Fomo, Moon, Lambo

The Complete Beginner's Guide to Cryptocurrencies

by Steve Tattersall

2020 Edition

Fomo, Moon, Lambo.

The Complete Beginner's Guide to Understanding Cryptocurrencies.

2020 Edition.

Published by Crypto Calligraphy Press.
Digital edition.

Although the author and publisher have made every effort to ensure that the information in this book was correct at the time of publishing, the author and publisher do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, external factors, or any other cause.

Disclaimer

This book is presented solely for educational purposes. The author and publisher are not offering it as professional, legal, financial, investment, or other advice. While best efforts have been used in preparing this book, the author and publisher make no representations or warranties of any kind, and assume no liabilities of any kind with respect to the accuracy or completeness of the contents, and specifically disclaim any implied warranties of appropriateness or fitness of use for a particular purpose.

Neither the author nor the publisher shall be held liable or responsible to any person or entity with respect to any loss or incidental or consequential damages of any kind caused, or alleged to have been caused, directly or indirectly, by the information contained herein. No warranty may be created or extended by website links, photos, videos, or written materials related to or referenced by the author and publisher. The content of any websites referenced in this book may change at any time.

The cryptocurrency markets are risky and unregulated. This book is not intended to provide investment advice, or to encourage the reader(s) to invest in any cryptocurrency or cryptocurrencies.

For the early adopters, because you believe in the potential

Fomo, Moon, Lambo: The Complete Beginner's Guide to Cryptocurrencies

www.beginnersguidetocryptocurrencies.com

Table of Contents

Fomo, Moon, Lambo: The Complete Beginner's Guide to Cryptocurrencies

www.beginnersguidetocryptocurrencies.com

Fomo, Moon, Lambo: The Complete Beginner's Guide to Cryptocