming. Apart from the USA SEC slowly implementing small pieces regarding their corner of the world. We have nations not only trying to bring their own fiat currency into a DLT system in terms of a Crypto Ruble announced by Russia, a Crypto Yuan announced by China and even here in Australia, a "Digital Australian Dollar" being proposed. We can already see news headlines for the looming regulation on an ever-increasing basis globally. One such example as below.

<https://www.coinspeaker.com/2017/10/25/vladimir-putin-instructs-government-prepare-legislation-ico-cryptocurrencies-july-2018/>

Additionally, the Anti-Money Laundering and Counter Terrorism Financing Bill going through Australian parliament right now in late 2017 is likely to take effect in 2018 and affect many Australian crypto users.

This first wave of regulation, amongst many others, starts to form an increasing trend toward regulation, and you should start to consider the importance of your compliance whilst investing. This is especially



true if you do not want to be bothered later on in life by legislative liabilities from past actions. Prepare now if you are concerned.

For those of you that believe that taxation will not affect you

It may take 5 years, but with Data Matching and Artificial Intelligence retroactively scraping the blockchain at some point in the future, discrepancies in your compliance may form into liabilities as time progresses. Everything you do is recorded on the blockchain forever. It would be wise to be aware of potential future threats of confiscation or over-taxation of your portfolio, and mitigate risks appropriately.

Tax And Crypto

Now this is a big topic. Sincerely, if you have images in your head of wealth and lifestyle from your investment in crypto... I fully recommend that you comply with all laws regarding your tax obligations and take the matter with utmost importance. It is often those people, which have sudden changes in financial circumstances, that are the usual target to audits and interest from authorities. Take the time to understand your tax obligations seriously (and fulfil them), as some of the easiest and risk-free strategies can have multiplied returns through tax efficiency, and also the all-important include certainty of holdings. These strategies also can, through tax efficiency, contribute to your bottom line over time – and also help you develop your strategy for navigating the crypto landscape in a less emotional, more logical manner.

A lot of people in the crypto world completely ignore any idea of tax obligations when it comes to crypto. Many also have created a potential mess of liabilities for themselves in terms of keeping track of their crypto-related tax obligations. Hopefully this chapter of information brings light to the tax debate in crypto and encourages others to seek answers for safe investing.

Is crypto an asset or a currency?

This is one of the most commonly talked about and debated concepts in the crypto world. I say when it comes to crypto it does not(yet) matter what we call it, whether it be a commodity, an asset, or a currency... However, when you are talking in terms of accounting and tax, crypto is currently, and certainly, considered an 'intangible asset' in Australia. Intangible Assets are defined in the International Accounting Standards (IAS) alongside things such as goodwill, intellectual property, etc. A very funky way to try to fit 0's and 1's into a currently existing regulatory framework for accounting purposes, but that is what it is – at least in Australia. If not a resident of Australia, you should research and find out about the tax treatment of crypto as it pertains to your country – you will notice similarities of various countries tax laws and much of this information and the strategies contained in this document are applicable to residents of other countries.

In Japan, as of April 2017, Bitcoin is seen as legal tender, meaning it is treated as a currency in Japan. However, here in Australia, even after the removal of double GST taxation on crypto post July 2017 – for accounting and investment purposes, crypto is still treated as an intangible asset, and thus, is still subject to Capital Gains Tax regulations. The only change in the regulations regarding the July 2017 GST treatment adjustments, was exactly that – relating to GST treatment only.



Whilst many proponents in the crypto world would heavily argue that crypto should be treated as a currency and not an asset – I cannot see that being practical at this point in time. The population would immediately start hoarding all of their money in crypto due to the tax efficiency of doing such - hoarding specifically the more stable crypto's, as their hard-earned money would not suffer the same inflation which is inherent in fiat currencies and the appreciation of their crypto's purchasing power due to its deflationary properties and sheer demand. The exacerbation of such market dynamics would increase the price and capital appreciation of crypto's even further resulting in an exodus from fiat into crypto. Such an event would likely dry up tax revenue of many countries as the current regulatory structure for taxation of currencies is different to that of assets.

The treatment of crypto as an asset does make more sense for the long term, or until regulation can be made - as most things which will be tokenised in the new economy are already assets such as commodities, shares in a company, etc.

It is also of note that whilst the world transitions into the formation of this crypto economy, the current regulatory framework for which guidelines have been stipulated by the Australian Taxation Office (ATO) since 2014 should be adhered to strictly if you are to invest in crypto.

<https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/>.

Where regulation does not exist, you should do your best to navigate and comply with comparable tax legislation and guidelines to ensure your investments are indeed yours with certainty in the future. The tax treatment of Bitcoin and other cryptocurrencies as an "Intangible Asset" at least gives us much to work with in terms of quantifying and legitimising our tax obligations as individuals.

Different ways of investing in crypto require different approaches

It is important to note that crypto is notoriously easy to trade. A very large industry now exists whereby every man and his dog can easily swap back and forth between these crypto "assets" from his PC or phone. This has created a community in the crypto sphere which is more about trading than investing. In doing so, the average person, unaware of the tax implications of their actions, buys and sells volumes of crypto in an effort to achieve financial gain. No exact regulatory framework exists for crypto trading specifically addressing these actions, and as a result, the tax regulations, specifically in terms of the ATO's guidelines relating to the tax treatment of cryptocurrencies for taxation purposes apply. The most specific of these are it's handling as an asset and the consequent Capital Gains Tax obligations upon disposal.

On top of crypto being considered an asset, and hence, subject to Capital Gains Tax, any income from trading also needs to be declared as income. This is true for exchanges between fiat-to-crypto as well as crypto-to-crypto. Also, if you are consistently or regularly exchanging between different types of crypto, then your assets are considered to be "trading stock/inventory" of your "business", and any realised capital gains are going to be included in your taxable yearly income. This means a large yearly tax bill for realised capital gains and a potential crypto harvest discussed later in this document. Additionally, if you do not hold the specific crypto for greater than 12 months, you are not entitled to a 50% discount on your realised capital gain tax obligation upon disposal of the specific crypto.



Alternatively, if you simply buy and hold, not consistently switching between cryptos, such holdings will not be considered "trading stock/inventory" and will be held as assets (to you as an Individual), generating no tax obligations until later in the future when you finally dispose of them. This is something I am sure many in the crypto community currently overlook, or ignore completely. Keep in mind, that the Capital Gain is not "realised" until the asset is disposed of, and hence many strategies, such as those described further in this document can assist.

It is of note that after the epic rise of Bitcoin in 2013, the Financial Year (FY) 2014 ATO Tax Assessment contained a section requiring the declaration of any cryptocurrency Wallet Addresses on your Tax return. This was not repeated in 2015FY, and 2016FY, but I expect that it is likely to appear in the FY 2018 or FY 2019 Tax Assessment which you complete through your myTax portal. It is also of note that tax evasion is a crime and brings with it harsh penalties. So, if you are unsure of the tax implications of your newly acquired and unquantifiable crypto endeavours, ignore the advice in this document, and go see a large entity professional accounting firm if you are so compelled.



Capital Gains Tax

Tax as it exists in its current form for most western nations around the world goes off the idea as to claim tax on "income" (what is coming in). This means via your job, you pay income tax, and if you put your money to work in investments, any gain you receive from that investment is considered extra income and taxed when you sell it ("dispose" of it). This is called Capital Gains Tax. Although there are concessions of various periods of time depending on your country – you can receive a discount if you hold an asset for longer than a set period of time. In Australia, if you hold an "asset" longer than 12 months, you will only be taxed half (YES – 50%) of the amount of gain (at your individual marginal tax bracket). This means, if you buy an asset at \$1000, and sell (dispose of it) at \$3000, you have made \$2000. Of this \$2000, you would normally be obligated to pay the full marginal tax bracket as if that \$2000 was part of your income for that financial year. However, if you hold that asset for more than 12 months, you only need to pay half of what is otherwise owing on that gain (i.e. as if the gain was only \$1000 – only \$1000 will be added to your total overall taxable income for that financial year). This has compounding implications and should be taken into account for your portfolio's long-term growth and investment strategy.

When you dispose of the asset, that is when it becomes determined that it is part of that financial year's income. This is called a Capital Gains Tax A1 Disposal Event. This has profound repercussions, and strategies around it can be developed and are discussed in further depth in this document.

Capital Gains Tax is a seemingly benign way to try to capture your income for each financial year using time as the declarative variable. If you decide to hold your crypto for a period greater than 12 months, you only have to pay half as much on tax, which can be significantly affect your bottom line. However, due to the lack of regulation, and the fact that in Australia, crypto is seen as an 'intangible asset' for now – every time you swap Fiat (i.e. AUD\$) to crypto, you essentially exchange a form of currency or legal tender for an asset. If you exchange that asset for another asset (i.e. Gold for Silver), or for example, Bitcoin for Ethereum, you also generate a CGT A1 Disposal Event for the Bitcoin with its disposal price as the "Cost Basis" of the Ethereum asset. In short, the CGT A1 Disposal Event sadly also includes (in Australia), the swapping from one type of crypto to the other. A very sad fact indeed, but yet strategies for tax efficiency can be grouped around such legislation and they are shared in this document.

This also means that you need to be aware of when you are creating these Capital Gains Tax A1 Disposal Events.

<https://www.ato.gov.au/General/Capital-gains-tax/Selling-an-asset-and-other-CGT-events/Types-of-CGT-events/>

How is CGT calculated?

CGT is calculated the following way. When you acquire an asset, the price in fiat(AUD\$) for acquiring that asset is what your "Cost Basis" is. Basically, this is the price of which the asset is acquired and will be used in calculating future realised gains.



If you purchase an asset such as crypto in another country, and then sell it in another country, the capital gain is taxed based on the relevant market value of each in the local currency of which you are a "tax resident" for that financial year. This means, no matter where in the world you purchased it from and sold it for, the fiat value of the item in the country you reside for tax purposes for that year. This means if you purchase crypto from and international exchange, you can use either the price you paid if you have proof of purchase, OR its fair market value in your local currency at the time for both its costs basis and disposal price.

The "income" from realised capital gain should be included yearly in your Tax Assessment and will be taxed as income at your marginal tax bracket.

So, if you make \$40,000 per annum as an employee, but also generate \$20,000 Capital Gains from a short term crypto "flip", then your total taxable income for the financial year simplistically equates to \$60,000 and you will be legally obligated to pay:

Tax rates 2017–18

Resident tax rates 2017–18

Taxable income	Tax on this income
0 – \$18,200	Nil
\$18,201 – \$37,000	19c for each \$1 over \$18,200
\$37,001 – \$87,000	\$3,572 plus 32.5c for each \$1 over \$37,000
\$87,001 – \$180,000	\$19,822 plus 37c for each \$1 over \$87,000
\$180,001 and over	\$54,232 plus 45c for each \$1 over \$180,000

It is of high importance to note that if you had not sold your crypto during this financial year, then no CGT A1 Disposal Event would be recorded, and your assessable taxable income would remain at \$40,000.

Makes you wonder if it's worth selling doesn't it? This is especially true when you consider where/how you are able to make passive income from your investments in particular crypto assets based on their potential utility value or other means of passive income generation.



How to tax blockchain fork inheritances, airdrops and other crypto income
During the course of your crypto journey, you are likely to receive crypto in many different forms. For example, whenever there is a “fork” of a blockchain, such as Bitcoin, a new “copy” of said blockchain with all current block data at such time of the fork is created. Holders of units of account in one blockchain will automatically receive the same balance in the newly “copied/forked” blockchain. When you receive such a blockchain asset it is considered income.

The “amount” of income you have generated from this split depends on the “market value” of the new crypto at the time of the fork. This is quite a predicament because quite often a “fair” market value is not established as it may take time to be listed by exchanges and enter the free market for trade. It is definite that the tax authorities would want a slice of your new “income”, but no specific legislation around the handling of such an event exist. If you wanted to be safe you could wait until the specific crypto is established in the fair market, select its first day of trading average price as its value, and “attempt to pay” your taxes on said asset. This can be beneficial if you plan on holding the asset if you believe it will increase in value and keep the asset as part of your long-term holdings – as it makes the “Cost Basis” used to calculate your future CGT obligation higher than \$0.

On the other hand, if you decide to classify it essentially as a gift/donation which you consider the value at the time of receipt is \$0, then your Cost Basis for calculating CGT in some time in the future as \$0 also. As stated, not specifically worded legislation exists to provide guidance on this situation and the tact you take to either argue that it is worth \$0, or utilise its first identifiable “fair market value” as it's income and basis price is up to you. Be mindful that legislation may or may not be retroactive in the future.

It is also of note that “airdrops” are often done by various organisations. If you receive an airdropped crypto which already has an easily identifiable “fair market value”, then this arguably needs to be considered as income at the price of the crypto at the time which it landed in your wallet address. You need to declare this as income and pay tax on it during your yearly tax assessment accordingly.

You may also receive crypto from various other means such as staking, dividends, or simply being paid for your work or services in crypto. This you also need to declare as income and pay tax on it during your yearly tax assessment accordingly.

Preventing the annual crypto harvest

It is possible that if you are constantly swapping between crypto assets to try to get “more” - according to current laws, you are also creating a CGT A1 Disposal Event each time. This does not seem too bad, and you are after all just trying to trade right? However, the truth is, that when you do this, you need to, at the end of the year, compile all CGT A1 Disposal Events which you created and pay tax on any realised gains of each and every one of those events. This rule does not apply to “futures” or “synthetics” whereby it is essentially just a betting platform – however, your income from such platforms should be recorded and reported as income based on the cumulative fair market value of gain in AUD on each date (day) that a gain or loss is made.

However, when exchanging actual crypto to another type of crypto, the CGT A1 Disposal Event created also creates a tax obligation which means you will have to pay tax on any realised gain



created from such event in that tax year. June 30th each year marks the end of that financial year, and your corresponding Tax Assessment, which you complete in July, will require you to declare such gain and pay the ATO the tax from such gains.

I can see this becoming a never-ending loop for many people. And I warn strictly against it. Erring in caution. Imagine if you purchase 1x Bitcoin at \$2000 in 2017, then sell or trade that Bitcoin in June 2018 for \$20,000. You hence in June 2018, create a CGT A1 Disposal Event), whereby you have to pay your marginal rate of income tax (as this realised gain, becomes part of your annual assessable income) on an extra \$18,000. Unless you have a significant amount of Australian Dollars (fiat) laying around, you are likely to have to sell part of your crypto portfolio in the latter part of 2018 to pay the Australian Tax Office (ATO). The subsequent sale of a portion of your portfolio in the latter part of 2018, has again, created a CGT A1 Event for which you will have another tax bill in 2019. Speculating on significant increases in capital appreciation of cryptos it could be foreseen that a constant cycle of "crypto harvests" would be required each August-October in Australia in order to pay the ATO for any tax obligations of the previous financial year.

This cycle can set you up for many years of unwanted "offloading" of holdings in order to pay ATO obligations. This cycle keeps repeating, affecting your bottom line - and each and every year, you have to liquidate holdings to pay the ATO. The expectant Capital Gains Tax A1 Disposal Events experienced in this type of cycle can become unmanageable and can more severely hinder your investment strategy long-term than if you would simply hold.

Tax evasion penalties

Various Tax related offenses carry with them differing penalty unit amounts. More information regarding this can be found on the ATO website.

<https://www.ato.gov.au/general/interest-and-penalties/penalties/statements-and-unarguable-positions/>

In Australia, the ATO has a set Australian Dollar amount of \$210 for each "penalty unit" generated by any offences you commit under relevant tax laws.

<https://www.ato.gov.au/general/interest-and-penalties/penalties/>

To try to simplify the penalties, it can be described that if you fail to declare crypto related tax liabilities in your next Tax Assessment, then you can face a fine of up to 75% of the value of that shortfall amount on top of the actual owing tax shortfalls. In addition to this, you have a range of fineable offenses which carry with them those mentioned \$210 penalty amounts.

For example, Joe works as a tradesman and has made \$60,000 per annum before tax for the last 10 years. Joe bought \$10,000 worth of Bitcoin in August 2017. In June 2018 (right before End of Financial Year), his Bitcoin is worth \$120,000, he decides to rebalance his portfolio into a diversified set of various altcoins, and offloads all of his Bitcoin. In doing so, he has created a large CGT A1 Disposal Event. He has made a profit from his investment of \$110,000 and as such, needs to declare that \$110,000 on his tax return – and pay tax on it according to the marginal tax brackets applicable to him, as if it were income which he made this financial year. This would bring his yearly income to \$170,000 for that



financial year. He has held the asset for less than 12 months, and so his assessable taxable income for the year includes his normal income as well as a \$110,000 income from his realised capital gains as he is not entitled to the 50% CGT discount, because he did not hold the asset for more than 12 months.

When Joe is completing his tax assessment, his accountant advises him that he needs to declare the capital gain. Additionally, Joe has read the ATO website and 2014 guidance on Bitcoin taxation. Joe believes that there is no way that the ATO could track his Bitcoin as he has read that it is anonymous, and he even flicked back and forth between "privacy coins" to hide his movements. He takes the chance – intentionally not declaring the Capital Gain on his Tax Assessment.

Joe gets away with it, and in July 2019, he decides not to declare his crypto capital gains a second time. He also does not declare the income he has made from utilising his crypto holdings for passive income.

In August 2019, Joe quits his job and retires, giving his boss the finger on the way out. Joe continues to invest and amass his portfolio. Joe buys a House outright from a seller, buys a luxury car, and the Artificial Intelligence (AI) data matching between the land registry, as well as the car dealership and ATO databases causes a red flag to be raised. The AI picks up that Joe has only made \$600,000 before tax over the last 10 years, and the AI finds no matching loans registered to the house, and that the property is not specified as a security or "under finance" on his home insurance policy. Joe's new \$1,200,000 house and \$200,000 car, mixed with his financial transaction statements from both his Commonwealth Bank Account, as well as his crypto-linked VISA report discrepancies in his spending habits and a constant flow of spending from his crypto-linked VISA.

The Australian Tax Office and Australian Federal Police then continue to track all of Joe's movements and transactions, tracing back to any unidentified Blockchain Addresses to source his "crypto-stash". Transaction history on the blockchain reports many instances whereby much more income was made for the previous 3 years, than what Joe has declared on his yearly Tax Assessment. The Australian Federal Police (AFP) Anti-Money Laundering Unit continue to build evidence for a case against Joe. Once they have a clear enough picture and enough evidence to prosecute, Joe gets a knock on the door... One which he could have avoided.

Joe may now have to sell his new car and house at a loss in order to pay the ATO fines and overdue tax. The additional information which the AFP may have found whilst going through Joe's life may also present criminal charges which may also fit into the legislative framework for Anti-Money Laundering and Fraud also... However, in this chapter we are only evaluating the ATO's prosecution of Joe under the tax legislation.

Joe made many mistakes which increased his liability in terms of Tax.

Tax shortfall:

First, let's work out the amount of tax Joe should have declared and paid. We will assume Joe's crypto investments kept on switching as he regularly rebalanced his portfolio and he now holds \$1,500,000 worth of crypto and is liable for Capital Gains Events everywhere. The below example assumes that Joe had created a Capital Gains Tax Event to rebalance his portfolio in June 2019 – leading to a large



Capital Gain of \$1,380,000 for that financial year (\$10,000 original investment, \$110,000 realised gains for FY2018, and \$1,380,000 realised gains for FY2019) – Totalling the \$1,500,000 stipulated above.

On two occasions, Joe did not declare his Capital Gains for both the 2018 Financial Year and the 2019 Financial Year.

Joe should have declared the following as his tax assessable income:

FY2018: \$110,000 (realised capital gain) + \$60,000 (tradesman salary)

FY2019: \$1,380,000 (realised capital gain) + \$60,000 (tradesman salary)

What Joe then would have been liable to pay in tax can be easily worked out using the simple tax calculator.

Joe has already paid some tax which his employer deducts via Pay-As-You-Go (PAYG) Tax Withholding. Joe has already paid \$11,047 towards tax each year. This means that for the undeclared portion of his crypto income/realised gains which he has not paid results in the following shortfall amounts.

FY 2018 Tax shortfall = \$39,485

FY 2019 Tax shortfall = \$610,185

Joe will be required to pay these amounts to the ATO and will also face a series of fines because of his actions.

Fines:

False or misleading statement fines apply, because Joe intentionally did not declare the income/realised gains on his Tax Assessment. He did not even attempt to make a guess and report during his Tax Assessment period. The fines have varying penalty percentages based on your level of disregard for your tax obligations. For this example, because Joe did not make any sort of reasonable attempt to declare his crypto gains or income, he faces a penalty which is 75% of the shortfall amount. This amount is just simplified, although the penalty amount can be increased or reduced if there are aggravating or mitigating circumstances. However, in this simple example, this means that Joe needs to pay additional penalties of 75%:

FY 2017/2018 = \$29,614 (tax shortfall x 0.75)

FY 2018/2019 = \$457,639 (tax shortfall x 0.75)

Additionally, Joe may also face additional fines for his failure to meet any of his other tax obligations as shown in this table below:



Penalties for failing to meet tax obligations

Tax obligation	Penalty for failing to meet obligation
Keeping or retaining records as required	20 penalty units
Retaining or producing declarations as required	20 penalty units
Providing access and reasonable facilities to an authorised tax officer	20 penalty units
Applying for or cancelling goods and services tax (GST) registration when required	20 penalty units
Issuing a tax invoice or adjustment note when required	20 penalty units
Both principal and agent must not issue tax invoices or adjustment notes for the same taxable supply or adjustment event	20 penalty units
Registering as a PAYG withholder when required	5 penalty units
Lodging an activity statement electronically when required	5 penalty units
Paying an amount electronically when required	5 penalty units



Each penalty unit holds a value of \$210. Hence, if Joe is also pinned with 60 penalty units, he has additional fines of \$12,600.

This brings Joe's total overall Debt to the ATO to:

Un-paid shortfalls = \$649,670

Penalties on shortfalls = \$487,253

Additional fines = \$12,600

TOTAL = \$1,149,523

Joe now has to sell his new home and car, and has essentially lost more than 78%+ of his crypto generated wealth. Joe has also lost one of the most critical variables that affect his wealth – TIME. Whilst Joe's example is simplified. I hope this illustrates the importance of not only investing in crypto strategically (as not to create large Capital Gains Tax events unless necessary), but more importantly, to become familiar with, and adhere to the tax laws of your country.

Tax summary

Courts regularly have made it clear that people who commit tax evasion should not expect lenient penalties. A lot of people happen to be drawn in by the crypto world and trade to the point of making their income and crypto holdings so messy that reporting an accurate number has become impossible... what the future holds in terms of regulatory developments, we do not know. However, every step is being recorded on the blockchain and is time/date stamped... available forever. It is also possible that due to the disruption to the tax, and tax collection of its residents, governments may take a harsh, and less magnanimous approach to the enforcement of laws in the developing crypto world. Take the time to self-educate on anything applicable to your circumstances.

It is hard to estimate where governments will go with trying to tax crypto. Perhaps they will introduce a "Tax-As-You-Go" method, whereby governments apply your tax obligation in real time by matching timestamps and events within the blockchain. Perhaps they will make blockchain mining activities a function of the state infrastructure for National Security reasons – meaning that they essentially make taxes by doing the mining (unlikely). Perhaps taxation on income will be eradicated completely and taxation will be collected based on spending or expenses instead, similar to Value Added Tax (VAT) in other countries. What the future holds we do not yet know... but one thing is for sure – it is going to need to change.



Personal Finance Structuring

In order to be able to develop efficient strategies around your journey in the crypto landscape, it is important to know how to structure your financial affairs accordingly. For example, as an Individual, you may want to just invest for the long term and have no intention to ever trade or generate a CGT A1 Disposal event until far into the future. On the other hand, you may see opportunities of making money from crypto by trading. You may also see opportunities in crypto by providing value to the crypto community or building useful software, websites or information resources.

In order to ensure your Tax compliance during the journey, you should decide your method of approach beforehand and take appropriate precautions to not “mix and match” financial structures or make a mistake which could leave you liable to unwanted tax obligations.

In Australia you must declare all of your income for the purposes of paying income tax – this relates not just to individuals, but businesses also. It is important to realise that your activities in the crypto landscape may actually be considered as “carrying on a business” by definition, and you would need to structure your personal financial affairs accordingly.

Hobbyist/Enthusiast

You can generally have a “hobby” on the side of anything you endeavour, which may generate income as a by-product of the hobby, but you must be seen to not be “carrying on a business”.

If, however, you are an old-school software developer that likes to tinker and has bought small amounts of various cryptos for the purposes of testing software or finding security bugs, hacking for fun, learning the tech, etc, then it is likely you are carrying on a hobby, but not a business. Other considerations not listed can come into effect also, such as if you don't make more than \$20,000 profit per annum from the hobby and have a trail of proof of your uses in such hobby. If your only interest in the crypto landscape is that of a hobbyist or enthusiast – Congratulations, as your affairs are easy to manage.

Are you an investor, a trader, or hybrid?

For the majority of those entering the crypto landscape they will be entering in order to make a profit. The closest related regulative framework for investing/trading crypto is that of investing or trading shares. Whilst regulation does not exist with specific mention to cryptocurrency, it is only a matter of time before the regulation is created and such regulation is likely to follow similar framework for that of shares and other assets.

There is also a lot of grey area whereby the authorities could argue in court that you were indeed “carrying on a business” due to your trading activities or investment activities in crypto. It is however possible that in the future, someone will be dragged into court for a ruling to be made on such a distinction. Either way, from the ATO's perspective, you will likely be liable to the same obligations of income tax using the same, or similar thresholds and criteria as shareholding/trading in future legislation for crypto as it is rolled out. It is best to be prepared.



Both investing and trading are done with the intention to turn a profit or achieve a financial benefit. However, the way in which an Individual is taxed, or expected to manage their affairs are different for investors and traders. When you engage in such actions as trading or investing you need to understand what your objectives are and structure your personal financial matters to suit. This may mean registering an Australian Business Number (ABN) or another legal structure to encompass your activities for legal and taxation purposes.

Investing as an Individual

It is quite common for Joe Citizen to purchase shares (usually through a broker), and hold them with the intent of long term wealth accumulation. Similarly, as a crypto investor you may purchase crypto for the same purpose. The purpose may also include profit distributions in terms of dividends from utility tokens, staking, airdrops, and other forms of passive income, not just capital appreciation. It is of note that investing and holding crypto as an "Individual" is a rather easy and straightforward process to manage and record. You as an Individual receiving those passive dividends, staking, airdrops, etc can easily declare that as extra assessable income on your Tax Assessment without the additional overhead of "carrying on a or business" according to the ATO's definition of such.

Carrying on a "business" in crypto

Many tokens have the ability to generate a passive income for you. This can come in many forms from simply holding them in your wallet and receiving free airdrops, to actively running a node to "stake" the tokens if the crypto uses the Proof-Of-Stake consensus protocol or actively trading on multiple exchanges to try to turn a profit. Additionally, and ever more increasingly in the future, utility tokens may require some input from a user utilising their tokens on a web platform in order to receive income from them.

If you are actively trading, you have a legal obligation to register for an ABN and record all matters of your "business" endeavour accordingly. If you are an Individual and have to take action with your tokens in order to get a passive return from them, and gain a significant passive return from those investments, you may want to get an ABN also. Specifically, you need to consider the following criteria for the ATO to consider whether or not you are "carrying on a business".

- You intend to make a profit
- You repeat similar types of activities
- The size and scale of your activities are similar to other businesses in the industry
- Your activity is planned, organised or carried out in a business-like manner

<https://www.ato.gov.au/Business/Starting-your-own-business/Before-you-get-started/Are-you-in-business-/>

The efforts you put into staking such as setting up secure server/firewall environments to stake your crypto, or performing some other action such as interaction with a web application to essentially utilise your tokens in order to turn an income, can be reflective of a business and not a hobby. As such you are obligated to acquire an ABN, keep track of all records and declare appropriate taxes. This is not always a bad thing once you really endeavour for efficiency in understanding the structure and



corresponding processes. Registering for an ABN could allow you to declare tax deductions on the taxable income from those efforts on things such as a (very small) percentage of electricity, office expenses, the computer equipment, account keeping software, learning materials, and other expenses related to carrying on such activities.

Trading to turn a profit

Now here is where many people are likely to fail to understand their obligations and fall short of looking after their affairs or keeping records. These are the ones most at risk of being burnt by legislative crackdown over 2018 or further in the future. Some will try to hide their gains, others will prefer the certainty that they are tax compliant and can go on enjoying their investment returns indefinitely, while others will sit on the fence. See the section regarding "Legitimising your Stack", for some ideas to begin the process of solidifying and legitimising your portfolio if you want such said certainty.

If you actively trade crypto with the intention of making a profit, whether you do turn a profit or not, it is likely that you will be considered as carrying on a business. The criteria for carrying on a business are just too broad, such that trading crypto in any significant way would be considered an enterprise, and hence you are "carrying on a business". Your ability to argue in a court that your trading activities are a hobby is almost impossible. A business, according to the tax office, includes "any money-making activity where you are not working as an employee". Additionally, registering for an ABN not only allows you to take advantage of tax deductions where applicable, but are important for separating your "trading stock/inventory" owned under your ABN and your long-term holdings which you hold as an Individual.

Many that enter the crypto trading landscape may only do trading for a temporary period of time, whereby as an individual, you may have some crypto holdings which you plan to never sell, or sell years from now. If you do not take efforts to separate the ownership of the crypto used for trading under your ABN, with the crypto used for long-term holding by you as an Individual, you may encounter issues taking ownership of such assets when you cease to trade and deregister your ABN. You may also be exposing yourself to unwanted tax obligations for your long-term holdings as an Individual, as they may be legally misconstrued as "trading stock/inventory" for your trading "business". When your trading (or other) endeavours ceases, if your entire inventory is mixed with other holdings used as trading inventory, you technically could create unwanted CGT A1 Disposal Events when passing ownership of your "business inventory" to yourself as an Individual. A small business CGT concession allowing a "rollover" of the ownership does exist, but has specific eligibility criteria, which without appropriate regulative framework and expansion to include crypto – you are not likely to explicitly qualify for.

To prevent your long-term holdings from being considered as your business' "trading stock/inventory", you should endeavour to get an ABN, setup a separate AUD business bank account in the name of the ABN and then transfer any funds you intend to trade with from your personal account fiat bank account into your ABN's bank account before sending it to an exchange to then enter the crypto trading world. You should also use separate Wallet addresses for trading activities linked to your ABN, to those that you use for long term holdings as an Individual.



Hybrid trader/investor

A Hybrid Trader/Investor understands all of the above and below, and keeps funds strictly separate (including separate individual/business fiat bank accounts for each business endeavour). They could make a loss trading and claim such a loss as a tax deduction on future gains. Likewise, they usually are trading only to increase their temporary (at the moment) income, in order to increase their overall holding position as an Individual, and route the funds accordingly, converting profits from trading into fiat in their ABN owned bank account, transferring said fiat to their personal (Individual) bank account before repurchasing any desired long-term crypto holdings. They also declare income from said trading and pay tax on it.

If hybrid, you may also have an ABN in order to declare the passive income you receive (dividends, staking, airdrops, etc) via your ABN as separate to trading activities. Either way, they tax-deduct computer equipment such as servers, firewalls, electricity (% based), as a deduction to the assessable taxable income to their other passive income activities that are not trading. It is however rarely efficient to have multiple ABN's for separate endeavours. If your endeavours eventuate to be quite significant, you may even find yourself registering a Pty Ltd.

Keep in mind that you should have greater than \$20,000 profit per annum for each separate "business" endeavour for it to be considered a business and not a hobby. You may also have to register for Goods and Services Tax if your yearly GST turnover (gross income minus GST) is of \$75,000 or more.



Keeping Records Of Crypto Endeavours

Once you start to understand your tax obligations and your desired personal finance structure, you may or may not require an ABN. You will immediately begin to realise the importance of keeping records of everything. Specifically, if your endeavours in the crypto world require you to register an ABN, then recordkeeping becomes necessary. Whilst you can keep track of your recordkeeping via simple spreadsheets, this becomes rather cumbersome. There are a few software packages that may help you. First, some notes on the method of calculation of Capital Gains Tax.

Put simply:

- If you buy your crypto and hold it, rather than trade it, keeping records for you will be a very simple task and you are not likely to create many CGT A1 Disposal Events throughout the financial year – and so a simple spreadsheet will do.
- If you are constantly exchanging or swapping between different crypto's or trying to generate an income via trading, or other income generating endeavours through crypto – you will want to keep immaculate records to be able to accommodate and fulfil any liabilities which you may have to tax or other regulations which may come in the future.

The First-In-First-Out (FIFO) method for calculating Capital Gains Tax

As shares and the handling of shares as assets are the closest similar asset class to crypto assets in terms of accounting methods used for Capital Gains Tax calculations, the following is worth knowing.

74. If a taxpayer can identify shares by reference to individual numbers, or maintains appropriate accounting records, as explained earlier in this Ruling, the taxpayer must use the specific identification method for CGT purposes. However, if the taxpayer is unable to identify the shares, the taxpayer will be required to use FIFO for the purpose of determining the capital gain or loss. Where it is possible to specifically identify the shares appropriated to a particular trade, that method should be used for both calculations.

<http://law.ato.gov.au/atolaw/view.htm?docid=TXR/TR964/NAT/ATO/00001>

Various investment vehicles have allowed different methods for calculating Capital Gains traditionally, such as “pooling assets” together into “lots” and being able to specify which “lots” you sell when disposing of the asset. Other methods include averaging out the Cost Basis of your asset holdings in a method called Inventory Averaging. It is understood and advised by many financial and tax advisors in the crypto world that these methods are not acceptable, and similar advice is contained within the Australian 2014 Guidance Papers relating to Bitcoin and other cryptocurrencies. The actual method which you are required to use to calculate your Capital Gains Tax obligations for crypto is a system known as First-In-First-Out (FIFO).

The FIFO method dictates that whichever specific asset you purchase first, is also the one considered to be disposed of first. This affects the way your Capital Gain is calculated. For example, if Joe buys 1 x



Bitcoin (BTC) for \$1000, then 6 months later, purchased another 1 x Bitcoin(BTC) for \$2000, he now holds 2 x BTC in total. After holding for another 3 months, Joe sells 1 x BTC for \$4000. With the FIFO method, Joe has a Cost Basis of \$1000, and a Disposal Price of \$4000, giving him a Realised Capital Gain of \$3000 – as the Cost Basis is worked out using his very first BTC purchase. Joe then has to declare a capital gain of \$3000 on his next tax assessment. Joe could not reasonably fulfil the requirements of proving he sold a particular “lot” of BTC, unless every single crypto purchase he makes is stored on a separate wallet (perhaps separate “paper wallets”) and specifically disposes of said specific lots linked to those wallet addresses. Additionally, without the required regulatory framework, Joe may be forced to use the FIFO method anyway.

Of particular note with the FIFO system is that it can be notoriously hard to keep track of when Joe decides to spend a bit of BTC here and there, before finally cashing out half a BTC, then spending some more, then buying some more, etc. It is necessary to keep track of all of the complexity to ensure you are accurately keeping track of it, and something like that is quite hard to do in a basic spreadsheet. This is where it becomes necessary to use a software to track your crypto endeavours correctly.

Accounting software quirks

There exists accounting software which is commonly used to track the holdings of a business. Two of note are QuickBooks and Xero. Unfortunately, although these two mentioned software packages do a great job of looking after and recording any affairs of your ABN and other business endeavours, both fall terribly short in terms of tracking crypto endeavours.

Quickbooks requires the enterprise version in order to be able to keep track of an inventory using the FIFO method, and even then, it does not allow more than 3 decimal points to be added to the quantity of the inventory item in question. This makes accurately tracking any cryptocurrency (some of which have 18 decimal places) inaccurate and useless. Additionally, the recording of price information in is tedious and manual.

Xero on the other hand offers no option for a FIFO method of inventory recordkeeping. Although one Xero plugin exists called “Sharesight” which allows the FIFO inventory tracking, it unfortunately falls short. Sharesight is excellent and extensively accurate with their tracking of the FIFO method, and the provision of Capital Gains reporting and tracking for tax purposes. However, Sharesights' ability to accurately track and or record custom inventory items (such as cryptos) presents many errors and bugs. Additionally, fetching price information is still manual and time consuming for something that will not work in the end anyway. Although the Sharesight/Xero combo seems promising as Sharesight have implemented a “beta” for tracking Bitcoin in their platform (buggy), I think they fall short of looking after the myriad of customers which will be holding a portfolio of 10-20 out of a market which is expected to be 10,000-100,000+ (in 2018) various cryptos in the coming years.

Ideally, it is best to use Xero/QuickBooks (or other) accounting software to manage your business (ABN) or Self-Managed Super Fund affairs and tracking your crypto endeavours separately. The best software the author has found to do this for now (as of Q4 2017) is <https://cointracking.info>.



CoinTracking (<https://cointracking.info>) allows you to track your crypto's via this FIFO method and provide records of any Capital Gains come tax time. I am not affiliated with Cointracking.info, although I have found it to be the most decent tool to use to keep track of your cryptos.

Keeping separate bank accounts for separate activities

It is worth mentioning here that if you are doing anything more advanced in your personal financial structuring, that you will want to have separate Bank Accounts in the name of each entity in order to keep separate any endeavours which may have separation requirements. Separation requirements may be having a separate bank account and separate crypto-exchange account for yourself as an individual and yourself as a trustee/director of your SMSF or yourself as an ABN holder (Sole Trader). Another example would be to get a business bank account in the name of your ABN, which is then used to get in and out of the crypto world for trading purposes, as not to mix up your personal long-term holdings as an individual with the constantly swapping short term trading activities. This is important for separating the holdings of each entity and preventing the ATO from potentially mixing the holdings of an ABN with your long-term holdings as an individual – as the tax treatment is quite different for each model (shareholder or sharetrader <> cryptoholder or cryptotrader). If investing in crypto within a Self-Managed Super Fund, your understanding of the importance of this separation must be immaculate.



Anti-Money Laundering/Counter-Terrorism Financing And Crypto

One of the most striking things to be prepared for in the crypto landscape is the regulation, which is coming into effect over time to combat Money Laundering. Whilst failing to fulfil your Tax obligations will land you fines which will severely impact your overall holdings if not adhered to... the consequences for not being aware of Anti-Money Laundering regulations could be more severe. At the time of writing this document, there is currently legislative draft's passing through the Australian Parliament aimed at combating Money Laundering and include specific inclusion of crypto matters. Many of the proposed changes to the current Anti-Money Laundering (AML) legislation are quite harsh and it is extremely important not to ignore them. I will go through much of what is discussed in the legislative draft and prospective future for crypto in Australia when it comes to hardening your holdings against being caught up in the AML legislative framework even inadvertently.

It is important to note that Money Laundering is the act of trying to hide income which may be linked to a crime. This highlights a special point that many in the crypto world may not want to declare gains which they have made in the crypto world so far and try as hard as they can to hide said gains. However, for those that wish to be 100% sure that they can never lose their crypto holdings due to legislative liability contained in AML legislation – **The best thing is to have proof that you purchased your crypto (receipt) and that it was done with legitimate income which has already been taxed appropriately (i.e. salary).** Otherwise, should allegations be placed upon you in terms of attempting to launder money via crypto – you can potentially kiss your whole portfolio goodbye until you can provide such proof. Many in the crypto world will gawk at such a preposterous idea and would probably vehemently state that the government does not have the human resources or proof to identify various crypto transactions such as those associated with privacy-centric coins, etc. If that is what they would like to risk, then that is their decision. Alternatively, and especially if you are a new adopter – focus on paying with legitimate origination of funds and acquiring a receipt on your way into crypto. You may never have to 'whip out the receipts', but I would rather have them and not need them, than need them and not have them.

Your risk mitigation strategies are your own, but this document contains a lot of elaborate material on the subject which always errs on the side of caution and limiting potential blowback from legal liabilities.

Overview of the latest AML/CTF regulation

There is currently a Bill going through parliament which aims to tackle the AML/CTF aspects of the crypto world. It is important to all who hold crypto to learn and observe its progress and implications. The explanatory memorandum of the recent Bill states, "These measures will have a positive financial impact by helping to prevent fraud against the Commonwealth and increase recovery efforts".

The draft Bill for the amendment of AML legislation brings a lot to be mindful of. In no specific order, I will note the current concerns of this likely legislation. It is of note however, that the proposed legislation



includes a 6-month grace period for compliance upon being passed – so those who take the time to interpret the effects of this legislation can prepare – this Bill is likely to affect many current crypto holders or traders in 2018.

Right now, in the crypto world, a lot of people are taking advantage of various last vestiges of anonymity which still exist due to the lack of regulation. Do note that these doors will close in the coming years. Keep an eye on any news and take the time to interpret the final passed legislation around AML when it finally gets passed. Self-educate and risk mitigate responsibly.

Regulation of digital currency exchange providers

The proposed legislative change would require "any person" (which means an individual or corporate entity) to be a registered digital currency exchange provider and comply with all transaction reporting requirements with AUSTRAC. This could mean that any exchange of digital currency such as those currently selling via localbitcoins.com or similar interpersonal transactions could be arrested, charged and punished according to the legislation if they are not registered. It is of note that this is no joke, as there are similar regulations in some US states with examples of people being arrested and charged for such actions already. How this eventuates, and whether the legislation ends up including exceptions for small transactions (such as <\$1000) is yet to be seen.

In short, it is important to understand that under the legislation, anyone desiring to perform any action relating to being a "registrable digital currency exchange provider" will face some very harsh prosecution if they do not register with the Australian Transaction Reports and Analysis Centre (AUSTRAC) as a digital currency exchange provider. Keep an eye out for the finalised AML Bill, as this may affect you if you are currently "selling" bitcoin or doing cash transactions via localbitcoins.com or any other means. It is also of note that the market availability to buy crypto through another person on "localbitcoins.com" is a market which may very well disappear in Australia in 2018.

Expansion of powers of AUSTRAC

The Bill additionally states some of its objectives as...

Provide regulatory relief to industry with measures such as clarifying due diligence obligations, qualifying certain terms and allowing certain bodies to share information; strengthen AUSTRAC's investigation and enforcement powers by expanding the powers of the AUSTRAC CEO; and give police and customs officers broader powers to search and seize physical currency and bearer negotiable instruments (BNI) and establish civil penalties for failing to comply with questioning and search powers;

That is correct – you read it – they used the word "seize". As a crypto enthusiast you may very well think that "good luck to them with that" ... as you would need to provide your private key to them in order them to actually "seize" your crypto. Whilst you may initially think that you would never give them your private key... there are provisions of punishments in the bill for refusing to surrender your crypto to them. Whether this includes your private key, or just your public key is not stated or discussed in the legislation, but considering that they usually confiscate any and all assets if you are alleged to have tried to launder money or the like, it may be presumed the worst case (private key) should be prepared for. How they will do this in future is yet to be seen, whether they transfer the crypto out of



your wallet into a wallet owned by the enforcement agency temporarily or not, is yet to be seen. It is at such a time that proof of origination of funds and receipts may come in very handy and be the only way to prove ownership.

Currently the seize part is only applicable when the funds are associated with a financial crime at the border and exists to prevent international money laundering predominantly, however these powers may expand in future. If you are cautious and protective by nature, you should prepare for the worst-case scenario and work to legitimise your proof of ownership of your portfolio as much as possible.

The Explanatory Memorandum of the Bill also states...

This would enable police and customs officials to demand to know how much money is being brought into or leaving Australia by travellers as well as order that money is produced upon demand.

Presumed innocent until proven guilty?

The Parliamentary Joint Committee on Human Rights (PJHCR) has raised concerns with the current draft Bill and is awaiting a response. They stated...

However, in this case the measure does not appear to be consistent with criminal process guarantees. For example, the application of a civil rather than a criminal standard of proof raises concerns in relation to the right to be presumed innocent.

It will be important to see if this concern is addressed in the final draft.

Strict liability offences

The specificity of the Bill is somewhat troubling and one such mention is that of Strict Liability Offences. Here is a dump of some extracts from the Explanatory Memorandum regarding the mention of Strict Liability Offences.

The bill amends the AML/CTF Act to establish a number of civil penalties in relation to an unregistered person providing digital currency exchange services, which are all subject to strict liability... it is not necessary for the prosecution to prove an associated fault element—such as intention, knowledge, recklessness or negligence.

...as a matter of principle, the Law Council does not welcome the notion of strict liability offences, more particularly, when it involves the potential for long periods of imprisonment. With an aggravated offence, the maximum penalty goes from two years to four years, and I think that, if the AUSTRAC CEO has given more than one notice, it's into a more aggravated category and it's a maximum of seven years. Given that there is no defence at common law—other than the defence of a reasonable mistake of fact, which carries with it certain requirements for the defence to establish—that is draconian.

Under general principles of the criminal law, fault is required to be proved before a person can be found guilty of a criminal offence (ensuring that criminal liability is imposed only on persons who are sufficiently aware of what they are doing and the consequences it may have). When a bill states that an offence is one of strict liability, this removes the requirement for the prosecution to prove the



defendant's fault. In such cases, an offence will be made out if it can be proven that the defendant engaged in certain conduct, without the prosecution having to prove that the defendant intended this, or was reckless or negligent.

It is items like this Bill which may unfortunately catch some undeserving crypto investors and enthusiasts off-guard in the future and I recommend that everyone assertively self-educates to mitigate any potential liabilities in their life which may come of future regulation of cryptocurrency endeavours. Whilst it is unlikely that the enforcement of such measures is going to affect each and every person – “the first man through the door is the one that gets shot” ... and early adopters may be a prime target to set and make an example of.

If you want to be 100% confident that you do not have to worry about such things – take extra effort to keep up to date with all of developing regulations and ensure you do what you can to “legitimise your holdings” against such potential future regulatory liabilities.

Other noted concerns of the bill as it stands in draft form

Here are some excerpts from the explanatory memorandum to highlight the importance of learning about and following developments regarding this legislation.

- *The Australian Bankers' Association (ABA) noted in its submission that the phrase 'other serious crimes' is used in the bill, but the words 'serious financial crimes' are currently used in the AML/CTF Act. The ABA stated that the expanded scope of the phrase 'other serious crimes' would result in every relevant organisation being required to expand their transaction monitoring scenarios to include crimes of a non-financial nature.*
- *The bill seeks to introduce a new designated service and register in order to regulate digital currency exchange, to be introduced within six months of the bill's commencement.*
- *The proposed legislative amendments do not seem to contemplate for the likely scenario that an individual can simply choose to exchange with a digital currency provider outside of Australia's national jurisdiction, one where the rule of law and reporting requirements in according with [Financial Action Task Force] guidelines are not adhered to stringently. In light of the highly mobile nature of offshore criminal networks, this is a matter that does not appear to have been adequately considered.*



Do You Actually OWN Your Crypto And Can It Be Taken Away?

There is an old saying that goes “if you don't hold it, you don't own it”. And whilst that is definitely true... I would like to address the importance which is stressed in this document regarding compliance with Tax and AML/CTF regulations as they relate to the crypto world.

Ultimately if you are investing and working hard in a desire to get something out of your journey in the crypto world – it is foreseeably just as important to protect your holdings from tax and regulatory liabilities as it is to protect from hackers and scammers. If you are serious enough to think that you will still be investing or holding crypto in a few years, or even short term, then appropriate measures should be taken to ensure that what you hold is what you really own.

Establishing proof of ownership

I will take the time now to stress with utmost importance that you should go through extraordinary lengths to ensure that you have proof of ownership. This means not only that you have a receipt for your crypto purchase, but also that you can prove that those funds came from a legitimate source of income. Specifically, in terms of the AML/CTF legislation, it is important to have a legitimate explanation of where the funds used to purchase your crypto holdings originated from. Under AML/CTF regulations, the ability to confiscate crypto assets if they are suspected to be linked to a crime exists. We also know that it is a punishable offence to hide your holdings if your funds are suspected of being linked with a crime.

To this end, you want to not only make sure that you are not laundering money intentionally or unintentionally (note strict liability offence section above). You should try to purchase your crypto holdings from a source of money which is legitimate such as a salary from a full-time job, or other source of funds which have already been appropriately taxed. This is most easy to prove if the funds original from a legitimate Australian bank account with a legitimate financial institution – so unfortunately, buying your crypto from a local seller you met online with cash, may not fulfil your desire to have bulletproof evidence of your ownership.

With regulation on the horizon, now is the time to “bolt down the hatches” and secure your crypto holdings to ensure you are not affected by future regulation rollouts. If you have already been in the crypto game for some time and wanted to “legitimise your crypto holdings”, the next chapter aims to suggest ideas around ways you could legally do such.



Legitimising your crypto holdings

Ideally all of your crypto holdings should come from a legitimate source of income and recording its transmutation from a valid income source, into an Australian Bank Account, then being sent to an exchange for the purpose of purchasing crypto, and to have a receipt for such purchase. Your records should also then include the traversal across any blockchains when you trade/convert one crypto asset for another (this is where cointracking.info helps).

Ideally, you want nobody to be able to come and take your crypto in the future, so that you can enjoy the benefit of investment reward from them, especially if it involves great effort on your behalf. It is not mandatory that you take the effort to "legitimise your holdings" as suggested in this document, but rather a recommendation for those that desire it and where only the best protection and certainty will suffice.

If starting fresh...

If you are a newcomer to the crypto world, and are starting fresh, you should not begin until you have the following:

- A clear plan of what and why you want to invest, and an understanding that you are investing in a considerably high-risk asset.
- Your personal financial structure planned and understood.
- One or many Hardware Wallets – Trezor or Ledger Nano S.
- An understanding of Security concepts in this document both Technical and Physical
- An understanding that everything you do has consequences and that "moves" or actions should be thought out carefully beforehand, and recorded considering tax obligations.
- An emotional resilience to ignore all the Fear, Uncertainty and Doubt (FUD) that exists as created by the predatory players in a largely unregulated market.

If the above is all adhered to, you should have relatively few events of "tripping over your own feet" in terms of exposure to unwanted liabilities.

If you have already been in the crypto game a while

In Australia, there are a multitude of laws whereby your crypto's can be taken away or confiscated just because you couldn't prove they were yours. For example, if you were previously in the business of drugs and utilised crypto for your drug-related endeavours, they would just show up to your house and take the lot. The onus would be on you to prove via receipts of purchase from a legitimate income and evidenced in the blockchain to prove that you are the rightful owner of such said crypto stash. It is important for legitimate crypto investors to separate themselves from the affairs of the criminals of this world and responsibly record their legitimate ownership of their portfolio.

If you are certain that you have not conducted any illegal activity with your crypto's, but wanted to gather the desired proof of ownership and receipts to mitigate any potential risks, this section will provide some ideas on accomplishing such. There are a few things which you can do in order to



achieve the desired proof items such as proof of origination of income from an income source which is not linked to a crime, and a receipt to provide proof of ownership.

For those with a modest amount of crypto

Hopefully you have been keeping records well enough to construct a sound picture of your current holdings, even if purchased from a source which does not provide a receipt. Whilst the ATO will likely accept a spreadsheet with some basic details which recorded dates, times, and parties to a transaction for the purposes of assessing your tax obligations, the AML/CTF framework may potentially leave you exposed to the other parties' actions. You could begin spending your current crypto holdings via legitimate means, and repurchasing your portfolio via a legitimate source of income such as your salary on an Australian exchange which provides a receipt for the purchase.

Due to the specifics already covered in this document, if you wanted to legitimise your crypto holdings, all future cryptos would be purchased using a legitimate source of income from a reputable exchange. Purchasing your crypto holdings from such channels are fairly straightforward, so I will go into further detail on the spending side of the process below.

The <\$10,000 exception for personal goods and services

Currently in Australia, the law allows an Individual who holds crypto to use it to purchase online goods or services, or items for personal consumption under the value of \$10,000AUD. So, if you have a small stack, you may have time to transition it, by "living off" of your crypto, whilst sending your usual income to an exchange like and rebuying your portfolio. Remember, this is not necessary, unless you want to be 100% sure that you own your crypto and want to clean up any future liabilities.

Specifically, the act of spending your cryptocurrency does not generate a Capital Gains Tax A1 Disposal Event (if <\$10,000AUD) ... so it does not generate a tax obligation for you at the end of the financial year.

<https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/>

Where can I spend my crypto?

A quick google around can lead you to a number of various places you can spend your crypto. Although you may be holding various crypto, and exchanging from your specific holding (i.e. an ERC20Token) into the specific crypto which is accepted by the retailer (i.e. Bitcoin) will generate a CGT A1 Disposal Event which you should keep track of and are legally obligated to report.

Paying your Bills with your crypto

Additionally, an excellent Australian company called "Living Room of Satoshi" (<https://www.livingroomofsatoshi.com>) exists whereby you can pay any bill in Australia with various crypto's – anonymously (for now).

Whilst directly spending your crypto at a retailer such as a coffee shop, or buying things online such as via Newegg.com is a direct transfer of the actual crypto for the personal use good or service... It is not regulated (and no court or organisation has yet ruled upon) whether spending your crypto via Living Room of Satoshi is actually an exchange event from crypto to fiat (and hence a CGT A1 Disposal



Event is created) or if it is indeed you purchasing a service online. As Living Room of Satoshi do not take any fees (which would specify it as a service), the entire amount could reasonably be considered the service, and so I think that if a ruling were ever to be made upon the matter, Living Room of Satoshi would potentially satisfy the criteria. Although we cannot be sure what the future holds in terms of regulation, so ensure you document and keep records of any spending you do with Living Room of Satoshi just in case if you are paying your bills this way.

Buying precious metals with crypto

Also of note is the tendency of investors to purchase precious metals with their crypto holdings. It is a rising trend for individuals to purchase precious metals such as silver bullion with their crypto's as a means to try to fit within the definition of "spending" their crypto on a personal use "good" valued under \$10,000AUD. Even precious metals dealers advertise the circumstance with very little specifics around wording and also mentioning people to seek their own Tax and Financial advice before doing so. Precious metals dealers will often state that you do not generate a CGT A1 Disposal Event because you are "spending" your crypto, which if it also falls under the \$10,000 threshold, saves you from creating a CGTA1 disposal event. However, I doubt that this could be argued effectively.

In my travels I believe that future regulation may dictate, and purchasers of bullion may come to find, that they have generated a CGT A1 Disposal Event by purchasing precious metals such as gold or silver bullion with their crypto, even if it is under the \$10,000 threshold. This may not be the case if the individual had legitimate proof of their "personal use or consumption" of the silver. Whilst we are delving into semantics here, there is a reason I bring such details forward. Most people will not be buying silver bullion for the purposes of "personal use or consumption". Specific legislation and rulings have been made regarding the purchase of personal use assets such as precious metals with regard to legislation surrounding Self-Managed Super Fund investment. This legislation considers gold and silver items such as collectible coins and numismatics as personal use items, but explicitly states that silver and gold in bullion form is not a personal use item, but an asset for investment purposes. As with much in the crypto world, without a ruling being made on such a matter yet, the circumstance remains unregulated.

Do I have to legitimise my crypto holdings?

No, it certainly is not. In most cases when something lacks regulation, then there is no legal means for prosecution to come to you. However, the ATO and other government agencies have been known to enact retroactive legislation. Considering the disruptive potential of crypto technology, I do not expect a smooth ride for potential future crypto holders. It is completely optional and up to each individual to establish and understand their tolerance for risk associated with such matters.

Some people will have too much of a holding to "legitimise their crypto holdings" as described in this document. It is certainly not suggested to be mandatory to repurchase your crypto holdings as suggested in this document, but rather presented as an idea for those that are concerned about potential future liabilities and mitigating potential risks.

Thinking about getting creative?

In no way do I recommend breaking the law. How creative you may need to be to start solidifying your holdings if desired is dependent on many factors. Do you have an income from a legitimate full-time



job you can use to buy cryptos whilst you spend your current crypto stash? If not, there are still avenues available to you if you are creative.

Many of these avenues are having the doors closed on them as new regulation comes into effect, so understanding your situation and deciding whether you want to solidify your statement of ownership of your crypto to such a degree is time prescient. Tread carefully, as once something is on the blockchain, it is there forever. Additionally, do not believe everything you read on the internet. There is significant reason to believe that things such as TOR are completely compromised due to the information revealed in the Snowden leaks. Additionally, and conveniently approximately 1-2 years ago, Australia enacted laws enforcing ISP's to retain metadata of all Australians internet usage for a period of 2 years. Since its enactment, the AFP has stated and proven that the metadata is indeed being used to target individuals – although their ability to use the metadata as part of evidence in court proceedings is not yet been fully granted despite multiple attempts to pass legislation allowing such.

If you are thinking about doing something illegal in an effort to avoid your tax obligations, hide any gains or illegitimate income, it is wise not to.

Instead, you may be better seeking the help of a larger firm with significant expertise in such things, and allowing them to get creative for you. Large firms such as Ernst & Young, Price Waterhouse Coopers, et al. have experience in legally helping people in such situations to legitimise their holdings and do it in a legal manner. This could also be recommended to those people who have created "too much mess" of their crypto endeavours. Ernst & Young have a good presence with some crypto aware people in the industry, and Price Waterhouse Coopers have now started accepting Bitcoin as a means of payment – so these two big names may be worth considering, although presumably expensive.

In the end, this document only hopes to highlight that the time window for preparing for such matters in a more flexible way may be closing in.

I'm just going to hide it where they cannot find it

Sure, it is certainly possible to hide your wealth in crypto's. Extremely possible. The book of excuses is quite long and can be quite creative.

- I put it on a paper wallet and put it through the wash
- I got hacked, scammed, etc
- I had bad trading losses

It is not hard to hide your wealth in crypto, but then again, you can just as easily hide cash under your mattress. The REAL problem exists whereby in a future (say 5 years from now), you may not have any easy or viable means of spending this money without raising red flags for audits or investigations or blacklisting/whitelisting of Wallet Addresses. The depth of the technological capabilities and the lack of privacy we may be moving into is yet to be seen. The REAL question if you plan to hide your crypto stash is whether or not you are even going to be able to spend it in future...



Already now, in early 2018 we are starting to see utterances and whispers of the potential criminalisation of intentional concealment of funds, especially cryptos. Slowly but surely, such regulation is likely to come into place. Pre-empting such moves, this document exists to help newcomers and current crypto enthusiasts alike to prepare for such regulation.

If you have created liabilities, which are too large to untangle in your crypto endeavours already, you should seek expert help from a large firm to secure your current ownership. It may be expensive; however, it is likely advantageous to take care of your situation BEFORE such draconian legislation exists.



Other Possible Avenues Of Unwanted Liability Or Risk

Here is some additional info of other areas in your life whereby you may face risk or liabilities.

Divorce or relationship breakdown

It is very unfortunate in modern times, that divorce is such a common occurrence. It is of note however, that a CGT rollover can be done for a crypto asset in the event of a divorce related Property Settlement. Traditionally, it was the family home, a large value single piece of equity which cannot reasonably be shared by the two parties which would have to be sold in order to return fiat in agreed portions to both parties. This would create a very damaging CGT A1 Disposal event, of which unless ownership of the tax hit was specifically identified in the Property Settlement contract – would be potentially severely financially damaging for the transferring party.

In the event of a Property Settlement from a divorce, a rollover of crypto assets can be done easily because of the very divisible nature of crypto. This not only prevents a CGT A1 Disposal Event from being created, but preserves the Cost Basis used to calculate future tax obligations and transfers them accurately to the receiving party. If an amicable rollover of the crypto asset can be performed if both parties want to receive the asset in its current form of crypto and not a payout in fiat, then it can be done.

Child Support payments

When endeavouring in crypto endeavours, due to the volatile nature of crypto, in addition to potential parabolic moves in market price values... the simple act of staking your crypto for passive income, which although relatively predictable in crypto units of account, the relative value of the income in fiat terms may fluctuate wildly. Because of this, you may have the additional burden of regularly updating the Child Support Agency (or any other government departments) of your income as it adjusts on a daily or weekly basis. At the end of each financial year, you do not want to be penalised for underpaying over time, or create a liability to the other party by over-paying and readjusting their expected receival amount.

Bankruptcy

The actual underlying concept of bankruptcy is that when you become bankrupt, whether voluntarily or involuntarily, you forfeit your legal right as the trustee of your estate. To put this in simple terms, it basically means that you get appointed a public trustee who takes over your financial decisions. The public trustee has an interest to ensure that any financial advantages you gain over a set threshold is intercepted and used to pay back your creditors. How this can play out in the crypto world is summed up in simple terms as follows.

While a bankrupt, you are free to accumulate all you want in cryptocurrency or other assets. You are encouraged to continue working hard and progressing with life. However, you have a legal obligation to report to your trustee any change in your financial circumstances – this includes your income and your assets, including crypto holdings. As you are no longer in charge of your own estate – the trustee is free to intercept and sell any assets or income which you obtain that exceed the AFSA bankruptcy



threshold values. Of course, if you do not report your crypto assets or income from crypto activities to your trustee, you are breaking the law and attracting future liabilities under the Bankruptcy Act which you do not want.

A note on borrowing money to buy cryptos

In the crypto world, the craziness of it all can make people do very crazy things. Some people have re-mortgaged their home to throw the borrowed money into crypto. Many have taken loans or maxed out credit cards to invest or trade crypto. It is very risky and ill advised, especially if you cannot guarantee your ability to make repayments and service such loans should the crypto markets take an extended correction like 2014-2015.

Additionally, many exchanges offer additional margin capabilities for trading. Margin trading is a very risky endeavour and doing so can result in exacerbated losses from only very minor movements in the market. With the risk of margin trading and borrowing to invest or trade in crypto you are compounding your risk and could end up being forced into bankruptcy.

In Australia, if you are unable to fulfil the repayment of a debt which is of a value >\$5000, your creditor is capable of forcing you into bankruptcy through the court system. If they succeed – then you essentially lose control of your financial affairs of your estate and you will likely miss the very disruptive investment potential of the crypto boom over the coming years. Be mindful of your risks.

Centrelink

For the readers in the USA, Centrelink is Australia's form of social security benefits. Centrelink provides an array of benefits claimable by those that are unemployed or in need of social assistance or subsidies in relation to general overall living matters. Each benefit which you claim from Centrelink has an eligibility criterion. Whilst trading or investing in cryptos, you may potentially be moving out of the various eligibility criteria for the benefits which you are claiming from Centrelink.

As an example, for the “NewStart” unemployment benefits, the criterion which you must have less than the defined asset limits shown below.

Family situation	Homeowners	Non-homeowners
single	\$253,750	\$456,750
couple combined	\$380,500	\$583,500
one partner eligible, combined assets	\$380,500	\$583,500

Additionally, to claim unemployment benefits, your fortnightly income needs to be less than the figure shown in the table below.



Family situation	Payment reduces to nil once your income reaches this amount per fortnight
single with no children	\$1,041.67
single, 60 years of age or older and have been receiving payment for at least 9 months continuously	\$1,120.67
single, principal carer, with a dependent child	\$1,576.00
single principal carer of a dependent child, granted an exemption from mutual obligation requirements	\$2,004.25
single, 60 years of age or older, principal carer with a dependent child and have been getting payment for at least 9 months continuously	\$1,591.50
single, with a dependent child but not the principal carer	\$1,110.34
partnered	\$948.17

Each Centrelink benefit has varying criteria to be eligible. If you are investing in crypto, and claiming a benefit from Centrelink, you are required by law to inform Centrelink if your circumstances change, especially if they place you outside of the eligibility criteria.

More importantly, if you are trading crypto, or receiving passive income from any particular crypto endeavours - any realised gains are considered to be income. There are surely many people out there right now who are trading in crypto and not reporting their change in circumstances to Centrelink. Each person makes their own decisions, however it is worth noting a caution regarding intentionally not updating Centrelink of a change in your circumstances, as it could be seen as defrauding the Commonwealth, a serious offence under Australian Law.

Defrauding Centrelink is seen as stealing from the national government, so it is prosecuted by the Commonwealth rather than the State prosecutor, using the Criminal Code Act 1995, which applies to all States and Territories in Australia. You will most likely be charged under either section 135.2 (obtaining a financial advantage) or under section 134.2 (obtaining a financial advantage by deception). During the 2011-12 financial year, 57% of people prosecuted for Centrelink fraud were sentenced to immediate imprisonment.



If you have defrauded Centrelink, you may be charged under section 134.2 – obtaining a financial advantage by deception. If you are found guilty, the maximum penalty is 10 years imprisonment. You may instead, or also, receive a fine between \$10,000 and \$100,000 and be made to repay the benefit to Centrelink. You are also likely to receive a conviction, which will make it difficult for you to find future employment.

If you were unaware that your endeavours in the crypto landscape were bringing you specific income, you may want to seek solid legal help to report and rectify such things as an oversight before your affairs and legal liabilities get out of hand. Otherwise, as all things on the blockchain are recorded, you may find it may catch up to you in the future when timestamps of certain wallet addresses and your requirement to prove where/how/when you obtained the crypto come to light if you ever wanted to spend the crypto.

A mention of discretionary trust structures

It is very possible to hold your crypto assets in a trust. The most common form would be in the form of a “discretionary trust” which is also known as a “family trust”. First and foremost, trusts have traditionally been used to protect you from losing your assets from litigation in such circumstances of which you may be sued. Trusts do not protect you from relationship breakdown or divorce in Australia (or most other countries), despite rumours you may hear.

The second reason you would setup a trust would be to tax efficiently gift money to beneficiaries of the trust such as family members, etc. If you are hoping to be somewhat of a philanthropist in the future, you may want to investigate further the structuring and limitations of trusts. It is however, also of note that in Australia, the use of trusts is often targeted for auditing and legislative drafts are regularly proposed (although not yet passed) to disallow or make less beneficial, the use of trusts for funnelling income to family members or loved ones in the respective “before tax” amounts.

Buying crypto for family members, friends or other parties

This is an important, but often overlooked factor. If your friends or family ask you to purchase crypto on their behalf you should decline. If purchased from a legitimate exchange in your name, YOU are liable to pay any capital gains on said crypto. You are better off sharing a book like this, or training them on how to acquire for themselves. After many years, if the crypto holdings you are holding for them have risen in value, they may expect that ‘n’ number of ‘x’ crypto is worth \$xxxxx. They won't want to consider that you have to pay up to 45% tax on the gains, nor will they care how that may affect your taxable income, government benefits, child support payments, or any other factor of your life. Such things could lead to the dissolution of friendships and unwanted litigation.

Additionally, if gifting a particular crypto for a special occasion, you should also provide and keep a copy of a transcript of the event and the transaction hash of the transfer on the blockchain to prove date of said gifting and you will also be required to declare such an event as a CGT A1 Disposal Event on your own tax return for that financial year.



Investing In Crypto Via A Self-Managed Super Fund

Before jumping into the idea of moving your Superannuation into crypto, you should be aware of the a few things. Not only is managing your own SMSF cumbersome and time consuming, but the largest burden is learning the legal structure and responsibilities if you wanted to do such. The task of managing an SMSF is a burden which very few undertake. It is often those already knowledgeable with the superannuation system as well as having experience in finance and business which endeavour to manage their own superannuation.

There is an immense amount to learn, and it is not something that can be done without understanding the responsibilities associated with it. An intensely strict, and ever intensifying legal framework filled with responsibility needs to be adhered to immaculately. Learning it all, is an intense process which would take a determined person perhaps 3 months to fully comprehend and do correctly. Although you can mitigate much of the work along the way by paying (often very expensive) professionals for help in setup and constant administration.

Regardless of this fact, you must be capable of defending your investment decisions as responsible and justified, according to all general investment discourse and frameworks.

Diversification

If you are to invest your Superannuation into cryptocurrency in any sense of the matter, you should show that you have a portfolio which is diversified over multiple macro-economic industries. Because of this diversification criteria, you may also want to put only a small portion of your superannuation into cryptos. You may also want to hold precious metals in your SMSF to help justify your portfolio and prove a diversification and risk profile appropriate to your age and risk tolerance.

Justifying your portfolio allocation

By investing in an industry and market space which is largely unregulated, you can expect that you will have to immaculately justify your position. The penalties for not managing an SMSF appropriately are significant, and you as an Individual are accountable for.

You need to accompany your SMSF with ample memorandum notes, as well as custom essays regarding your justification for your decision-making process. You also need to be willing to lawyer up in a court of law should your actions be questioned following an audit, or if you fail to meet your obligations.

If you are young, you can use your age as a reason to accept slightly more risk when compared to older investors who may have less time to recover from potential losses. You should also create and prepare large and comprehensive Digital Security Processes and Standards which you will follow immaculately whilst managing crypto within your SMSF. You need to know what you are doing not just technically, but legally also.



In the not too distant future, registered superannuation companies, hedge funds and financial firms may begin providing packages of managed crypto investment options, saving you a lot of the burden.



Look Before You Leap!

Know what you are aiming to achieve from your investment in crypto

The risky and volatile price movements of the crypto markets can be very stressful. It is important to know what it is that you wish to achieve from entering the crypto market for investment or trading purposes. Most people entering into the crypto market will be looking for financial return – and everyone's particular situation is different. One main factor, which causes so much stress to those investing in crypto, is fear. Many are fearful that they are buying metaphorical tulips, and that the old adage of "if it looks too good to be true, it probably is" goes through many investors' minds. Once one realises that the technology cannot reasonably be destroyed, banned, taken out by an EMP, or any of the other fears constantly touted by those without a technical understanding of how it works – that is when strategic decisions can be developed. If you do not have confidence that crypto in some form will still exist in 3 years, then do not invest. Most importantly, only invest what you can afford to lose.

A note to Millennials about their Lambo...

Many young and inexperienced investors will flock to the nearest promise of the quickest returns. A small minute amount will end up making significant returns and literal "lifespans" worth of wealth in a very short period. However, for most, it will be a case of being burnt repeatedly until lessons are learned and responsible actions are taken. Be careful not to waste too much time learning these lessons – as time is one of the most important variables in wealth creation. The largest majority of people entering into the crypto market will be the ones making the mistakes and feeding the lucky few that get the "Lambo's".

On another note, the massive bull-trend in the crypto world, which is only just barely getting started, can present a solid investment opportunity if you take care and tread strategically. Many will chase the quickest and immediate gains, and in doing so may simply just be encumbering themselves with the types of liabilities discussed in previous sections of this document.

One small point I would make to those that want to guarantee their success in the crypto world would be that one should seek not to gain quick riches, but to build wealth.

A note on the importance of passive income

Especially if you are young, you tend not to think very long-term. The desire for immediate reward, overpowers the logic to be stoic. However, as you get older, start gaining responsibilities, mixed with the everyday grind of work, you tend to look for a long-term solution and finally think about building wealth.

Many people in the coming crypto advent will be made very rich, however not all of them will retain it in the form of wealth. The importance of aiming for wealth instead of riches needs to be stated. In a world whereby, everything is essentially operating from a system of "lending and borrowing", strategies come into play such as compounding interest and time.



Many people tend to ignore the fact that they will need to continue to work, day in, day out, for the rest of their life as if it were just a fact of life. In reality, there is a multitude of wealthy individuals living life without ever really “working” the same way most do. They, or their parents or grandparents accumulated an amount of wealth at some time in the past, and they have lent, rented and compounded their wealth to ever-increasing amounts. This is done by using their investments to make them passive income or equity gains – and then never spending more than they make in passive income. For example, someone with \$2,000,000 in investment or equity can usually find a way to earn a 5% or greater return on his or her investment each year. This 5% annual return equates to \$100,000 annually. They essentially then choose to live a quality of life that does not require expenditure beyond \$100,000 each year. Their continually growing capital reserve, mixed with the reinvestment of any unspent passive income creates a growing snowball effect, which eventuates to significant wealth over time and true financial freedom.

On the other hand, many that come into possession of riches quickly will immediately buy the items they desire such as an expensive house and car. They are then left with little to no capital reserve to reinvest to make passive income, and are forced to continue working each day of their life. Although the structures and operations of money in our society do not benefit the whole, but rather foster concepts of greed – such a topic and the solutions to such are outside the scope of this document.

It is important that if the concept of passive income and wealth building is new to you, then you should spend a lot of time reading books which will help you understand how to manage and grow your wealth appropriately.



Tax Efficiency Strategies For Investors

A mention on the benefits of white-knuckling (AKA: HODLing)

As you have read in this document, the tax repercussions, which will fall into your lap yearly if you generate large tax obligations by realising your capital gains often throughout the year, can significantly affect your efforts of investing. As most people actually lose money when trying to trade, the risk to reward ratio is (for most people), more favourable to simply white-knuckle your investments for a period of at least 12 months.

This is even truer if a realisation of a capital gain never eventuates, but the crypto you hold also has passive income potential in terms of a dividend, staking reward, etc. For example, if Joe had purchased 1000 Ethereum (ETH) for \$12 each for \$12,000 in January 2017, he would now have \$1,200,00 AUD worth of ETH in January 2018 . If he white-knuckled it he also would not have any additional tax obligations and would still have all 1000 of his ETH. He may then be able to use this ETH for spending, staking, lending, or even collateralising a fiat loan in the future.

It is of extreme importance that if you are planning on white knuckling, that you carefully select a crypto, which you believe will not die in the long term, but also has potential for passive income or other wealth building utility in some form.

The never-ending pack of Tim-Tams

Useful for when the passive income is in the same form as the original crypto.

The name comes from an old Australian advertisement whereby a woman holding a pack of Arnott's Tim-Tam biscuits has a genie granting her three wishes. She makes two very stupid wishes quickly without thinking, and for her last wish (equally as stupid), she commands the genie to provide her with a never-ending pack of chocolate Arnott's Tim-Tam biscuits.

As an example, we will use Joe with his 1000ETH, which he purchased for \$12 each in 2017. In 2018, upon the movement of the Ethereum network to the Proof of Stake consensus algorithm, he will essentially be able to "stake" his 1000ETH to earn passive income. Now it is very hard to tell how much passive income Joe may make by staking – but let us assume 5% per annum for simplicity. This means that Joe would get 50ETH per year in passive income for staking. He would have to pay income tax accordingly at the end of the financial year on the ETH, which he passively earns, but remember that the value of the "income" in ETH is based on the market value of ETH on the date (day) that the staking reward is received in his ETH Wallet Address. This means that if the bull-trend continues for ETH, and that if ETH were \$1500 per ETH in July/August 2018 for Tax Time, he may actually only have to offload a small percentage of his ETH to pay the ATO, not his marginal tax rate x 50ETH x \$1500, but only the AUD equivalent of his tax obligation which may end up being only 18ETH or so.

The strategies in the next chapters called "a different form of passive income" and "the salty taxman", become very useful for the purposes of squaring up your liability at the end of each financial year with the ATO for any outstanding tax amounts. Both "a different form of passive income" and "the salty



taxman" strategies help Joe to avoid having to offload this 18ETH to pay his tax - saving him the trouble of generating a CGT disposal event of enormous proportions, which would be, payable in his FY2019 Tax Assessment. Otherwise, if your portfolio is not diversified, and you only had the one never-ending pack of Tim-Tams, his investment gains on the ETH he has to offload would be calculated with a CGT Cost Basis of \$12 and a Disposal Price of \$1500 as the FIFO method is required to be used – that is a significant realised capital gain.

The true scope of this strategy is to achieve a never-ending supply of crypto funds, which you can spend directly on personal use assets, which are under \$10,000 value (or whatever the legislation in future allows). Specifically, because the ability to directly spend your crypto via a plastic card will show up in 2018, and also the main multiplier of benefit is that you can spend the returns perhaps to essentially pay for all your shopping for the rest of your life (if you select a crypto that lasts that long). The massive kicker of a benefit of this strategy is that as you spend your crypto, the concepts of the FIFO accounting method for working out your CGT Cost Basis apply. This means that over the course of time as you are earning passive income from staking, you are also spending the particular coins, which you initially purchased first - lowering the difference in price between your Cost Basis and eventual Disposal Price of the asset in the future.

It is important to select a long-life crypto, which is stake-able or provides passive income in the same specific crypto type that is being accumulated in order for this strategy to be effective. Additionally, ETH currently requires a minimum of 1000ETH to stake – a goal of which many may not be acquirable. There is a plethora of other cryptos already available and upcoming onto the market which provide this capability, and additionally, this same strategy works with almost any crypto if you are willing to provide your tokens for purposes such as margin lending on exchanges, other forms of lending, etc. However, the counterparty risk associated with trusting crypto in the hands of exchanges or staking pools for lending or pooled staking is potentially risky and caution and due diligence is recommended. Even solo staking has potential security concerns if you are not confident in configuring firewalls, networking, etc. However, some cryptos allow you to participate in staking without actually setting up a node so do plenty of research.

This particular investment strategy is not necessarily useful for buying large value items, but can be useful for such when coupled with "the salty taxman" strategy. It is also of note that for most instances "a different form of passive income is preferable".

A different form of passive income

Useful for when the passive income is in a different form as the original crypto.

Many cryptos out there offer the ability to stake or utilise them to generate passive income. In this strategy section, it is of note that the key difference to the way to utilise this strategy is that the coins useful here provide passive income in a different crypto denomination than the originating crypto denomination. Selecting for no specific reason, the example at time of writing with the highest market cap is the crypto known as NEO.

By staking NEO, investors are rewarded with a completely different crypto known as GAS. This differentiation in the actual denomination of the crypto is specifically important to note when the tax



considerations are taken into account. You can immediately transmute your GAS (or passive income in whatever form) upon receipt, into any other type of crypto you may plan to hold in the long-term, reinvest, spend on items >\$10,000, or cash out to fiat. This is a reasonable action, specifically because if done regularly, the difference between your Costs Basis and Disposal Price for CGT purposes will be minimal and your yearly tax obligations will not pile up.

For example, our mate Joe buys 1000 NEO and using a simple NEO to GAS calculator available online I can see that it generates approximately 10 GAS (\$300AUD) per month (at current rates). Joe keeps excellent track of his earnings using a software like cointracking.info that automatically provides accurate market rates and automatically imports his staking reward transactions daily for working out his Cost Basis price for use with the FIFO accounting method. If Joe transmutes (exchanges) his GAS into whatever else he wants (maybe more NEO, or any other crypto) he will be generating a CGT A1 Disposal Event. However, if he continually and regularly does this frequently, the difference between his Cost Basis and Disposal Price will never be too extravagant. For example, GAS may be \$28 at the start of the month and only \$30 at the end of the month, meaning he has only made a small capital gain of \$2 and have a very small CGT related realised gain. Additionally, if done regularly or timed for the desired effect, he could actually do his transmutations during "dips" in the market price of GAS to actually create claimable capital losses for his ABN "business". Joe has the option to accumulate funds in his "business" (ABN) for use of purchasing business related items as tax deductions, or he can immediately cash back out to AUD in his ABN Australian Bank Account, before spending the passive income, or sending it to his AUD Australian Bank Account which he holds as a "Individual" (Personal Account), to reinvest and buy more crypto for him as an Individual and build up his long-term holdings.

Additionally, if Joe has a diversified portfolio of crypto assets, enough of which provide him with enough return to generate a significant amount of income, it is possible that he may be able to simply accumulate said passive income for a period of a month or two around tax time each year to pre-empt any expected tax obligations. The benefit of this lies within the fact that he did not purchase the GAS years ago for 1% of their current market value and he will not realise any significant capital gains when he pays his taxes from this generated passive income. This helps him pay his tax obligations in case he is unable to perform the next strategy which is herein dubbed "the salty taxman".

There are also a lot of ERC20Tokens which return ETH, not the original ERC20Token. The same concepts can be applied to these tokens also. I expect that in 2018 even more tokens of this nature and capability will arise. As usual be extremely selective as not to accumulate a token which will die in the coming years or suffer from depreciation rather than appreciation in value over time.

The Salty Taxman

The lending industry which is forming in the crypto landscape could be expected to emerge in 2018. Whilst still in their infancy stages, concepts such as the SALT platform will probably emerge in growing number in the following years. Others such as "Coinlend" and "EthLend" also exist, but mentioning these platforms is NOT a recommendation to use them or advocacy that they are not scams. Do your own research and wait patiently for a reliable platform to come to fruition which provides the desired avenue of collateralised fiat loans backed by your crypto. It could even be speculated that traditional banks will offer loans whereby you are able to receive a loan in fiat (i.e. AUD) and give your crypto as a security/collateral for the loan.



The ideal benefits of this are as follows:

- You are able to continue to be the “owner” of your crypto provided you fulfil your obligations under the loan contract and service/make repayments on the loan.
- Large expenses such as a significant tax bill, house, car, etc can be settled in fiat without creating a CGT A1 Disposal Event.
- Other benefits outside the scope of this document for those which want to get creative.

Diversification

A great amount of information available online stresses the importance of diversification when investing. It is preferable to keep a multitude of various types of crypto in your portfolio in order to spread your risk and reduce the volatility within your portfolio. However, it is important not to overdo it to the point that you cannot keep track of the various market events and movements of so many cryptos. Ideally, a minimum of 5 different cryptos and up to 20 could be an example of adequate diversification.

The crypto world moves fast and over the next two years many project deliverables will be released, causing spikes or sudden appreciation of value to specific cryptos which will calm down once it finds its nominal market value through price discovery. These bursts will likely garner a lot of attention when they happen, however the importance of holding your portfolio within your logically decided allocation is important not to create unnecessary taxable events.

The traditional number one rule of investing is “Don’t lose money” – And one traditional strategy to enact that rule is to diversify. It is worth note however that concentrated allocation in choosing the right horse to bet on is often how wealth is grown, while diversification is used to protect that wealth in the long run. As the rush into this new economy happens over these coming years, almost any strong crypto project may rise in value. However, over time, specific cryptos which specialise in a particular macro-economic market will emerge to be the “leaders”, whilst underperforming cryptos will likely dwindle or fail. During these periods, it would be wise to identify which positions in your portfolio are simply speculative and which positions are strong. Over time you may have good reason to initially invest in a greater number of cryptos, but offloading and contracting your portfolio from more speculative positions into more solid positions over time as the market leaders emerge and your satisfaction level with accrued wealth increases.

Strategic buying and portfolio expansion

A great man once said that “rising tides raise all ships” – and over 2018 and 2019 such may be the case. Expanding your portfolio is important, in order to gain the diversification and it is likely that the significant amount of new cryptos being released for Initial Coin Offerings (ICO's) which may capture your attention. Try to identify buying opportunities for established crypto's during market pullbacks for crypto's that have strong fundamentals. If going into an ICO it is important to note that you are investing in a much riskier asset which may not even have a working product yet and take extra care not to over-allocate from emotion.

The worst time to buy a crypto and expand your portfolio is during the hype and buzz of a sudden surge. If you see a particular crypto raising heavily in value with a sudden burst – then you are already



too late. If you “buy at the top” you are quite likely to be paying too much and will find yourself waiting longer than necessary to see any potential further price appreciation of that particular crypto. You will like also suffer depreciation of that asset whilst it consolidates and price discovery sets in. That time which you will have to wait to see appreciation in nominal price value of such a coin is called “opportunity cost”.

opportunity cost

noun ECONOMICS

the loss of other alternatives when one alternative is chosen.

The best time to identify buying opportunity is to look for a strong crypto with solid fundamentals and have fiat available and ready for purchasing during the next market pullback/correction. It is important to identify and invest only in cryptos with strong fundamentals and which appear to have a long lifespan to ensure your tax efficiency strategies can help grow and preserve your wealth over time.

Strategic selling and portfolio contraction

Diversification and portfolio expansion can present a good opportunity to catch specific bursts in nominal price also. As the market dynamics change over time and the stronger market leaders emerge, as well as your wealth builds, you may want reallocate your portfolio or lower your risk by selling off more speculative positions into the stronger cryptos and “market leaders”. The tax implications of offloading a specific crypto is certainly something to take into account before offloading a particular crypto or changing your allocation due to a change in your confidence of each crypto.

If you feel that you must offload a particular crypto, first take into account your reasons for doing so and consider a few things.

- Has the crypto been leapfrogged by another crypto in the same macro-economic industry?
- Do you see the lifespan of the particular crypto coming to an end?
- Is your portfolio allocation too heavy in a particular crypto?
- Has the particular crypto had a significantly large spike in price appreciation recently? (influencing variable for a potential selling opportunity)
- Do you have other strategic investment goals to meet (i.e. accumulating a particular type of crypto you require a minimum of in order to generate passive income with)?



It is smart to see a sudden enormous spike in a crypto as a good time to offload a particular crypto if you must. This seems a bit contrarian, but in the long run, using the sudden "spikes" in price appreciation of less desired holdings as opportunities to offload and reallocate holds true over the long term as you will be minimising opportunity cost.

Confidence based buying

It is wise to establish and maintain a dynamic "confidence rating" in the cryptos you hold and are looking to acquire. Think of your confidence level as a "compass" which roughly guides you through the investing landscape as it changes in front of you. You can then allocate your fiat to those cryptos which you are most confident in effectively as you build your portfolio or reinvest passive income gains. Your confidence rating may also dwindle in a particular crypto over time, showing you where to best allocate your portfolio and identify opportunities to reallocate or shuffle your portfolio.

You can create a spreadsheet for example in Microsoft Excel, which connects to <https://coinmarketcap.com> via API to get current prices, and to track your confidence and notes in each crypto. You can also form some criterion to calculate your personal "confidence rating" of each of your holdings. Your confidence rating can be gathered through due diligence and research. Estimates could be made by comparing market capitalisation, circulating crypto supply, macro-economic outlook and potential market penetration of a particular industry.

It is important to note that even once a crypto has a significant "foothold" in a particular industry, they themselves are not immune to being "disrupted" or leapfrogged – this especially holds true when already established traditional economy entities (with large bankrolls) in the space begin adopting and rolling out their own crypto projects.

Due Diligence

Scams and frauds abound and it is important to do significant research and exercise strict personal due diligence standards especially when speculating on cryptos and projects which are not yet established. Here are some pointers to help with your due diligence. Such due diligence should definitively be done before investing in any Initial Coin Offering (ICO).

- Check and verify all details you can find about the prospective investment. Do significant research.
- Don't just believe photos and names of people or claims of endorsements.
- If technically capable, perform a WHOIS lookup on any domain names which are registered and be cautious if the WHOIS information is protected or not available.
- Create a fake LinkedIn profile which you can use to browse and verify team member claims – and even still do not trust the information in such LinkedIn profiles, but google the individuals further to look for oddities and potentially false claims.
- If the returns promised by a particular crypto or project look "too good to be true", then it could be. Stay away from anything promising daily returns which are unrealistic or look like Multi-Level Marketing schemes which often require you to refer other people to gain said "interest" or "earnings".



A significant amount of good information on how to conduct due diligence is available online and it is advisable to spend some time on the subject matter if investing in the riskier crypto offerings.

Continually betting on the same horse to win the race

Although many will be tempted to reinvest in the very token which is gaining them passive income in an aim to compound future returns, I would suggest alternative approaches in most circumstances. In the raging wild west of crypto-land, this may not be the best option. You could end up reinvesting your entire earnings from that passive income token only to find that one of the large business in the same macro-economic industry enters the space and eats a large portion of market share only to have that same token suffer capital depreciation and diminishing returns.

If earning passive income from a token, and you are not planning on spending that passive, but rather reinvesting it, then it is often a useful opportunity to either try to catch the next big rocket, to hedge by betting in similar (potential competitors) of the token you currently hold, or to stash away in the least risky options to increase the permanency of your newfound wealth and corresponding quality of life. If you are unsure and you want to reinvest into your most confident tokens which earn you the most passive income, you certainly can, but keep the above suggestion in mind. You would be wise to base where you put your reinvested income off your "confidence rating" just as you would any fiat which you invest to build your portfolio, but also keep it diversified over time.



Tax Efficiency Strategies For Traders

This short chapter will highlight a few pointers for those who actively trade. Without expanding into too much detail, here are a few pointers:

- For tax purposes you are better off trading on futures platforms instead of actually swapping around coins. This prevents capital gains tax events and separates "winnings" as separately declarable income.
- If carrying on a business as a trader, keep track of everything so you can claim any losses and additionally claim any further tax deductions such computer, office equipment, etc.

The benefits of keeping good records when making income from trading crypto

When making income from crypto endeavours, whether by trading or staking or another form of passive income, it is important to keep good records. The main reason for this is because the date of which you made the crypto (the day it hits your wallet address) acts as the date used to calculate the market value of your income in fiat terms.

For example, if you are trading on a futures platform, and made 0.01BTC realised profit for that day, your income for that day would be 0.01 x market value of BTC on that day. So, if the price of BTC at that date was \$4,000AUD on that day you essentially have made \$40 income that day. 6 months later, the price of BTC may be \$10,000... however, your tax liability for tax assessment purposes does not become \$100.

How trading crypto is taxed

It is important to keep track of your records immaculately. Both Australia and the USA have rulings from previous court occurrences which have shown in similar markets such as the share markets, where the Cost Basis of an asset cannot be ascertained, then the entire amount as at market value is taxable, and not just the capital gain. Likewise, with crypto profits whether received by staking or trading... If you cannot show the transaction or ledger history of the exchange of which you were trading. It is likely you may be taxed on the entire amount, as income, at the market rate of the day the ruling about your stash is made. This equates to saying goodbye to up to 45% of your portfolio value due to tax obligations. This is because there is no way for the ATO to prove that you did not just send various amounts to yourself at a later date (i.e. during massive dips, or a short time before disposing of an asset) to lower your purported income or Capital Gains Tax obligations. Have the proof, and have the records.

Proof is key to avoid over-taxation

It is important to keep immaculate track of all you do and keep records. If you are unable to prove your acquisition from start to finish of each of your cryptos, you could almost consider the tax man will end up taking almost half of it. Likewise, if you cannot prove that you acquired that crypto with



legitimate fiat which is not linked to a crime, then it is possible you may lose all of it if AML/CTF related allegations are unfortunately besotted upon you.

It is also of note that if trading, and you have also registered for an ABN, you can claim up to \$20,000AUD in losses as a tax deduction per year, which can be used to offset tax obligations for future years. Ironically there is a \$20,000AUD cap on losses, but not on gains.



Cautions

Trading

Trading is the art of buying low and selling high in order to increase your underlying portfolio value. It truly is an art, takes years, not weeks to understand and more reflective of gambling to the uninitiated.

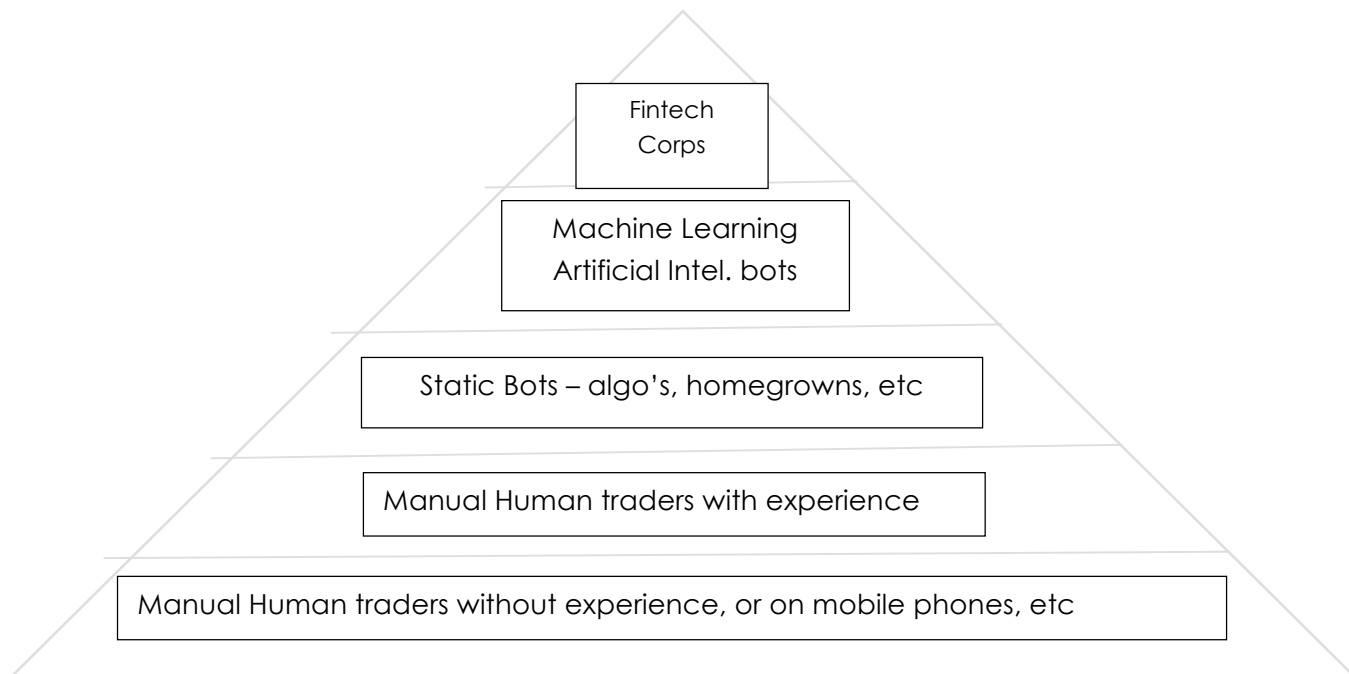
As established in this document, trading actual coins creates Capital Gains Tax A1 Disposal Events upon each trade. There are platforms dedicated to traders which are referred to as “futures” or “synthetics” platforms. If you are going to trade, this is probably the more tax efficient way for you to do so.

However, before rushing into trading, there is much for you to know. It is the heights of unregulated, “no-ceiling” risk. When considering how prescient time is in the equation in the rollout of this new technological upheaval (of DLT in general), it begs to wonder whether you should bother trading at all. Often the risk/reward ratio of trading, when mixed with the current tax framework makes it unrewarding and most suffer losses. Additionally, you need to take into account that your marginal tax bracket will affect your overall risk/reward ratio. As time has developed, the margins available for the average Joe to make a gain by trading have slimmed to the point whereby the ratio of winners/losers in trading has acutely contracted. The average Joe has but the slimmest chance, bordering on luck to actively day trade successfully. The rush periods of “noob” traders may allow some easy money for those that realise what is happening, but eventually they lose all their money and flush out of the exchange burnt, and move onto investing.

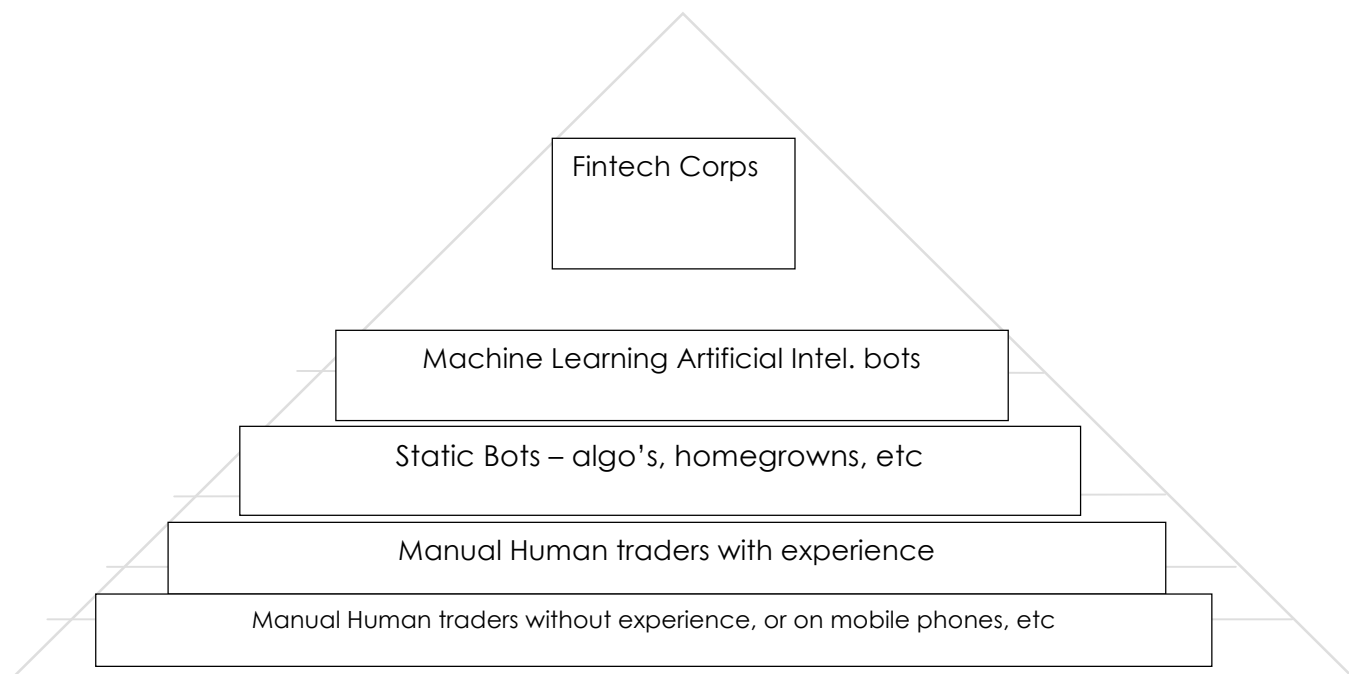
Essentially 95% of traders will lose money, where the top 5% will make it. The money has to come from somewhere, and the losers usually aren't the ones on YouTube making a peacock of themselves. On this note, whether trading or investing, have a humble respect for all others in your endeavours, as the “money had to come from somewhere”.

As trading in the crypto sphere has developed over the years, more and more actual traders are bots and not humans. I will break it down into a more easily understandable pyramid below. Imagine the pyramid as being only that share of the **top 5% which make money**. Underneath the pyramid below is an invisible trapezoid which is 19x larger which comprises all those who lost money trading.





This above pyramid is representative of the trading conditions in mid-2017. The pyramid area represents the amount or quantity of the specific type of trader, and their position (top to bottom) on the pyramid represents their percentage of associated profit share. In both pyramids, the Fintech Corps make the most as they have the best algorithmic bots, whereas the manual human traders will often as an overall percentage, receive the least reward. Over the coming years, to illustrate the direction of the markets another pyramid is presented below.



With the attention that the crypto world now has from big corporations opening up crypto trading futures platform, along with the expansion of experienced and highly funded software development teams filled with mathematicians - the profit of the average Joe trader will decline in time.

Many will tell you that you cannot beat the market. The truth is you cannot beat the market forever. You may however be able to time certain moves and actions to gain benefit from market movements. With the introduction of sophisticated bots which may only make modest returns, eventually the money generally all funnels to the trading bot owners in time anyway. Additionally, these bots require constant tuning and suffer from decay over time as the market becomes more saturated – eventually, he with the biggest software development team and budget wins the most.

Be warned and do not be lured into the world of trading unless you are willing to lose your shirt trying, only to learn some lessons. You, like most, will likely lose more than you gain – additionally, you will likely waste a lot of valuable investment capital appreciation time.

Mining and cloud mining investments

We all still occasionally see the average Joe jump on reddit and ask about how to mine Bitcoin or other cryptocurrencies. To those of you that wish to mine Proof-of Work blockchains, you are too late to the party. In Australia, where electricity costs are high, mining is not profitable anymore. No consumer GPU's will help you in most cases, and you will not outperform the gains you would otherwise experience in just spending the capital investment in the crypto's themselves, rather than the hardware to mine them. You will pay hundreds of times more fiat on your electricity bill and capital expenditure on hardware, than you could ever achieve if you were to simply just place strategic investments.

Additionally, you will likely find companies proposing investing in their mining operations. Whilst some might end up providing a return in the long run, it is more likely that greed as well as the challenges above for the mining industry will prove an unsatisfactory investment decision in the long run. Additionally, many platforms, including the most popular at the time of writing (Ethereum) are moving towards "Proof of Stake" consensus algorithms which solve the financial distribution requirement for security, without the requirement for investment into overbearing hardware. Rather than mining – "staking" would be a good thing to research into if you like the mindset of having "shovels during a gold rush".

Emotions can make or break you

A very well needed caution regarding FUD (Fear, Uncertainty and Doubt) and organised crime and deception. I will start off with this simple reddit post from Nov 2017 to give you an idea of the cunning and level of deception that flourishes in this wild west unregulated industry...



Warning Stay away from the BigPump Discord channel. It is a certified scam! (self.CryptoCurrency)

submitted 14 hours ago * by FudgieThaWhale  Trader

BigPump is marketed as a coordinated pump and dump Discord channel run by a guy called Vizard.

He organizes the channel to slowly alert everyone to a coin that will be pumped. Once he releases the name of the PnD coin he has already pre-pumped it to 40%-50% of a gain.

Once all of the channel members know the name of the coin they buy into it and he immediately dumps his holds on them at a massive gain.

I've seen this channel posted on this sub numerous times. If you do not want to feed your hard-earned crypto to a troll do yourself a favor and STAY AWAY AT ALL COSTS.

You can see the most recent evidence of this on the coin LUN. Do yourself a favor and stay away from these PnD groups. They not only hurt the crypto community but they will lose you money.

I hope this post saves someone from this scam. Please upvote this so that others in the community are aware and do not fall prey to this.

Whilst most of those accustomed to the FUD simply browse over invites to unrealistic ICO's... those coming new to the crypto landscape will not – early adopters – that is YOU. Additionally, you have traditional, well organised crime gangs which operate regular Multi-Level Marketing (MLM) schemes, alongside the pump'n'dumps and you also have those that setup a website to receive your funds and simply "do a runner". Sometimes, paid shills will post on reddit or newsgroups for weeks prior to the "pump" of a crypto (often of a coin you have never heard of – beware) ... only to build to a fake announcement which sends it parabolic whilst the organisers cash out. Do NOT get suckered. It takes some time to hone your skills to spot the fakes, and if you don't want to deal with it then simply ensure you have a diversified portfolio, do your due diligence and only place your money where you are confident.

It is also of note to not be too emotional about any news you read. Specifically of mention are crypto related news websites, of which all of them take in huge sums of money for paid news articles which are biased. Do ample research and take your time before acting or throwing your money at an ICO or any other crypto investment.



Security (Technical)

Before jumping into the crypto world, it is important to make sure that you are aware of the risks in order to avoid loss. A hacker can ruin you financially. The first and most important point about your crypto investment journey is the acquisition of a Hardware Cryptocurrency Wallet and not just settling for a Software Wallet on your PC.

Software Wallets

Software Wallets are simple applications which you install on your PC, Phone or Tablet. It is quite simple to install a software wallet on your home PC such as Exodus (<https://exodus.io>), or the proprietary wallet software from the blockchain developer or organisation directly. Some Software Wallet providers such as “Jaxx” and “Parity” have caused their users pain and loss of funds – and also have a regular stream of complaints in public internet forums, and so I would caution before using either of them.

Because this is software installed on your PC, Laptop, Phone or Tablet - this presents a problem whereby such devices can be hacked if not kept secure to a professional degree. Many users browse websites, do not keep their PC up to date, click suspicious links in emails, etc. There is an entire black-market of known “zero-day” exploits constantly being traded on the Dark Web. If you do not practice extreme care with your PC, phone, tablet or other device, it is safest to just presume it as compromised. Additionally, when using such software, your public and private keys are often stored in a “wallet.dat” file on the PC. This means that if your PC were to suffer a hardware failure, or you drop your phone in water, etc... your public/private key may be unrecoverable – rendering your only access to your crypto impossible. The backup procedure via something called a “seed phrase” is also prone to hackers and malware if created on a PC due to screen capture malware.

Ultimately, if you are like 90% of people out there that are not very confident in actively ensuring the security of your PC (and even if you are), then a Hardware Wallet is what you need.

Software Wallets such as Exodus Wallet (<https://exodus.io>) are quite useful for exchanging safely and also convenience for smaller amounts of value and temporary holdings. However, long term storage of your crypto portfolio on a software wallet or an exchange is not recommended.

Hardware Cryptocurrency Wallet

The Blockchain essentially exists in the cloud spread out in multitudes of synchronised copies across the globe. Users interact with the blockchain using their Public Key and Private Key.

Enter the Hardware Cryptocurrency Wallet. There are two current dominant players in the Hardware Cryptocurrency Wallet space. That is TREZOR (<https://trezor.io>) and Ledger Wallet (<https://www.ledgerwallet.com>). The devices simply plug into your PC / laptop via a USB port and provide the most secure form of cryptocurrency storage. In terms of practical security, both devices are equal. Trezor seems of a slightly better build quality; however, the Ledger Nano S supports a broader array of cryptos.





What the Hardware Cryptocurrency Wallet actually does is handle and store your Private Key within the device itself so that you never have to type your private key using the keyboard of your PC, or display it on screen. It also means that there is no "wallet.dat" file sitting on your PC waiting to be stolen and used to drain your funds. This ensures that even if your PC is infected with malware, your interactions with the blockchain(s) are all authenticated via the hardware device, and not exposed to a potentially compromised PC.

Your SEED Phrase

When you initially setup a Hardware Wallet, it utilises a Hierarchical Deterministic Wallet... which is a fancy way of saying that it provides you with a wallet for every type of crypto which it supports. It then also wraps up the private keys of all of those wallets into a 24-word seed phrase. This seed phrase is simply a list of 24 random English words in order. For example:

- 1) FLOWER
- 2) REBATE
- 3) SWIM
- 4) CAT
- 5) ~ through to 24 words total...

The order of these words is important and this 24-word phrase becomes your almighty "god password" for all of your crypto holdings. Needless to say, that these 24 words are the "real" wallet. If you ever drop your hardware wallet in water, crush it, lose it, etc... you can simply enter these 24 words when setting up another hardware wallet or software wallet on your PC to recover. You quickly begin to realise that the hardware wallet is more of a convenience device, with your "seed" as being the important part.

The 24 words from the seed are presented on the screen of your hardware wallet and not your PC, where screen capture malware can grab it – so as you write down the seed words, treat them as if they were the ultimate "god key" to your future crypto portfolio. Check the "Security (Physical)" section of this document for further instructions on how to protect this very important 24-word seed.

It is recommended to purchase your hardware wallet directly from the manufacturers' website and not from a reseller. If you are investing any more than \$1 in crypto, I would advise that a Hardware Wallet is the first thing you buy. You can consider that your Wallet(s) generated by your Trezor or Ledger Nano S is the only place that your cryptos are truly safe.



Only use a PC you are confident is secure

Only use a PC which you are confident that it is free from malware. If you have ever browsed casually or stepped on the net into unsafe websites, even if you think you do not have a virus, assume that you DO have a virus and format your PC before doing anything related to crypto on it. Start fresh and try your best to keep it fresh... your crypto portfolio will thank you for it. You could also purchase a spare, cheap PC or laptop for the sole purpose of crypto. Consider that your PC is always a point of vulnerability unless you are expert at securing your PC. Despite having a Hardware Wallet, you will still need to use your PC for various crypto exchanges as well as your day-to-day banking.

Do not hold funds or crypto on exchanges

I cannot describe how many times I have seen this asked as a question or stated as advice. If you do not hold the private key (i.e. Trezor, or Ledger Nano S) in your hand, then you do not own the crypto! Consider yourself engaging in significant counterparty risk by keeping anything on an exchange. Go to the exchange, buy your desired holdings and immediately transfer them to your Hardware Wallet. Never type your private key or seed phrase into any website without knowing exactly why and what you are doing (i.e. recovering a Wallet).

Use only hardware wallets for permanent storage

The security provided when you setup and use a Hardware Wallet ensures that your private key and seed are never exposed. Because of this reason, consider your hardware wallet (and you may own multiples) as your VAULT. When transferring coins from an exchange for the purpose of exchanging, or staging your coins in another wallet (perhaps Exodus), consider it a temporary holding place only. Additionally, if you have the option of using a hardware wallet to interface with an exchange – for example, the Ledger Nano S Plugin for EtherDelta, then use it. You may also want to purchase multiple hardware wallets – for example, a Trezor for permanent storage, and a Ledger Nano S for using EtherDelta and other interfaces/applications.

Some people online still do not trust the hardware wallet providers. Such super-strict individuals keep an offline Linux PC which never touches the internet and manually use a barcode scanner to “scan in” any inputs or interactions they do with the blockchain. Such individuals are absolute legends for being so careful with their cryptos. However, for the average person reading this book – a Hardware Wallet is going to be your best option. Additionally, for extra safety within your capability, purchasing both 1 Trezor and 1 Ledger Nano S for holding equal amounts of value of your overall stash effectively halves your risk to potential manufacturer specific security events.

Effectively hiding your income or donations which you get in the form of crypto

The purpose of this chapter is not about effectively hiding your income or donations from the government or tax office. If you were hoping for a book on how to launder money – this book is not for you. This section is for those people who own YouTube channels, or run a business that transacts in cryptocurrency. Such people might have a very real requirement to prevent random members of the public on the internet from knowing how much crypto they actually hold, and in which forms.



A note on privacy coins

It is the opinion of the author that privacy coins whilst effective for hiding transactions on the blockchain, do not comprehensively stop the data collection of individuals to the scope of which have been revealed since the Edward Snowden leaks and recent Wikileaks releases in terms of governmental and law enforcement capabilities. Edward Snowden even admits publicly on his twitter that the TOR network, which is used by individuals to access the dark net “anonymously” is just a “honeypot”. This is because of the overarching systems in place by government agencies at all of the endpoints via the XKeyScore, PRISM, ECHELON programs, etc.

Needless to say, the same deciphering capabilities and data retention capabilities to decipher captured network data packets from the ISP level, which would then contain the original blockchain input and output code - would effectively allow deciphering of attempts to use privacy coins to launder or hide money. Additionally, with the Australian law now forcing all ISP's to retain the metadata matching you the individual, to the IP Address for a period of two years and further technological developments around such increasing by the day with significant velocity – one would be naive to believe that privacy coins are a “sure thing”.

This is simply the opinion of the author, and many IT “experts” may not agree with such presumptuous conclusions. Either way – if you wanted a way to launder your funds from government agencies – you may well be wasting your time and incriminating yourself in the process. Whilst true that the government agencies may not end up having the Human Resources and funding to track and prosecute each individual – the question still remains – Why would you want that potential liability in the future? And when such a thing becomes so prevalent, the regulation around such, including its ability to be used in a court of law will only increase.

Not exposing your crypto holdings

There are currently many people running legitimate businesses or running a YouTube channel and providing their donation addresses publicly. The YouTube channel owners would provide regular updates and chats about crypto in a personable fashion, not knowing that organised crime gangs could be targeting them. Many of them simply transfer the donations and payments that they receive from their donation wallet, straight back to their VAULT (or the wallet they keep ALL of their cryptos in). This means that any person with a small amount of knowledge using a blockchain explorer website like <https://etherscan.io> can see that the specific YouTube Channel owner has 'x' number of crypto holdings. If you search, you can already link identities to people who own \$300,000+ worth of crypto. I fear these individuals may be leaving themselves open to being targeted either by technological or physical means by organised crime gangs or criminals in the future. It is advisable that if running a business or online presence which access cryptocurrencies as payment – you should employ this method or another valid method to keep your holdings as private as possible.

How to do it

For those legitimate users, which would like to know how to keep their customers, or YouTube subscribers from seeing their holdings, one such method would be as follows.



One way to stop a blockchain exploration in its tracks is to transmute your money from one blockchain to another. This means swapping Bitcoin for Litecoin (LTC) for example. This does not include swapping ETH for an ERC20Token, or vice-versa, because the ERC20token, exists on the same (ETH) blockchain.

Ideally, your business should have a wallet (yes, hardware wallet) for the purposes of collecting income which is separate from the wallet which you use for your “vault” or long-term holdings as an individual.

One way of hiding the funds you receive from your publicly presented and viewable crypto addresses is to traverse from one blockchain to another. This is done by exchanging your crypto for another type of crypto. This can be done by sending the funds to an exchange and exchanging into the desired crypto, then withdrawing that crypto out to a different wallet which is not your publicly presented/viewable wallet address (for example, your “vault”). On the blockchain explorer, the specific crypto will show as being sent to an exchange owned address, then stop. The tie will be broken from that point forward.

This method can also be simplified by using ShapeShift (<https://shapeshift.io>) or the Exodus (<https://exodus.io>) Software Wallet with the same underlying principles. You can use privacy coins to hide transactions, but your capability to prove what you did with the funds should the ATO audit you, whilst recordable manually, are hard to prove with perfection.

Additional security and privacy tips:

- If you do not know how to use and keep secure a Linux machine, then opt for Windows 7 over Windows 10 due to Microsoft inbuilt spyware on Windows 10.
- Use Brave browser instead of Google Chrome. Not only does this remove YouTube Advertisements, but has a myriad of other great features that help protect your privacy beyond that of Internet Explorer, Chrome or Firefox.
- Use a ProtonMail (<https://protonmail.com>) account for your email rather than big organisations like Google and Microsoft, who track and share all of your data and internet history (amongst other things). Hackers who may know you own crypto will target you, and if they gain access to your Google account they also have access to all your GPS data from your Android mobile phone as well... Take a second to comprehend that. (<https://www.androidcentral.com/how-view-your-location-history-google-maps>)



Security (Physical)

The most important thing in your crypto endeavours is actually security. Many people involved up to now have learnt the hard way by being either hacked, phished or robbed. It is critical for you to understand that the very knowledge by other people that you own cryptos is essentially a potential security risk in itself. Here are some useful concepts to adopt in order to ensure the Physical Security of you as a person relating to your involvement in the crypto landscape.

Discretion

Every person has a different personality type, and different ways to express themselves. Some people enjoy the attention from others, which they might get from bragging about large gains, well-timed trades, etc. There is also a large number of people, who do not express their ego, but have chosen to make themselves publicly visible and actively involved in crypto for the betterment of the community. Whether you are a significantly involved person on social media actively spreading the word and knowledge about crypto, or a small-time dweller in a small chat room, you are potentially opening yourself to being targeted if you are vocal about your holdings.

There are some general tips whilst conducting yourself online in any social media platform or chatroom which are important to follow. It may seem like common sense for online activities, however if you wanted to be absolutely sure of your security you should never announce how much crypto you have - even what you consider is a small amount now, others may view it as a fortune in the future. Also, do not provide any traceable information about yourself online such as address, real name, family members' real names or associations, etc. Be extremely wary of people trying to befriend you and acquire information about you.

Organised crime syndicates exist online and are certainly going to be (and already are) extremely prevalent in the crypto world. You may want to be mindful of worst-case scenarios before you publicly devolve any personally identifiable information about yourself online. If you have been scrupulous with your technical security, then the ultimate thing such criminals would be after to steal your funds would be your 24-word seed phrase.

Simple method for securely storing your all-important seed phrase

A simple method for storing your seed phrase is to spread out the words of your seed phrase between multiple parties who will all be able to come together in the event of your death or funeral and combine the words together to access your "crypto estate". You could give 2 close parties 12 words each, or 6 words each to 4 different parties. You may also want to provide an "overlap" for the involved parties. What is meant by this is that if you had 5 parties, you would give words 1-10 to person 1, words 6-15 to person 2, words 11-20 to person 3, words 16-24 to person 4, and words 21-24 + words 1-5 to person 5. This makes sure that if you are travelling with one of the other members during a fatal car accident - the remainder of the group have the whole of the 24 seed words.

It is important to note that doing such still holds counterparty risk if multiple parties collude. More importantly, it would be hard to argue that you took enough due diligence for securing your funds for your Self-Managed Super Fund if such counterparty risk existed surrounding the secure handling of your



seed. If you have, a Self-Managed Super Fund I would recommend a more thorough process such as is described in the next chapter.

The ultimate method for securely storing your all-important seed phrase

There are a large number of extremely creative ways to store your 24-word seed phrase. After all, your seed phrase is the most important, "all access" key to all funds stored on your cryptocurrency wallet. The method described below is one way to abstract your 24-word seed phrase into a simple, memorable password, whilst removing all counterparty risk with storing your seed phrase with other parties. This method also encompasses access by your loved ones should you pass away or meet unfortunate circumstances.

This is quite an extensive method, but it essentially removes almost every potential risk vector and contingency possible.

First step: decide on a memorable password

Decide on a password which you can remember easily, but is part of a larger text. For example, a Bible verse is easy enough to remember for most people such as "Exodus 2:13", "Peter 2:19", etc. Another example might be "Satoshi's Whitepaper, page 5", "Grandma's Carrot Cake Recipe".

Notes:

- Using a song is usually a bad idea as lyrics often lack grammatical accuracy.
- Bible verses, and any publicly available text should be quite secure for now, but are potentially targetable by Artificial Intelligence or other extensive cracking toolkits that may be developed in the future.
- A Book such as a family recipe book which each family member (or trusted person) all have a copy of which is the same year, or another document like "Grandad's Eulogy" or something similar is potentially the most cryptographically secure.

Once you have decided on your password, we will end up leveraging the larger text of that document in order to apply a simple cipher to your seed phrase. For this example, I am going to use the following Bible verse as the selected password for purposes of providing an example of the process...

Proverbs 13:22 - *A good man leaveth an inheritance to his children's children: and the wealth of the sinner is laid up for the just.*

With the example above, all that you have to remember is "Proverbs 13:22". Remembering "Proverbs 13:22" is a lot more realistic a task than remembering all 24 words of your seed phrase.

Remember – you can simply keep a 24-word seed phrase in plain text in your house, however, if you ever get broken into whether by coincidence or targeting – the thieves will have won.

Second Step: Encipher your SEED Phrase



This part is important as it saves you from counterparty risk should you keep the seed phrase printed out in a safe in your house and someone steals it. It also allows you to store copies of your seed phrase elsewhere, or with family members without the counterparty risk if their house was broken into and it were stolen.

Write down the full body of text of your password in capital letters. For the example, you would write out on a piece of paper by hand, in exact and precise spelling, the full text of Proverbs 13:22. You will probably have to continue writing many verses after Proverbs 13:22 (i.e. through to Proverbs 13:28+), in order to have enough letters available to encipher all 24 words of your seed.

With your sheet of paper in hand, starting from 1 and moving sequentially through the text, place a number under each letter of the body of text. For example, with "Proverbs 13:22" being your password, your sheet of paper would have the following body of text...

A GOOD MAN LEAVETH AN INHERITANCE TO HIS CHILDRENS CHILDREN AND THE WEALTH OF THE SINNER IS LAID UP FOR THE JUST... (Continued until at least 150-300 letters available)

Using this simple cipher method, you would place a small 1 under "A", a 2 under "G", a 3 under "O", a 4 under "O", a 5 under "D", a 6 under "M", and so on until you have about 150-300 letters.

Take the 24 words, which you have in your seed phrase and translate them accordingly from their letter equivalents into numbers. Whenever you use one of the letters on your sheet, **cross it off so that you never use the same number twice** for your entire seed. If you use the same number twice, the cipher loses entropy.

For example – If the first word in your seed phrase is "DOME", you would write... "1) 5, 3, 6, 10". It is important to **note the order** of each seed word also – as the seed words order is as important as the word itself. Upon going through and ciphering all 24 words, you should have something that looks like this...

SEED WORDS:

- 1) 5, 3, 6, 10
- 2) 18, 24, 68, 44, 32
- 3) 22, 11, 48, 57, 12
- 4) 150, 211, 34, 51, 77
- 5) 73, 91, 47, 41, 16

(and onward until all 24 words are done)

This is a somewhat time consuming and painful process. **You also need to keep a note in your WILL of instructions of how to decipher this.** As an individual, you may always remember your password, and decipher method, but you **MUST** keep a copy of instructions in your WILL for how to decipher it in case you have a car accident and suffer amnesia – or die.

Now you have a list of 24 "number combinations" which can only be deciphered if someone is aware of what your easily remembered "abstract body of text" password is. For the example above, we used



Proverbs 13:22 as the starting point for enciphering. By doing this we have enciphered our seed to avoid counterparty risk. You can now store your seed in a Safety Deposit Box with a copy of your Will, with a family member, at your house, etc.

Third Step: Backup your password

Essentially as our seed words are now abstracted and enciphered, the most important piece of the puzzle becomes your password (i.e. "Proverbs 13:22"). Without the password, no one can decipher your seed in the event of your death or amnesia – so this password now becomes the last single point of failure... So, ensuring that this password is never forgotten and always recoverable is the most important thing.

As suggested in the "Simple method for securing you all-important seed" paragraph – the same concept for spreading your password over multiple friends/family or other parties can ensure that this password does not get lost in the event of your death or amnesia. Likewise, it is a good idea to split the password up over multiple parties to protect from home robbery or other forms of being targeted. For this example, the password used was "Proverbs 13:22". Here are a few ideas of how you could split it up across multiple parties:

Person 1	Person 2	Person 3	Person 4	Person 5
PRO	VER	BS1	3!	22
(list of numbers linked to an array of letters only decipherable by a corresponding hint in person 2's document)	(list of numbers linked to an array of letters only decipherable by a corresponding hint in person 3's document)	(list of numbers linked to an array of letters only decipherable by a corresponding hint in person 4's document)	(list of numbers linked to an array of letters only decipherable by a corresponding hint in person 1's document)	
"Pea"	"Roe"	"Verbs"	"Thirteen Hours"	"Twenty Two Minutes"

As you can see above, there are many ways of which you can creatively separate and obscure the words so that counterparty risk is nullified. Take your time to really protect your password well, but do not go too far. Sometimes less is more... and the last thing you want is it being indistinguishable to your loved ones should you pass away.

This enciphering method removes the counterparty risk of events like:

- House robberies, common thefts, silent thefts (take picture and leave in place), etc.
- Having to trust your Safety Deposit Box Company to not snoop and/or provide the contents to other parties without your permission – including audits or investigations by anyone without said permission.
- Additionally, this solves the counterparty risk whereby each family member only has a riddle or partial part of your password, not the seed. This method allows exceptional security and provides defensible compliance for your SMSF and the SMSF's ("arm's length" compliance rules) if you have one.



Kidnappings, \$5 wrenches, and the only way to guarantee against them
With all other aspects of security and compliance addressed in this book, it is important to note the very unlikely, but possible event of a potential kidnapping, or \$5 wrench attack. The \$5 wrench meme comes from the fact that it is easier to rob you by buying a \$5 wrench and beating you with it until you divulge your password than it is to “hack” you or the blockchain directly. When it comes to preventing these things – the above methods for securing your seed with the ultimate method described in this book can come into play as an important step.

You can keep your “vault” wallet, seed enciphered and stored in a safety deposit box to which is not physically available to you and is only stored in the safety deposit box requiring an appointment and containing a duress password. You can also leave it with a family member or friend, of which you have a “duress word” which they are aware of.

There is also a feature of the Ledger Nano S whereby you have your main wallet, and also another “decoy” wallet if a different pin is supplied. This is likely to be known in the future especially by organised premeditated attackers and so should not be relied upon. Ultimately you need to be confident that the largest majority of your funds will be 100% unavailable to the kidnappers even if you divulge the entirety of the information. It is truly a matter of psychological and spiritual understanding which you need to come to terms about and decide whether you are willing to die to ensure that your children and loved ones are guaranteed to receive the benefit. Most thieves, especially if they do not bother to cover their face, are planning on, or willing to kill you anyway – so in such an instance you want to have a plan.

That said, ultimately in crypto - you “ARE” your wealth... your password (if using the ultimate seed strategy above) is only available by torturing you and so your duress passwords may help here. Although if you have a means of escape, it is likely your best option. Unlike previous times whereby it made sense to stand your ground and defend your house if your house contained a safe with all of your wealth in it. The stark and undesirable outcomes of such situations which arise by people wanting what you have are absolutely best avoided.

This means that such a situation is only really “preventable” by following the technical, privacy, and physical aspects of security mentioned in this book – specifically exercising **discretion**. Discretion on who you tell what to, both online and offline. Your practiced discretion is the only way to definitively limit your exposure to these types of liabilities.

Hopefully a technological solution to this problem is found soon and blockchains evolve to enforce in a secure manner, a Time Delay of a configurable number of days before a node will process said transaction on the blockchain, and/or requiring a second signature after said period of time for any significant value transfers. Some companies are inventing some really great technological ideas, and I am sure it is only a matter of time before such a solution could be implemented.



Other Tips

Here are some smaller tips which will hopefully save you making any major mistakes during your travels in the crypto world.

Don't send your Tokens to an exchange that does not support them

Just as you should not consider an exchange as "your wallet", you should also not expect the web interface of the exchange to support whichever particular ERC20 (or other) Token you send to a blockchain address as if it were your wallet. For example, if you wanted to Deposit Ethereum to an exchange, and the exchange supports Ethereum and provide an Ethereum Wallet Address, it does not mean that if you send the ERC20Token (ETH Blockchain compatible Tokens) to that address that you will have access to them. As a matter of fact, you are more likely to have lost the Tokens completely for your mistake.

This concept also applies when trying to participate in an ICO. The company providing the ICO and Token will warn heavily about using you "exchange based" Ethereum Wallet Address for the ICO and caution about withdrawing from the exchange address to the ICO contribution address in order to participate. You will never receive or have access to your funds. In the words of a well known crypto enthusiast "If you don't hold the private keys, it's NOT your crypto!". Participate directly from your hardware wallet for ICO's.

Encrypt your USB Drives

If you are used to carrying USB drives on you, you should create an encrypted container on them and store all your files in your encrypted container. It is recommended, depending on your desire for privacy to use Veracrypt (<https://veracrypt.codeplex.com/>). However, if you are a bit more paranoid, you can use version 7.0, or 7.1 of TrueCrypt. TrueCrypt, if you can find a clean copy of it on the net that is trustworthy, was the progenitor of Veracrypt, and TrueCrypt was shut down at version 7.2 by what is arguably presumed to be the United States, National Security Agency(NSA) – presumably because the NSA could not find a backdoor into it. It is not said here that you would want to use RIPMED 160 as the hashing algorithm and a triple layer algorithm such as Serpent-Blowfish-AES to encrypt your container, utilising a LONG password if such security were your concern.

Regardless, if you are going to carry anything on your person relating to your involvement in crypto which might help you keep track of your holdings or anything of the matter that links you to crypto – you want the best protection possible to secure your "discretion" and technological security as discussed in the "Security(Physical)" sections of this book.

Do not use cloud providers for storage

Even if you encrypt your data before storing it in the cloud on a provider such as Google Drive, Dropbox or Microsoft OneDrive – it is still potentially unsafe. Despite Snowden revealing that the NSA have Tera-hashes of Rainbow Table compute farms at their disposal to crack low-complexity AES256 encryption very quickly in 2012 (6 years ago), people still think it is acceptable to place their data in the hands of the very giant corporations which contract with such organisations. There are a few



outliers like SpiderOak (<https://spideroak.com>) who may present an option, but still trust is a concern. Be mindful where you store your data – as even Trezor use DropBox to secure some add-on apps to their product.

Bitcoin or Altcoins?

There is no right or wrong answer. Bitcoin is likely to remain and have strong staying power because of its current and significant market share and the encumbrance of invested parties and technologies. On the other hand, many “altcoins” have significant potential. Many altcoins will develop in 2018 which represent an almost uncanny resemblance to a security or share in a company. Some will be redeemable for a particular product, commodity, etc... and if the product is successful, you may do well in terms of investment returns. Other cryptos may present utility value for earning passive income via a web App of sorts. Where you invest your money is up to you, but remember, in the Dot-Com Boom, 97% of those companies don't exist anymore. At the same time, it gave rise to the Googles and Amazons of today.

You should invest on your own goals for passive income or capital appreciation, doing your own research and due diligence – refining your methods constantly – as the crypto world changes faster than ever. It is needless to say that it is likely that “today, the day you are reading this book, is the slowest day of technological development of Distributed Ledger Technologies of the rest of your life”.

Two Factor Authentication

Whenever or wherever you are offered an option for Two-Factor Authentication, use it. The U2F devices, the YubiKeys, the Google Authenticator Apps on your phone, the SMS 2FA, etc – It is all better than just having a simple password. Do not trust fully in the Google Authenticator App or SMS, but in general U2F and YubiKey are secure. Criminal Organisations have insiders inside the phone companies that regularly sell PIN/PUK codes on the dark web and also can redirect SMS's from your phone to theirs during a targeted attack. Anything that rests solely on SMS or Google Authenticator are not definitively secure.

Airdrops are not always your friend

Often, companies will reward their token holders by means of an “airdrop”. The concept is to reward the support of users (holders) of their token and progress their business. These airdrops are usually quite welcome, but you need to remember that you will have to declare the value of said airdropped tokens as “income” for that financial year. Sometimes this is a welcome bonus – but not always.

Sometimes organisations will drop unwanted cryptos into your wallet for the purposes of advertising, similar to spam email – just to get your attention. Unfortunately, you have to record in cointracking.info, and declare these small amounts as income at their value during the time you received them (facepalm).

Additionally, you never really know what the code behind one of these tokens actually does, and so you should not interact with it if you don't know what it is. Several, perhaps unforeseen attack vectors may exist whereby random code is placed into smart contracts. Be wary. Be vigilant and do not trust anything – verify instead. Be cautious forever in the future, and especially 2018. You can verify a Tokens legitimacy through personal research or by going to <https://etherscan.io> and browsing their “verified contracts” section.



Cryptocurrency Dictionary

From WikiCryptoCoins.com

Cryptocurrency related acronyms, terms, vocabulary and slang are often used in crypto conversations. Knowing the terminology will really help you to follow cryptocurrency news and discussions in social media. Disclaimer: Some of these terms are used in fun and humor.

2FA (TFA) = A "2-Factor Authentication" is a simple method of enhancing your security, representing an independent channel of authentication.

51% Attack = A situation where more than half of the computing power on a network is operated by a single individual or concentrated group, which gives them complete and total control over a network.

ADA = A symbol for Cardano currency.

Address = In cryptocurrency terms, an address is a code used to send, receive or store cryptocurrency. These addresses consist of 26-35 characters, a combination of letters and numbers. The address can also refer to the public key, a pair of keys needed to sign their digital transactions.

Addy = This refers to a cryptocurrency public address (or key). For example: "Send me your addy, please."

Agreement ledger = An agreement ledger is distributed ledger used by two or more parties to negotiate and reach agreement.

Altcoin = "Alternative coin" is every other cryptocurrency than Bitcoin (BTC). Bitcoin is considered the main index for cryptocurrency market.

ANN = Announcement. Likely to view this near an announcement of a new cryptocurrency project that is about to launch or on forums like Bitcointalk.

API = An "Application Programming Interface" is a set of subroutine definitions, protocols, and tools for building application software.

Arbitrage = The act of buying and selling on different exchanges to earn the difference in the spread. Arbitrage opportunities occur due to differences in exchange reputation, community coin preferences and ease of bank funding. Take note that fees, limits and prices could change anytime when you are transferring your coins between exchanges, especially during volatile times.

Ashdraked = A situation where you lost all your money.

ASIC = "Application Specific Integrated Circuit". ASICs are silicon chips specifically designed to do a single task. In the case of bitcoin, they are designed to process SHA-256 hashing problems to mine new bitcoins.

ASIC miners = The hardware which houses the ASIC silicon chip. Connected to the internet.

ATH = "All time high". This means that the price of a certain cryptocurrency has broken all of its past records and is trading at the highest price it has ever achieved.

Attestation ledger = A distributed ledger providing a durable record of agreements, commitments or statements, providing evidence (attestation) that these agreements, commitments or statements were made.

AUD = Australian dollar.

Bagholder = A bagholder or bagholder is an investor or a trader who has been holding (or hodling) for too long on a certain cryptocurrency and now has to face the consequences of that decision.

Bags = Holdings of altcoins, with each altcoin being held in a different "bag".

BC = "Bitcoin Classic", is one of alternative bitcoin development branches. This solution has little support from the overall bitcoin community right now, though.

BCH = A symbol for Bitcoin Cash.

Bear = This is a term borrowed from the Wall Street people. This means a trader or investor who believes the prices of a particular cryptocurrency or market will fall and wants to profit from that fall.



Bearwhale = This term means a trader with a fat account who is bearish on the price of a cryptocurrency.

Big Blockers = Those who believe in a scaling path for Bitcoin that increases the block size above 1MB. Notably, Bitcoin Unlimited and other factions/supporters.

BIP = "Bitcoin Improvement Proposal" is a standard to submit potential changes or improvements that will have a positive effect on the bitcoin protocol as a whole.

Bit = A unit used to designate a sub-unit of a bitcoin - 1,000,000 bits equals 1 bitcoin (BTC).

Bitcoin (uppercase) = The well known cryptocurrency, based on the proof-of-work blockchain.

bitcoin (lowercase) = Bitcoin is the first decentralized, open source cryptocurrency that runs on a global peer to peer network, without the need for middlemen and a centralized issuer.

Bitcoin maximalist = The truest believer in bitcoin's original mission and design, often paired with a disdain for altcoins.

Bitpay = Bitcoin processing company who allow merchants to accept bitcoin as a payment method.

Block = Blocks are packages of data that carry permanently recorded data on the blockchain network.

Blockchain = Originally block chain, is a continuously growing list of records, called blocks, which are linked and secured using cryptography.

Blockfolio = Keeps track of your crypto holdings.

Block height = Block height refers to the number of blocks connected together in the block chain. For example, Height 0, would be the very first block, which is also called the Genesis Block.

Block reward = A form of incentive for the miner who successfully calculated the hash in a block during mining. Verification of transactions on the blockchain generates new coins in the process, and the miner is rewarded a portion of those.

Bloodbath = When a certain cryptocurrency or most cryptocurrencies are nosediving (values in red).

Borrowing rate = When you open a leveraged position, you will be borrowing coins at a pre-determined rate. This rate will be added to reflect your position's overall profit and loss.

Breakout = When market price moves passed a predefined support or resistance level.

BTC = A symbol for Bitcoin.

BTFD = "Buy The Fucking Dip". When people are running around and selling because of fear, this is the time to buy.

BU = Bitcoin Classic (BC) is one of the alternative branches of bitcoin development. BU, or "Bitcoin Unlimited", is another alternative bitcoin solution. So far, it appears only a small portion of the bitcoin community supports this proposal, though.

Bubble = In the 2010s, various scholars and journalists have claimed that some cryptocurrencies have been involved in, or are displaying the signs of, an economic bubble phenomenon.

Bull / bullish = A market in which coin prices are rising, encouraging buying.

Butthurt = A description of where you will feel the pain when your shitcoin goes to zero.

Buy / sell wall = A wall as seen in the depth chart of exchanges is an amalgamation of limit orders of the same price target.

Buying pressure = Occurs when the majority of traders are buying, indicating that the majority think the market price will increase.

C&H = "Cup and Handle" refers to a trading pattern on the charts that looks like a cup with U shape with a handle visible on the graph as a slight drift.

CAD = Canadian dollar.

Charlie Shrem = Flamboyant and early bitcoin entrepreneur.

Charlie Lee = A person who created Litecoin. He is a former Google employee.

Choyna = A deliberately distorted way of referring to China. As China is a country which is immensely influential in the Bitcoin space, it has largely dominated mining and trading activities.

Central Ledger = A central ledger refers to a ledger maintained by a central agency.

CFTC = The U.S. "Commodity Futures Trading Commission" is an independent agency of the US government created in 1974, that regulates futures and option markets.



CHF = Swiss franc.

Circulating supply = The price of a coin has no meaning on its own. However, the price of a coin, when multiplied by the circulating supply, gives the coin's market cap.

CNY = Chinese yuan renminbi.

Coinbase = One of the world's most popular cryptocurrency web wallet.

Cold storage = A secure way of keeping cryptocurrencies off exchange.

Commodity Money = A currency whose value comes from the commodity from which it is made.

Confirmation = The successful act of hashing a transaction and adding it to the blockchain.

Consensus = Consensus is achieved when all participants of the network agree on the validity of the transactions, ensuring that the ledgers are exact copies of each other.

Core = The group of individuals that are most active developing a cryptocurrency.

Correction = A reverse movement, usually negative, of at least 10% to adjust for an overvaluation.

Corrections are generally temporary price declines interrupting an uptrend in the market or an asset.

CPU = A "Central Processing Unit" is the electronic circuitry within a computer that carries out the instructions of a computer program by performing the basic arithmetic, logical, control and input/output (I/O) operations specified by the instructions.

Crypto anarchist = Someone who totally hates the government.

Cryptocurrency = Also known as tokens or coins, cryptocurrencies are representations of digital assets.

Cryptographic hash function = Cryptographic hashes produce a fixed-size and unique hash value from variable-size transaction input. The SHA-256 computational algorithm is an example of a cryptographic hash.

Cryptography = The study and practice of secret communication.

CYA / CYOA = "Cover your Ass" / "Cover Your Own Ass".

Dapp = A decentralized application (Dapp) is an application that is open source, operates autonomously, has its data stored on a blockchain, incentivised in the form of cryptographic tokens and operates on a protocol that shows proof of value.

DAO = "Decentralized Autonomous Organizations" can be thought of as corporations that run without any human intervention and surrender all forms of control to an incorruptible set of business rules.

DAO attack = DAO was breached in 2016 in a case that resulted in \$50-\$60 million worth of Ether being stolen.

Dash = An open source peer-2-peer cryptocurrency started in 2014.

Day Trade = The term for trading AltCoins on trading platforms on a consistent basis to try to gain higher wallet %.

DCA = "Dollar Cost Averaging". Used to reduce the volatility of market portfolios by spreading out buys and sells over a more extended period.

DDoS = "Distributed Denial of Service". A well-timed DDoS attack at exchanges during volatile movements may be devastating as traders will not be able to execute any order manually and will be at the mercy of their pre-set, or the lack of, limit orders.

Difficulty = Difficulty, in Proof-of-Work mining, is how hard it is to verify blocks in a blockchain network. In the Bitcoin network, the difficulty of mining adjusts verifying blocks every 2016 blocks. This is to keep bitcoin block verification time at ten minutes.

Dildo = Long green or red candles.

Distributed network = A type of network where processing power and data are spread over the nodes rather than having a centralized data centre.

Distributed ledger = An agreement of shared, replicable and synchronized data, in this case spread across multiple networks, across many CPU's.

Dolphin = Someone who has graduated from the ranks of minnows and has some influence over the price movement of a cryptocurrency, but hasn't yet reached the status of whale.

Double spending = This occurs if someone tries to make purchases with their digital coins at two different places.



Dump = To sell off a coin.

Dumping = Downward price movement.

DYOR = "Do Your Own Research". The trader's caveat that advice shouldn't be taken at face value.

EEA = The "Enterprise Ethereum Alliance" connects Fortune 500 enterprises, startups, academics, and technology vendors with Ethereum subject matter experts.

EIP = "Ethereum Improvement Proposal" is a standard to submit potential changes or improvements that will have a positive effect on the Ethereum protocol as a whole.

ETH = A symbol for Ether, token of the Ethereum blockchain.

Ethereum = A blockchain-based decentralized platform for apps that run smart contracts, and is aimed at solving issues associated with censorship, fraud and third party interference.

EUR = Euro.

Evan Duffield = The creator of Dash cryptocurrency.

Exchange = Where you buy or sell bitcoin and altcoins to or from your bank or credit card or from various coins on the open market. There are internal wallets yet the exchanges have the private keys to the wallets so it's never safe to store the cryptocurrency on these exchanges for a long period of time.

FA = "Fundamental Analysis" is a method of evaluating a security in an attempt to measure its intrinsic value, by examining related economic, financial and other qualitative and quantitative factors.

FATCA = The "Foreign Account Tax Compliance Act" is a 2010 United States federal law requiring all non-U.S. ('foreign') financial institutions (FFIs) to search their records for customers with indicia of 'U.S.-person' status.

Faucet = A reward system on a website that dispenses bitcoin in the form of a Satoshi (a hundred millionth of a bitcoin)

Fiat currency = A currency without intrinsic value established as money, often by government regulation (\$ USD, € EUR, £ GBP, ¥ JPY etc.).

Fill or kill = A limit order that will not execute unless an opposite order exceeds this limit order's amount.

Flipping = The term for constantly rotating your altcoins on a trading platform trying to catch the raising percentages as the coins constantly go up in value.

Flipping = The name given for the event where a cryptocurrency who surpasses bitcoin in market capitalisation (yet to happen at time of writing).

FOMO = "Fear of Missing Out". FOMO means the fear of missing out on the profit which might result from an investment or a decision.

Forging = The name giving to the process in proof of stake blockchains where there is no block reward. Forgers keep transaction fees instead.

Fork = Forks create an alternate version of the blockchain, leaving two blockchains to run simultaneously on different parts of the network.

FUD = "Fear, Uncertainty, and Doubt". This term usually refers to investors who are unsure of the potential of a situation.

GBP = British pound.

Genesis Block = The very first block in a block chain.

Gox crisis = A critical point in Bitcoin history when more than \$480 million of it disappeared due to mismanagement of the cryptocurrency. The name is derived from the Tokyo-based Mt. Gox Bitcoin exchange.

GPU = A "Graphics Processing Unit" is a specialized electronic circuit designed to rapidly manipulate and alter memory to accelerate the creation of images in a frame buffer intended for output to a display device.

H&S = "Head and shoulders" refers to a trading pattern viewed on the charts that predicts the price of cryptocurrency is expected to increase and opposite when it is expected to decrease.

Halving = Bitcoins have a finite supply, which makes them a scarce digital commodity. The total amount of bitcoins that will ever be issued is 21 million. The number of bitcoins generated per block is



decreased 50% every four years. This is called "halving". The final halving will take place in the year 2140.

Hard fork = A type of fork that renders previously invalid transactions valid, and vice versa. This type of fork requires all nodes and users to upgrade to the latest version of the protocol software.

Hard wallet = A device which allows cold storage of coins, for increased security.

Hash = The act of performing a hash function on the output data. This is used for confirming coin transactions.

Hashrate = Measurement of performance for the mining rig is expressed in hashes per second. Mh/S (mega hash per second) is the speed that a graphics processor, GPU, can hash per second.

HF = "Hard fork".

Hodl = "Hodl" is originally a typo of the word "hold" which appeared on the Bitcoin talk forum in 2013. It came from a member named GameKyuubi under the thread "I AM HODLING". The writer seemed to be drunk. Hodl is one of the most used funny term in cryptocurrency world.

ICO = "Initial Coin Offering", which takes a page from the usual IPOs investors know. Coins bought during ICOs are usually sold for a profit when the coin first hits exchanges. This is due to the initial hype which increases demand for the coin. On the supply side, ICOs create entry barriers as the buyer has to set up his private wallet to receive the coins from the ICO purchase.

IMO = "In My Opinion".

Inflationary / deflationary = If you are familiar with finance, don't be fooled by these common words used with cryptocurrencies. They have nothing to do with credit cycles and instead mean that some people think a large number of coins are good and others think the opposite.

INR = Indian rupee.

ISO = "Initial Scam Offering", simply a play on words for Initial Coin Offering, referring to the fact that majority (if not all) of them are scams.

JOMO = "Joy Of Missing Out".

JPY = Japanese yen.

KYC = "Know Your Customer" refers a situation where you have checked the identity of an individual and have taken precautions so that the money you are receiving is clean and not associated with laundering.

Lambo = Shortened form of Lamborghini (an Italian sports car) and the preferred transportation method of cryptocurrency enthusiasts once they've made their fortune. Lambo refers to insane returns, enough to buy a \$1 million Lamborghini.

Ledger = An append-only record store, where records are immutable and may hold more general information than financial records.

Lending rate = Some exchanges have lending accounts. You may deposit your coins into these lending accounts to lend your coins for others to execute their leveraged trades. The lending rate fluctuates throughout the day based on the demand for shorting the coin.

Lightning network = Builds on networks like bitcoin and litecoin to allow off-chain settlements.

Limit order = An order placed at a future price that will execute when the price target is hit.

Litecoin = A peer-to-peer cryptocurrency based on the Scrypt proof-of-work network. Sometimes referred to as the silver to bitcoin's gold.

LN = One of the future bitcoin scaling solutions goes by the name of LN, also known as the "Lightning Network". This particular proposal allows for bitcoin microtransactions to be bundled into one single transaction, reducing delays and excessive fees.

Long term hold = A position that a trader takes. To take a long position on something is to believe its value will rise in the future.

LTC = A symbol for Litecoin.

Margin trading = A term for 'trading with leverage'. In this instance of trading, you borrow one side of the trading pair at an agreed loan rate and sell it for the other side of the trading pair. Depending on the direction you believe the market to move, you may place a long or a short bet on the trading pair of concern.



Market cap (Market capitalization) = A stock's market cap refers to the market value of the company's outstanding shares. In the cryptocurrency market, the market cap is used to illustrate a coin's dominance in the entire cryptocurrency market.

MCAP = Market Capitalization.

Medium Term Hold = The Term for holding onto altcoins for a medium amount of time, generally hours to days, before trading them for a different coin.

Mining = The process by which transactions are verified and added to a blockchain. This process of solving cryptographic problems using computing hardware also triggers the release of cryptocurrencies.

Miners = Servers/computers which are used to solve the cryptographic problems attached to blockchain transactions. Miners receive a reward in the form of cryptocurrency for providing transactions on the blockchain.

Minnow = Someone who has a small amount of cryptocurrency and is thus considered a "small fish".

MIOTA = A symbol for IOTA currency.

Moon / mooning = Extreme bullish movement of a coin. "To the moon".

Mountain peak / mountain top = A term for a candlestick on the trading platform being at it's highest peak before a dip.

Multisignature (Multisig) = Multi-signature addresses provide an added layer of security by requiring more than one key to authorize a transaction. Multisignature addresses have a much greater resistance to theft.

MW = One of the potential solutions to make bitcoin scale goes by the name Mimblewimble, sometimes abbreviated to MW.

Nick Szabo = A creator of bitgold, an unimplemented forerunner of bitcoin. Thought by some to be Satoshi Nakamoto, which he always denies.

Node = A copy of the ledger operated by a participant of the blockchain network.

Noob = A person who is inexperienced in cryptocurrencies.

OCD = "Obsessive Cryptocurrency Disorder". Suffered by those who can't stop monitoring the value of their coins.

Off-Ledger currency = A currency minted off-ledger and used on-ledger. An example of this would be using distributed ledgers to manage a national currency.

On-Ledger currency = A currency minted on-ledger and used on-ledger. An example of this would be the cryptocurrency, Bitcoin.

Oracles = Oracles work as a bridge between the real world and the blockchain by providing data to the smart contracts.

OTC = "Over The Counter".

P2P / Peer to Peer = Peer to Peer (P2P) refers to the decentralized interactions between two parties or more in a highly-interconnected network. Participants of a P2P network deal directly with each other through a single mediation point.

Paper wallet = A form of cold storage. These are public and private keys held on a piece of paper. A good designer can make them look like branded bank notes.

Payment processors = Merchants who accept bitcoins, use specific processors to handle the transactions. This can include online merchants, brick and mortar businesses, or individuals.

Peer to peer exchange = A person who owns bitcoin or other cryptocurrencies willing to sell it to you or you buy/sell to them.

Poloniex = A popular cryptocurrency exchange.

Ponzi scheme = A fraudulent investment operation where the operator generates returns for older investors through revenue paid by new investors, rather than from legitimate business activities or profit of financial trading.

Pol = "Proof-of-Importance" algorithm. Pol is different from other initiatives which use a fee-sharing model that does not take into consideration one's overall support of the network.

PoS = "Proof-of-Stake" is a type of algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus.



PoW = "Proof-of-Work" system (or protocol, or function) is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer.

Private key = A private key is a string of data that allows you to access the tokens (cryptocurrency) in a specific wallet. They act as passwords that are kept hidden from anyone but the owner of the address.

Private key cryptography = This key is encrypted so that it is confidential to only its owner.

Public Address = A public address is the cryptographic hash of a public key. They act as email addresses that can be published anywhere, unlike private keys.

Pump = Upward price movement.

Pump and dump (P&D) (PnD) = The recurring cycle of an altcoin getting a spike in price followed by a huge crash. Such movements are often attributed to low volume, hence the 'pump'. Traders who pump, buying huge volumes, may wish to invoke FOMO from the uninformed investors and then dump, or sell, their coins at a higher price.

Pyramid = Where an organization is setup on a referral to referral basis constantly accepting investments with locked contracts in order to hold onto investors money. The more people underneath each other investing in the system, is the only fuel for maintaining these infrastructures until they can no longer withstand the demand for payouts. At this time, they will generally disappear or crumble.

RBF = "Replace-By-Fee" was introduced to allow users to rebroadcast a previous transaction but with a higher fee. This also nullifies the original transaction, as it is effectively "overwritten" by the new one.

Rekt = This is a misspelling of the word "wrecked". This term refers to a trader or investor who is utterly ruined and destroyed with losses from the current downfall of a price. Term "rekt" also traces back to multiplayer video games.

Resistance level = A price point in which upward price movement is resisted due to market conditions.

Reverse indicator = Someone who is always wrong predicting price movements.

Ring signature = A type of digital signature that can be performed by any member of a group of users that each have keys.

RingCT = "Ring Confidential Transactions" help to create stealth addresses that mask receiving address. RingCT hides transaction amounts as well.

Ripple = A payment network built on distributed ledgers that can be used to transfer any currency. The network consists of payment nodes and gateways operated by authorities. Payments are made using a series of IOUs, and the network is based on trust relationships. The banking industry is adapting this platform.

ROI = "Return on Investment". How much you've made (or lost) on your cryptocurrency since buying.

RSI = "Relative Strength Index".

Ryan Fugger = A person who conceived Ripple in 2004 after working on a local exchange trading system in Vancouver.

Saj candle = Huge green candle.

Satoshi = The satoshi is currently the smallest unit of the bitcoin currency recorded on the blockchain. It is a one hundred millionth of a single bitcoin (0.00000001 BTC).

Satoshi Nakamoto = The name used by the unknown person or group of people who designed bitcoin and created its original reference implementation.

Scammer = You are nobody in the industry until you are either called a scammer, or you have called someone else a scammer. It is a rite of passage. A popular bitcoiner, @tone_LLT would have nothing to say if you removed the word "scam" from his vocabulary.

Script = An alternative proof-of-work system to SHA-256, designed to be particularly friendly to CPU and GPU miners, while offering little advantage to ASIC miners.

SegWit (Segregated witness) = A proposed scaling solution for bitcoin involving a soft fork.

Selling Pressure = Occurs when the majority of traders are selling, indicating that the majority think the market price will decrease.



SF = "Soft fork".

SHA-256 = A cryptographic algorithm used by cryptocurrencies such as Bitcoin. However, it uses a lot of computing power and processing time, forcing miners to form mining pools to capture gains.

Shill = The act of unsolicited endorsing of the coin in public. Traders who bought a coin has an interest in shilling the coin, in hopes of igniting the public's interest in that particular coin.

Shitcoin = This is not necessarily a bad term. Traders don't avoid a coin because it is a shitcoin. There have been seen traders rally a coin with a broken blockchain. Just never fool yourself and start believing in a shitcoin.

Short term hold = The term for holding onto coins for a short amount of time, usually seconds to minutes and sometimes a few hours before trading them. To take a short position on a coin is to believe its value will fall in the future.

Signature = A mathematical operation that lets someone prove their sole ownership over their wallet, coin, data or on. An example is how a Bitcoin wallet may have a public address, but only a private key can verify with the whole network that a signature matches and a transaction is valid. These are only known to the owner and are basically mathematically impossible to uncover.

Silk Road = The first modern dark net market, achieved notoriety. Subsequently shut down by the FBI who then auctioned confiscated bitcoins.

Small Blockers = Those who believe in a scaling path that does not require an increase in the block size of Bitcoin. Namely, Bitcoin Core and their supporters.

Smart contracts = Smart contracts are contracts whose terms are recorded in a computer language instead of legal language. Smart contracts can be automatically executed by a computing system, such as a suitable distributed ledger system.

Soft fork = A soft fork differs from a hard fork in that only previously valid transactions are made invalid. Since old nodes recognize the new blocks as valid, a soft fork is essentially backward-compatible. This type of fork requires most miners upgrading in order to enforce, while a hard fork requires all nodes to agree on the new version.

Software wallet = Software wallets are installed on computers, phones, and other mobile devices.

Solidity = Solidity is Ethereum's programming language for developing smart contracts.

Support Level = A price point in which downward price movement is resisted due to market conditions.

Swing = Zig zag price movement (Upwards and downwards).

TA = "Technical Analysis". It is used by analysts to predict the price action and direction of a coin in the near future. Some people believe it is nothing short of quackery but many analysts think they can generate handsome profits with the typical volatility that occurs in crypto markets.

Testnet = A test blockchain used by developers to prevent expending assets on the main chain.

To the moon = This refers to a cryptocurrency's upward momentum as it keeps climbing in price, as in, "The price of this coin will one day go to the moon!"

Token = Same meaning as a "coin".

Trading bot = Many people trade cryptocurrencies using a bot as a way to generate passive income. Some famous trading bots are Haasbot, Tradewave, Zenbot, Cryptotrader, Gekko and BTC Robot.

Trading Volume = The total amount of crypto that was traded during a certain period of time.

Transaction block = A collection of transactions on the bitcoin network, gathered into a block that can then be hashed and added to the blockchain.

Transaction Fee = All cryptocurrency transactions involve a small transaction fee. These transaction fees add up to account for the block reward that a miner receives when he successfully processes a block.

TRX = A symbol for TRON currency.

TTD = "Time To Dump".

UAHF = "User Activated Hard Fork".

UASF = "User Activated Soft Fork".



USD = US dollar.

UTXO = "Unspent Transaction Output", which refers to a number of coins held by a specific wallet address.

Vitalik Buterin = A Russian-Canadian programmer who created Ethereum and is a co-founder of Bitcoin Magazine.

Volatility = A measure of the price movement of an investment over time. The cryptocurrency markets are well known for their high levels of volatility.

Wall = A term used for an extremely high candlestick followed by several more so steep that there's bound to be a hard dip afterwards.

Wallet = A secure digital wallet that houses private keys. It usually contains a software client which allows access to view and create transactions on a specific blockchain that the wallet is designed for.

Weak hands = Those who can't be patient and sell at loss when the market is down.

Web wallet = Also referred to as a hosted wallet. Web wallet is hosted by a third party.

Wei = A denomination to Ether, like cents to Dollars or pennies to Pounds.

Whale = This term is borrowed from gambling people. It means a trader with a fat account, usually one who is bullish (one who thinks the market will rise) on the price of any specific cryptocurrency. These people are also referred to as bullish whales.

White paper = In cryptos is prepared by a party prior to launching a new currency. A White paper is authoritative reports that inform readers in short to understand complex issues, solve problem and make right decision.

Winklevoss Twins = Early proponents of bitcoin, tried to establish a bitcoin ETF (exchange traded fund) which was rejected in March 2017.

XEM = A symbol for NEM currency.

XLM = A symbol for Stellar currency.

XRP = A symbol for Ripple currency.

Yellow paper = A formal paper that is used for research. It is type of thesis or research paper of specify topic and have not any legal or authorized value.



Acquiring Crypto

Getting started...

If you are just getting into crypto, you will want to start-off pragmatically. Here is a base template for someone new to crypto to help get started.

You will first want to do ample research in identifying any particular cryptos, which you may want to invest. If you are unsure and just want to jump on the Bitcoin wagon, then you certainly can – and doing so will help get you initiated into the process of buying, transferring, securely storing and keeping records. Over 2018, the landscape will expand in a remarkable pace and so the rudimentary learnings will be an important stepping stone to helping you warm up to the technology and gain confidence handling your new “virtual” money.

You will also want a cryptocurrency hardware wallet. Using anything other than a hardware wallet is like taking your savings and storing it in a glass jar in your closet instead of paying \$100 for an unbreakable safe. If you just plan to acquire readily available cryptos from various exchanges then a single hardware wallet will be enough. If you want to acquire cryptos for your portfolio, which are only available on the decentralised Exchange EtherDelta – then you should additionally purchase a second hardware wallet, which must be a Ledger Nano S for using the EtherDelta Ledger Plugin. Setting up and getting started with the hardware wallets is an easy process, just follow the manufacturer's instructions on setup writing down your seed phrase by hand and not on your PC.

You will then want to sign up for an account with a reputable Australian exchange and deposit funds – and also have an understanding of your personal financial “layout”.

Example personal financial structure layout

You may develop your own system and financial layout based on your circumstances. However, if you do not have any idea what you are doing and have not entered into the crypto world yet – here is a base design which you may want to think about.

As an individual, not trading, no ABN, no SMSF, and just a desire to invest in crypto and hold for the long term, a suitable approach which you could take could look like the following.





Without drawing lines between the above pictures, I will explain what is going on. Joe Citizen wants to buy crypto. He earns his salary or wages which land in his Australian Bank account. He also has an account setup in his name on an Australian crypto exchange known as Independent Reserve. He also has purchased two (not one) cryptocurrency hardware wallets. One of the hardware wallets is a Trezor, which he calls his "Vault". His other Hardware Wallet is a Ledger Nano S which he uses only for the purpose of interacting with EtherDelta (a decentralised crypto exchange) to buy his ERC20Tokens and he refers to this as his "EtherDelta Staging Wallet".

He transfers his AUD from that bank account and deposits it into Independent Reserve. He buys his crypto from Independent Reserve, then withdraws it directly to his "Vault" for long term safe storage. If he wants to purchase a particular ERC20Token, he specifically buys Ethereum (ETH) from Independent Reserve and transfers said ETH to the "Staging Wallet" on the Ledger Nano S – then buys desired ERC20Tokens on EtherDelta – then transfers them off to his "Vault".

Feel free to adopt this layout as this document will refer to "Vault" and "Staging Wallet" for the guide. If you are only wanting to invest in Bitcoin (BTC) and Ethereum (ETH) – then you do not need an EtherDelta Staging Wallet.

Some notes regarding the layout

- The "Vault" can be a Trezor or a Ledger Nano S.
- The EtherDelta Staging Wallet must be a Ledger Nano S – as EtherDelta has a software plugin designed to work with the Ledger Nano S, but not Trezor.
- A separate Ledger Nano S is used for interacting with EtherDelta. This is not crucial; however, I do not trust that the EtherDelta code is not one day changed, phished or exploited in future to generate transaction data that drains other coins out of the Ledger Wallet when you authenticate them with the Ledger Wallet. Of course, EtherDelta is on GitHub and code is visible, but better to mitigate as many risks as possible – additionally if you acquire a significant amount of crypto – the last thing you want is to have your Ledger Wallet always on your person when you take into consideration the suggestions in the Security sections of this document.



- If Joe had an ABN, he would have a separate bank account in the name of the ABN and would replicate the above structure for his ABN – using his ABN or Trading Name on all accounts. He may also replicate the above once again for his SMSF meaning that in total he would require 6 crypto hardware wallets!
- Joe does not create any more wallets, or use multiple addresses under the hardware wallets (i.e. using all 5+ wallets available within his Trezor) because he likes to keep tracking his tax obligations as manageable as possible.

The process

Before even purchasing your first crypto – you should have done the following:

- 1) Setup your Secure Hardware Wallet(s) - (i.e. Trezor or Ledger Nano S)
- 2) Identified the specific crypto asset you want in your portfolio and the amount of it based on your confidence model portfolio allocation strategy. Once you know what you want, you then go the safest, least complex route of acquiring it and then send it to your secure hardware wallet such as your "Vault" as described above.

For this example, let us assume that you have \$3000AUD in fiat currency, which you want to invest into 50% BTC, 25% ETH and 25% ERC20Token.

Exchange selection

Whilst there are many exchanges in Australia which are available, the two best in terms of reliability and price are btcmarkets.net (<https://btcmarkets.net>) and Independent Reserve(<https://www.independentreserve.com>).

In this example, we will use Independent Reserve. Independent Reserve is reputable for the following reasons.

- Always a competitive Price with lots of liquidity in the order books to ensure you are getting as close to "spot" market value and are not simply ordering through Joe Citizens garage BTC operation charging 7-15% above real market price for your crypto purchase.
- Excellent online reputation and reviews.
- Excellent support.
- The CEO Adrian P, is regularly involved with Parliamentary enquiries and the regulation process. This shows an avid determination to be compliant with all legislative requirements which addresses ongoing operations.
- Excellent features including a "duress" password for your login to the exchange. PGP Email signing (for those that use it), and other general security-minded exchange features.
- The ability to create an Exchange Account in the name of an Individual, a Company, or a Self-Managed Super Fund.

For the purposes of this document, we will use Independent Reserve as the example of how to acquire your desired crypto.



The author has no affiliation to Independent Reserve and this is not an endorsement.

Account creation

The account creation step is fairly simple. Click on "Create Account" and read what is on the screen in front of you to create an account. Use your correct legal details.

Depositing funds

Depositing funds is relatively straightforward, but there are some very important things to look out for. Independent Reserve accepts many currencies, including AUD, NZD, USD, BTC and ETH. The things to note during the process are as follows:

- Independent Reserve refers to Bitcoin (BTC) as XBT. Do not be scared off by this, as XBT is a common Ticker Symbol Acronym used to represent the underlying asset of the original, 2009 Satoshi Nakamoto invented Bitcoin Blockchain. When purchasing XBT from Independent reserve you are buying the real thing. It is not Bitcoin Cash (BCH), Bitcoin 2X Segwit NYA (B2X) or any of the other bitcoin "forks".
- Be very careful and specific EVERYTIME that you make a deposit into Independent Reserve. Ensure you check and double check the Account Name, BSB, Account Number and Reference EACH AND EVERY TIME that you make a deposit. Banks in Australia give Crypto Exchanges a hard time and it is not uncommon for accounts of exchanges to encounter issues and the Exchange to have to utilise one of its other accounts for deposits at the time of your particular purchase.
- Ensure you are clicking the correct button relevant to the currency, which you are depositing (or withdrawing). Ensure if you are depositing \$AUD, that you click the deposit button next to the AUD listing.

Timeframes have been quite predictable with Independent Reserve. Provided that you send the Transfer (i.e. via NetBank Transfer) with all of the correct details (especially Your Account Reference which is usually a 7-letter combination), you can expect it to show up on Independent Reserve within 12-24 hours. Once the funds have arrived on Independent Reserve, you are then able to move forward in purchasing your desired crypto.

Purchasing crypto

Provided your funds have been received and credited to your Independent Reserve Account, you can now proceed to purchase your desired crypto. For this example, we will assume that you have \$3000AUD and wish to purchase 50% Bitcoin (XBT), 25% Ethereum (ETH), and 25% ERC20Token.

Before we go any further, it is to be noted that the Independent Reserve website has a drop-down list to specify whether you are buying ETH or XBT(Bitcoin). These drop-down menus are there under the "Trade" menu... Be aware of them.



One thing to note is that if you are unfamiliar with general markets is the lack of a straightforward "Buy" or "Sell" button. Instead, you will generally have 'BUY(Limit)' and 'BUY(Market)' buttons.



The operational model of the exchange includes an orderbook for buyers and sellers to negotiate price, and this model allows the exchange activity to happen in a relatively orderly fashion. It is the dynamic of supply and demand which will dictate the price of the underlying asset, and this dynamic over time is what is represented on the many charts you probably have seen which reflect the price of the asset over a period of time. This essentially means that you are not walking into some retail outlet that essentially sells crypto and simply purchasing it at a set price like you would a burger at McDonalds, or an item from Kmart. The price can (and will) fluctuate in front of you right before your eyes.

The difference between a Limit BUY and a Market BUY is simple.

If the price is currently going up and down between \$10,000 per Bitcoin and \$10,280 over several minutes of you watching it, and you are only willing to pay \$10,000. Then placing a LIMIT BUY for 0.15XBT @ \$10,000/XBT price point, then a LIMIT order allows you to specify that. Keep in mind however - if the dynamics of supply and demand dictate that there is more demand at that period than supply, it is possible that your order might never be filled. This is because someone is not willing to sell bitcoin at that price (and the price may never go below \$10,001 again for some period of time, or ever).

On the other hand, when doing a Market BUY, you simply specify how much you want to spend (i.e. \$1500 AUD), and you will essentially be filling the sell orders from the exchanges orderbook which is comprised of other people's Limit Sell orders. This gives you the feeling of it being more like a retail purchase and I would recommend using a Market BUY order if you simply just want the crypto now, and are not actively trading.

Once your Limit order is filled, or you have performed a Market BUY, your account will reflect a credited balance of XBT. Now that you have secured your XBT, you can proceed to purchase the ETH.

Currently, Independent Reserve only supports XBT, ETH and BCH. This is perfectly fine, as for this example you also wanted 25% ETH and 25% ERC20Token. Try to think of an ERC20Token as a "Sub-Token" of the Ethereum Blockchain. So, when you send and receive ERC20Tokens, you use the same wallet address as your ETH address. So, to purchase your ERC20Token portion (25% ETH, + 25% ERC20-Token) you actually want to purchase 50% ETH (\$1500AUD worth). Do so via your desired Limit or Market BUY method and then withdraw them from the exchange into your Hardware Wallet. To find out what the Wallet Address of your hardware wallet is, you can use the Trezor Wallet application or the Ledger Nano S application. **It is suggested that if this is your first time buying crypto – that you send a very small amount to begin with to familiarise yourself with the process.**

Just remember, be conscious and have the mindset that your crypto is not secured for long-term storage until it is in the address of your Trezor or Ledger Nano S. Do not leave your funds sitting on an exchange if you are not confident in your personal security practices – and do not leave funds on the exchange for long periods of time in any circumstance. Once you have purchased the desired \$1500 worth of XBT and \$1500 worth of ETH, withdraw these amounts to your hardware wallet from the "accounts" page. The next chapters of this document will focus on how to transmute your BTC or ETH into other forms of crypto which you may desire.



Acquiring ERC20Tokens and other crypto through Shapeshift

ShapeShift is a useful tool for exchanging one type of crypto into another type of crypto (i.e. Bitcoin to Litecoin, Ethereum to ERC20Token, etc). Provided that your hardware wallet supports the specific type of crypto you are after, you can send funds (i.e. ETH) from your hardware wallet, and convert it into your desired other crypto and have them sent back to your hardware wallet in the form of your desired crypto at a somewhat reasonable conversion rate.

The website address is <https://shapeshift.io>. Take some time to familiarise yourself with their "Getting Started" page and read online guides to familiarise yourself with the process. It is of note that shapeshift support a lot of the most common cryptocurrencies and the process is easy to perform. As I am sure you have done a significant amount of due diligence, self-education and research into your desired crypto, you will know what you are doing enough to understand how to use shapeshift and so a step by step guide on such is outside the scope of this document.

Acquiring ERC20Tokens and other crypto through the Exodus Wallet

The Exodus Wallet is a very user-friendly software wallet which you can install on your PC. It provides a very useful interface and has also integrated several coins available via ShapeShift. Not every crypto available via ShapeShift is available to exchange via the Exodus Wallet, but the list of supported cryptos is regularly expanding. The Exodus website is <https://exodus.io>.

Acquiring ERC20Tokens and other crypto through other exchanges

Other exchanges such as Bittrex (<https://bittrex.com>) and Poloniex (<https://poloniex.com>) offer a wide array of crypto trading pairs. Familiarise yourself with the exchange interface and keep track of any purchases you make. Do not leave your coins on these exchanges for any significant period of time.

Acquiring ERC20Tokens from EtherDelta

Some particular crypto offerings are only available from decentralised exchanges like EtherDelta. EtherDelta is not a company, but rather a software program running which allows people to trade in a somewhat orderly fashion. The step-by-step guide for exchanging your ETH into ERC20Tokens via EtherDelta is included in the scope of this document because it is often the only place to acquire some more "fringe" or newly released cryptos, but also has one of the largest array's of ERC20Tokens available as at the time of writing.

Warnings

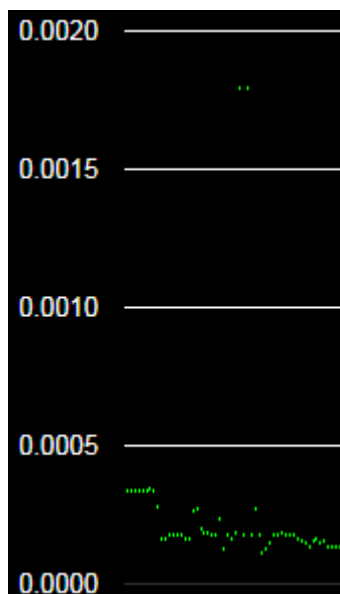
It is important to be careful when using EtherDelta. People have lost money on EtherDelta in many different ways.

There was an incident in Q3 2017 whereby the Admins/Creators of EtherDelta decided to change where on the internet it was hosted and redirected it from GitHub to a new URL <https://etherdelta.com>. Access to the site was lost for about a day and panic ensued. Eventually those stuck with funds on the Decentralised Exchange had to go through a very arduous task of sending code commands to the EtherDelta Smart Contract on the Ethereum Blockchain to withdraw their funds back out – something which is beyond the grasp of most people and is beyond the scope of discussion for this document.



Ensure you always manually type the address in your browser each time, or type it once, and save it as a favourite/bookmark in your browser. Additionally, always check that the site spelling is correct and that it begins with "https" and not "http". Once you send crypto to a fake site, consider it gone forever.

Also, when using EtherDelta, be extremely careful and take your time confirming and reconfirming any orders you place. Many people have done the old "fat-finger" mistake and mistyped their intended buy or sell price only to have lost hundreds of thousands of dollars in some instances. The below screenshot has two green dots showing 1 or 2 people who have essentially paid 10x the price for a particular token simply because they left out an extra "0". It happens more than you would think.



In addition, before going through with acquiring any ERC20Tokens on EtherDelta, or handling crypto in general, be sure to re-read through and familiarise yourself with the other security practices mentioned in this document.

One last thing for those doing this for your first time – EtherDelta only interacts with the Ethereum Blockchain. Only Ethereum and ERC20Tokens can interact with EtherDelta. Do not try to send Bitcoin or another Blockchain asset to EtherDelta.

EtherDelta Ledger Wallet Plugin

The EtherDelta Ledger Wallet plugin is an astounding convenience and security measure. Not only does it ensure that your private key is protected whilst using EtherDelta, but it also generally abiding by the same security concepts which are wise for general usage on a PC. Although this does not protect against the potential unknown outages, or human error. This is a reason, whereby if your personal investment strategy includes purchasing ERC20Tokens via EtherDelta, that you should purchase a Ledger Nano S for the specific reason of using the Ledger Nano S plugin of EtherDelta and using said Ledger Nano S as an "EtherDelta Staging Wallet".

EtherDelta Staging Wallet

Try to always use the Ledger Nano S Plugin for use with EtherDelta, and re-use the same wallet for "staging" funds for use with EtherDelta. Many will say that it is best to use a different Ethereum Wallet



each time, and doing such is certainly easy once you get the hang of it. However, to keep Tax recordkeeping easy to follow, allocate one Ledger Nano S for this specific purpose.

This guide will assume that you do not have a Ledger Nano S and hence, will show you the process without the Ledger Nano S plugin. Do note however, that you should be strictly adhering to security principles if you are going to use this method. Do not use a PC of which you even remotely suspect may be infected, and strictly minimise the time of which funds are placed in the EtherDelta Staging Wallet, returning the funds to your Trezor or Hardware Wallet immediately after acquiring them.

There is also an option to use MetaMask on EtherDelta, but I find that just as insecure as this method, and will advise new users not familiar with MetaMask to not install or use MetaMask with EtherDelta.

Getting to EtherDelta

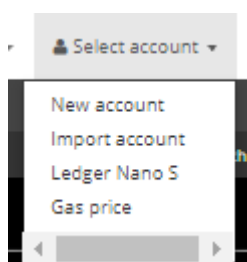
OK, so to get to EtherDelta, type in your browser <https://etherdelta.com>. DO NOT Google it and click a link – instead, manually type it with exact spelling. Once there, confirm the Lock icon in your browser is visible and that the path still contains “https”. Once confident, save it as a favourite or bookmark for future.



Creating a new Ethereum Wallet for use as an EtherDelta Staging Wallet

This step is only necessary if you do not have a Ledger Nano S and are not using the Ledger Nano S Plugin.

In the top right hand corner, you will see a “Select account” button. Click on that and go to “New Account”. **However, if you are using a Ledger Nano S – instead of clicking on “New account”, click on “Ledger Nano S”.**



If not using the Ledger plugin, a small informational screen will show up giving you a new Wallet Address which you should consider your EtherDelta Staging Wallet. The top key is your Public Wallet Address, and the bottom key the almightily important Private Key. It cannot be stressed with enough importance that if you do not write down this Private Key, and you send funds to the top listed public key wallet address, you will not have access to your funds. That bottom Private Key is essentially the Key to a new, fresh wallet for which you will use with EtherDelta and it is of critical importance. When it says “BACKUP” it means it.





You just created an Ethereum account:
0xEFECd0e62a05423b7e3eC391C881D3Db7A63

Please BACKUP the private key for this account:
be76614a47fe237f4998f85b30f8689dd1dbfa64a8:

If you do not want to write it down (which can be risky subject to human misspelling), then create a new text document and save it in your PC in a plain text document, BUT remember – especially if your PC is not secure – you are conducting a security risk by storing said private key this way. This is another reason to acquire a Ledger Nano S and use the Ledger Nano S plugin.

Remember if your PC is currently compromised with a virus, it is quite possible that hackers will have scripts created in the future to automatically withdraw (steal) any funds you send to this wallet as soon as it happens. Consider this a temporary solution and never leave funds in this wallet sitting idle.

Depositing funds into the EtherDelta Staging Wallet

Now assuming for the rest of this guide that you do not have a Ledger Nano S – lets continue on. Note that you now have an Ethereum Wallet which you intend to use as a staging wallet for using and interacting with EtherDelta, you were shown and have recorded the public and private key of said ETH wallet. You now need to deposit some funds into that Ethereum Wallet.

Assuming you are Joe Citizens who had just spent \$3000 at Independent Reserve and purchased \$1500 worth of ETH, which you subsequently sent to your “vault” hardware wallet... It is at this point that you should send the 25% (\$750 worth) desired allocation or amount of Ethereum from your Hardware Wallet to this Staging Wallet which you intend to transmute into the ERC20Token(s). You can do this simply from the user interface of your hardware wallet, which if it is a Trezor will be <https://wallet.trezor.io>. Be mindful that you want to send ETH to the Public Wallet Address of your newly created Ethereum Wallet from the previous step. In the screenshot above, that is the address starting with “0xEFECd0e62~”.

Double check that you have the address correct and send the funds. After some time, the amount of Ethereum you sent should show up in that Wallet. You can check this by ensuring that in the top right-hand corner of EtherDelta – ensuring that your address (i.e. “0xEFECd0e62~”) is shown, followed by a quantity of ETH and a green “EtherDelta (Private Key)” sign is showing.

0.597 ETH EtherDelta (Private Key) ▾

Handy Tip: If you click on your account in the top right-hand corner of EtherDelta, it will display a drop-down menu showing many options.



- New account
- Import account
- Ledger Nano S
- Etherscan address
- Export private key
- Forget account
- Gas price

Of particular note is the "Gas price" menu, whereby you can adjust the Gas price you pay for interacting with the exchange. Compare the current "Recommended Gas Price" at <https://ethgasstation.info> and set the Gas Price in your EtherDelta session to a cheaper level than default, but ensuring that it is above the "SafeLow" recommended on <https://ethgasstation.info>. This ensures that you do not essentially spend any more for your transaction than you have to. Do note however, that during times of extreme load on the Ethereum blockchain you may need to manually set the Gas price value to "60" or higher just to get your transactions successfully processed.

Depositing funds from the Staging Wallet into EtherDelta
 You will also see an amount in the ETH row on the EtherDelta "BALANCE" area.

BALANCE		
Deposit	Withdraw	Transfer
Token	Wallet	EtherDelta
CDX	0.000	0.000
<input type="text" value="Amount"/>		<input type="button" value="Deposit"/>
ETH	0.597	0.000
<input type="text" value="Amount"/>		<input type="button" value="Deposit"/>

Looking above, the column of "Wallet" represents the funds in your EtherDelta Staging Wallet which you have created. The right-hand side "EtherDelta" column represents your account balance on the Decentralised Exchange EtherDelta.

You will also notice the three buttons above – Deposit, Withdraw and Transfer. Most new users will never use the Transfer button so ignore that one for now. You must first "Deposit" funds from your Staging Wallet ("Wallet") to the exchange ("EtherDelta").

Importantly, you must leave some amount of Ethereum(ETH) in your Staging Wallet to be used as "Gas" to pay for the transaction of sending your Ethereum to the exchange, as well as interacting with the exchange. So, for the example picture above, it can be noted that the "Wallet" now contains 0.597ETH. If the ETH network is not congested, and you are able to set your Gas Price to "1" or "2", then you can leave at least 0.01ETH in the "Wallet" for use as "Gas". If the network is currently congested, and you have needed to set your Gas Price to "60", you may need to leave up to 0.05ETH to "burn" as



gas for your EtherDelta transactions. For the purposes of this example, we will assume that the network is not congested and you have set your Gas Price to "2". So, at this stage you would enter 0.587 (or whatever your balance, minus 0.01) in the ETH row text input field and click the Deposit button...

BALANCE		
Deposit	Withdraw	Transfer
Token	Wallet	EtherDelta
CDX	0.000	0.000
<input type="text" value="Amount"/>		<input type="button" value="Deposit"/>
ETH	0.597	0.000
<input type="text" value="0.587"/>		<input type="button" value="Deposit"/>

After clicking on the Deposit button, you will be greeted with a popup like below...



You just created an Ethereum transaction. Track its progress:
[0xd34def1a5fd3410c261b94a5c34bfdebe6d89b845ecc3eb7ff](#)

You should click on the link which will allow you to watch the transaction take place in real-time. If you get any errors, feel free to repeat the previous step, utilising a slightly higher gas price if you suspect Ethereum network congestion is an issue. Once the transaction completes, you should then see the Balance of ETH in your "EtherDelta" account has appeared and your "Wallet" balance still has your desired 0.01 ETH for use of interacting with the exchange.

BALANCE		
Deposit	Withdraw	Transfer
Token	Wallet	EtherDelta
CDX	0.000	0.000
<input type="text" value="Amount"/>		<input type="button" value="Deposit"/>
ETH	0.010	0.587
<input type="text" value="0.587"/>		<input type="button" value="Deposit"/>

Purchasing your desired ERC20Tokens

You will notice a small drop-down menu at the top left-hand side of EtherDelta. From this drop-down menu, select the abbreviated ticker symbol for your desired ERC20Token which you would like to



purchase. For this example, we will purchase some CDX. If you are unsure or curious as to other tokens you see, you can browse <https://coinmarketcap.com> to explore.



Here is where it gets specific. The order book, whilst oversimplified, will show Sell Orders on top in Red, and Buy Orders on bottom in Green. Since we are purchasing CDX, we will be clicking on one of the Red Sell Orders on top which represents someone else on the exchange wanting to Sell CDX (or whichever Token you selected from the drop-down menu) at this time.

0.000260000	8000.000	2.080
0.000260000	614.376	0.160
0.000260000	614.376	0.160
CDX/ETH	CDX	ETH
0.000220000	3500.000	0.770
0.000215110	100.000	0.022
0.000215100	16.599	0.004
0.000210000	4760.000	1.000
0.000210000	4760.000	1.000

Handy tip: In the screenshot above, you will notice 3 orders, ALL at the same price of 0.00026ETH per CDX Token. If we now wanted to spend ALL 0.587 ETH we have on CDX Tokens, we have the option to click the order closest to the middle(cheapest), wait for the order to go through, then click once again on the order closest to the middle (cheapest), etc until we have spent all our ETH and received all our desired CDX Tokens. However, because the price is 0.00026 for all 3 orders, and we want a total of 0.587 ETH worth, it is easier and more cost efficient (when including transaction gas cost) to simply select the order above which is offering a parcel of 8000CDX (AKA 2.080ETH worth), and fill our 0.587 ETH worth from there. Be mindful and careful however that more often than not, the further from the middle point the Red Sell Orders are, the more expensive the price usually becomes. It is easy to make mistakes... so take your time and get it right.

However, as I only want to buy 100 CDX for this example, I will click on ANY of the 3 Red Sell Order parcels above and type in my desired amount as shown and click Buy.



Buy

Order

8000.000 CDX @ 0.000260000 CDX/ETH
Expires in 9578 blocks

Amount to buy (CDX)

ETH

Fee (ETH)

You should then see another popup window displaying the transaction, of which you can click on the link to watch the transaction complete in real-time.



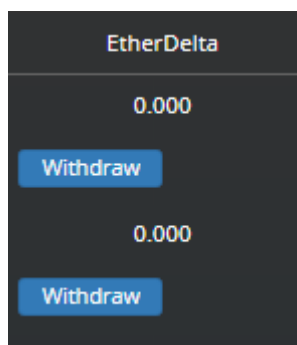
You just created an Ethereum transaction. Track its progress:
[0xf9c2cd05431875deda91a4bb22f5ddf0e549f4dc948ba43c74](#)

Once the transaction is done, we will see the balance of our desired Token in our "EtherDelta" account. So just as with the Deposit process, except this time in the text input field of your desired token (top row) – type in the amount you wish to withdraw (in this case 100CDX), and click the Withdraw button.

BALANCE		
Deposit	Withdraw	Transfer
Token	Wallet	EtherDelta
CDX	0.000	100.000
<input type="text" value="100"/>		<input type="button" value="Withdraw"/>
ETH	0.010	0.561
<input type="text" value="Amount"/>		<input type="button" value="Withdraw"/>




When you are finished with acquiring all the ERC20Tokens you set out to get, and have withdrawn all tokens, and all remaining Ethereum in your "EtherDelta" account (if there is any) ... Feel free to close your browser.



Sending funds from your EtherDelta Staging Wallet to your Hardware Wallet "Vault"
In this section I will introduce you to a very handy tool called MyEtherWallet. Whilst the Ethereum Blockchain exists in a distributed fashion, MyEtherWallet is a company which has provided a very useful interface for interacting with the Ethereum Blockchain in the form of a website.

As with browsing to EtherDelta, you carefully need to browse to <https://www.myetherwallet.com>. Check the Lock symbol is displayed and that the address is spelled exactly as shown.

 MYETHERWALLET LLC [US] | <https://www.myetherwallet.com>

If you are confident that the site is spelled correctly, then save it to your favourites or bookmark the page.









Next, click on the heading button which states "Send Ether & Tokens".

If using your Ledger Nano S – select Ledger Wallet from the options and proceed from there. Otherwise, if using your EtherDelta provided wallet which you saved in plain text, then select "Private Key" and type your Private Key into the text input box to the right. It is of note that the Private Key which you enter here is the one created in the previous step and is the Private Key of your EtherDelta Staging Wallet.



Send Ether & Tokens

How would you like to access your wallet?

- Metamask / Mist 
- Ledger Wallet 
- TREZOR 
- Digital Bitbox 
- Keystore / JSON File 
- Mnemonic Phrase 
- Private Key 
 - Parity Phrase 
- View Balance Only (Must use one of above options to send)

Paste/Type Your Private Key

```
4838196be14x6c4e649e0f086b126f  
8|6b612f9710xcb
```

It is of note at this step whereby you will see your exposure to potential keyloggers and screen capturing PC malware. It is at this point where you would rather be selecting "Ledger Wallet" instead of typing or copy/pasting your precious Private Key.

Once you have entered your Private Key, click the "Unlock" button.


Now click on the "Load Tokens" button to have it display any tokens you have in your EtherDelta Staging Wallet.



You should then see your Token Balance which you purchased and withdrew from EtherDelta available under the "Token Balances" section.



Token Balances

 Remember, you can always view your Balances On <https://etherscan.io> or [Ethplorer.io](https://ethplorer.io)

 Not seeing your token? [Learn how to Add a Custom Token](#)

100

CDX

Show Tokens

Add Custom Token

Also, if desired, take the time to adjust your Gas Price value in the top right-hand corner of MyEtherWallet. Remember, you can see the current SafeLow value at <https://ethgasstation.info>.

Gas Price: 1 Gwei ▼

Now, importantly, copy and paste your Public Wallet Address of your Hardware Wallet ("Vault") in the To Address field.

Select the token type (double-check you select the desired token type) and click on "Send Entire Balance". If you have double checked that you have the correct token type (i.e. CDX in this example, not the default ETH), then proceed to click Generate Transaction.

Send Ether & Tokens

To Address


0x7cB57B5A97eAbe94205C07890BE4c1aD31E486A8

Amount to Send

100

CDX ▼

[Send Entire Balance](#)

 Gas Limit

21000

[+Advanced: Add Data](#)

Generate Transaction

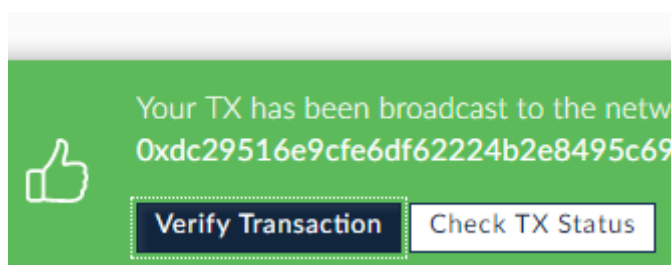


The Raw Transaction data will be displayed to you, and you should proceed to click on Send Transaction. In the screen that pops up, double check the details and actually read what is on the screen and if the quantity and address details are correct, proceed to click "Yes, I am sure! Make transaction".

Are you sure you want to do this?



You can then Click "Verify Transaction" to once again, watch the transaction take place in real-time.



Congratulations! You have now successfully drained your Staging Wallet of the newly purchased ERC20Tokens. Note that in this example I transferred 100qty CDX Tokens, and that your Token symbol will not be CDX but the ERC20Token symbol of the token you desired and purchased. Now one last step is to change the drop-down list from CDX (or your selected ERC20Token) to ETH, and finish draining all the ETH from the Staging Wallet back to your Hardware Wallet also. Remember to click the "Send Entire Balance" button before clicking on Generate Transaction and Send Transaction.

Amount to Send



Please take note that it is a wise decision to always keep a little bit of ETH in your Hardware Wallet for any future transactions where you wish to send ERC20Tokens from your Hardware Wallet.



Guide To Keepings Records With CoinTracking.info

This document has extensively covered the importance of record keeping. This chapter will go through the rudimentary underpinnings of how to effectively keep track of your crypto tax obligations so that you have a clear picture when tax-time approaches.

There are a few software products on the market designed to help you keep track of your crypto activities abiding by the First-In-First-Out method, however cointracking.info seems to be a significant step above the rest for the underpinning legalities of the matter.

To receive a 10% discount on your purchase of CoinTracking you can use this referral code. You may need to type this URL manually into your browser if the link is not "clickable".

<https://cointracking.info?ref=E816709>

Setting up an account at cointracking.info

Account setup is relatively easy. Browse to <https://cointracking.info>, and click the register button. Follow the steps to create your account.

If your crypto affairs become more complex than just the individual, single-wallet white-knuckler – then you may find yourself needing to upgrade your account from a FREE plan to a PAID plan.

Importing your crypto data

One of the things that sets cointracking.info apart from others is that they have the largest library of importing features available on the market. This helps you to get started with tracking your crypto using their site in a quick and easy way. Ideally to get up and running in the fastest way, your best to import all of your crypto related blockchain data using their import wizards, and then making the adjustments as described in the following paragraphs in order to increase the accuracy.

Connecting to your exchange API to import your exchange data

In this example, I will use Independent Reserve, however, the process should be very similar for most exchanges. To import your Independent Reserve Data, cointracking.info provide and API wizard for such. You will first need to create an API Key in the Independent Reserve website. This can be done by going into Settings > API Keys > Generate API Key. **It is important to ensure that you DO NOT tick the box that states, "Allow this API Key to withdraw Digital Currency".**

Generate API Key

Confirm generation of a new API Key by entering your password.

Allow this API Key to withdraw Digital Currency ⓘ



Once you have created this API Key, you follow the wizard for Independent Reserve API connection on cointracking.info and enter the API Key when prompted. This is accessed by going to Enter Coins > Exchange API Imports > Independent Reserve API on cointracking.info whilst logged in.

Importing and monitoring your various blockchain addresses

Cointracking.info has import wizards for almost every type of crypto. Use the relevant import wizard for your various cryptos. Be sure to include them all. Apply the same tax treatment and record keeping methodology to all cryptos.

How to record certain Events

Various events in the crypto world will be taxed differently. Here is an overview of common events, whether they are taxable, how to record them in cointracking.info and the reasoning behind each one. It is important to note that the guidelines refer to tax residents of Australia only. It is important to note that tax laws can be changed and are likely to change once regulation is formalised for crypto. For now, below is a practical guide on how to record your potential taxable events in your crypto endeavours for future tax use.

Network Transaction Fees

Taxable Event: No

Reason: According to the ATO guidelines 2014, transactions whereby a person is paying for goods or services online, under the value of \$10,000AUD does not generate a CGTA1 Disposal event. Because the amounts will always be under \$10,000AUD for a transaction fee and that indeed you are paying for an online service (paying miners/stakers for providing the consensus framework) it is safe to say that Network Transaction Fees are one of the easiest to identify in terms of non-taxable events for Australians.

How to record in cointracking.info:

List as a "Spend". [Cointracking.info](https://cointracking.info) may or may not be able to automatically get this data for some blockchain assets and you may need to do a .csv dump from the specific blockchain explorer is available and possible. It is worthwhile to do this as it affects your long-term FIFO tax rates. Additionally, taking the time to input them can have compounded tax effects for business; and such events are arguably tax deductible unless explicitly regulated in the future.

Exchange Fees

Taxable Event: No

Reason: According to the ATO guidelines 2014, transactions whereby a person is paying for goods or services online, under the value of \$10,000AUD does not generate a CGTA1 Disposal event. Because the amounts will always be under \$10,000AUD for a transaction fee and that indeed you are paying for an online service. It is also of note that such Fees are tax deductible if you are exchanging under your ABN or a business structure.

How to record in cointracking.info:



List as a "Spend". Cointracking.info may or may not be able to automatically import this data for some exchanges. If so, then enter them manually into cointracking.info. Additionally, compile a report at the end of the financial year and list it all as an expense in your accounting software (i.e. Xero) for the entity which you paid said fees.

Spend crypto for item valued at < \$10,000AUD

Taxable Event: No

Reason: According to the ATO guidelines 2014, transactions whereby a person is paying for goods or services online, under the value of \$10,000AUD does not generate a CGTA1 Disposal event.

How to record in cointracking.info:

List as a "Spend". Cointracking.info may list this as a "Withdrawal". If such is the case – Manually edit this to a "Spend". Backup and keep receipts in case you need to provide proof of the spend. Although in future Crypto linked debit cards should provide transaction statements which can be substituted.

Spend crypto for item valued at > \$10,000AUD

Taxable Event: Yes

Reason: According to the ATO guidelines 2014, transactions whereby a person is paying for goods or services online, under the value of \$10,000AUD does not generate a CGTA1 Disposal event. This does not cover large value purchases. This is a taxable event which generates a CGT A1 Disposal Event.

How to record in cointracking.info:

List as a "Trade(Exchange)" between the specific crypto and AUD. Cointracking.info may list this as a "Withdrawal". If such is the case – Manually edit this to be a "Trade (Exchange)". Backup and keep receipts in case you need to provide proof of the spend or track disposal prices.

Convert crypto to fiat in any way

Taxable Event: Yes – Capital Gains A1 Disposal Event. Even if amount is <\$10,000AUD. Even if immediately used to buy an item from said fiat as a "spend". *Except if the other party receives the crypto into either their own crypto wallet, or a third-party payment processor, of which an account on behalf of the other party is owned (i.e. a retailer which has a BitPay payment gateway to sell their goods, regardless of whether they choose to receive the crypto or fiat for payment on their end – these instances would be a "spend" if <\$10,000AUD and for a good or service).*

Reason: This is a direct representation of a CGT A1 Disposal Event. Record in Cointracking.info as described below to ensure Capital Gains are calculated correctly at tax time on any realised gains or losses.

How to record in cointracking.info:

List as a "Trade(Exchange)" between the specific crypto and AUD. Cointracking.info may list this as a "Withdrawal". If such is the case – Manually edit this to be a "Trade (Exchange)".



Rollover crypto assets during a divorce related Property Settlement

Taxable Event: No* – Provided the process is documented thoroughly and match the criteria defined within <https://www.ato.gov.au/general/capital-gains-tax/relationship-breakdown/agreements-the-rollover-applies-to/>.

Reason: Classified as an Intangible Asset, a CGT rollover can be performed, whereby the Cost Basis for CGT calculation can also be transferred to the other party. The criteria for ensuring this is possible is quite extensive and so an amicable property settlement is required.

How to record in cointracking.info:

List as a "Spend" if the criteria defined above are met, otherwise a CGT A1 Disposal event will take place, in which instance you should list the disposal as a "Trade (Exchange)" to the relevant AUD value. Cointracking.info may list this as a "Withdrawal". If such is the case – Manually edit this as a "Trade (Exchange)" if a CGT Event is recordable or a "Spend" if not.

Sell or exchange crypto purchased at ICO price with bonus, but not spend it

Taxable Event: Yes

Reason: This is a direct representation of a CGT A1 Disposal Event. Record in Cointracking.info as described below to ensure Capital Gains are calculated correctly at tax time on any realised gains or losses. You must ensure that your Cost Basis includes bonus Tokens and the relevant AUD value for entry is accurate including said bonus Tokens.

How to record in cointracking.info:

List as a "Trade (Exchange)" whereby if selling for fiat, the sell amount and price were in AUD. If selling for crypto, the purchase price for newly acquired crypto would form the disposal price for the ICO Tokens. Do note however, the Cost Basis price for your investment into ICO would be the AUD equivalent at which time you entered the ICO, NOT the first recorded price or value of Token once it hit an exchange, and as such any Cost Basis calculations in Cointracking.info may be wrong. If as an example, you entered the ICO for 1 x ETH and received 'n' number of specific Tokens in exchange for that one ETH. At the time you sent the 1 x ETH to enter the ICO, ETH was at \$500AUD. The collective price for all Tokens received would be \$500. So, the price per Token which forms your Cost basis would be \$500 divided by the number of Tokens received during the ICO. The transaction recorded in Cointracking.info which constituted you contributing to the ICO would be listed as a "Trade (Exchange)" of ETH to AUD, and the receipt of your tokens in your Wallet will also need to be edited to list the Tokens "Deposit" as a "Trade (Exchange)" from \$500 AUD to 'n' total Tokens.

Cash purchases and sells (i.e. Localbitcoins.com, or P2P trade)

Taxable Event: No - for purchasing in cash or other medium. Yes - for disposal to Cash or other medium which is not a personal consumption item <\$10,000AUD value.

Reason: According to the ATO guidelines 2014 (reference here), transactions whereby a person is paying for goods or services online, or personal consumption items under the value of \$10,000AUD does not generate a CGTA1 Disposal event. It is of note that converting crypto to fiat on any exchange, including into cash via a personal transaction is a taxable disposal event. If your cost basis is



higher than your disposal price you can claim a loss. If your cost basis is lower than your disposal price you will have to pay tax on the amount of realised gain. If your transaction (purchase and disposal) is done in cash you should include and record as much detail as possible regarding the transaction.

How to record in cointracking.info:

Manually enter relevant details into Cointracking.info as a "Trade (Exchange)" if buying or selling. Except in the instance that you were buying an item for personal consumption directly with the crypto – in which instance you would list it as a "Spend".



Thinking In Crypto Or Fiat Terms (End Note)

It is only a matter of time after you start interacting with crypto as a form of value that your predispositions and affection for forms of money which you have grown to be accustomed to change. Your world-view expands and you start to realise that maybe you start measuring your personal wealth in terms of crypto holdings and not fiat holdings.

When you understand the reality of the future that is coming, you can truly appreciate it as a work of genius that will push society forward. Good luck with your own crypto journey and do not get lost in the wild world of crypto.



If you enjoyed this guide:

The next project is a follow-up eBook (ETA March 2018) covering many topics including, but not limited to:

- Investment landscape update and practical guides for any new developments.
- Handling your income from various crypto endeavours and directing the funds (i.e. ABN) to maintain tax compliance with ease and surety.
- Creating a low power, immaculately secured multi-crypto staking server.
- Various guides and strategies to maximise your ROI for various passive income crypto platforms.
- Documentation to accompany your SMSF for justifying your portfolio allocations, security standards guide, investment limitations statements, risk tolerances, etc.
- Preparing all your collected info for Tax Submission to your accountant, bookkeeper, or the ATO directly for FY 2017/2018 Tax Assessment for any activities for you as an individual, as a Sole Trader, business or SMSF (Corporate Trustee).





mobile: +61439333379

email: disrupt@47.com.au

SYDNEY • MELBOURNE • BRISBANE • ADELAIDE • PERTH

www.47.com.au

Need Crypto Onboarding?

- Step 1 Download our Practical Guide to Crypto
- Step 2 Contact us to help you get into Crypto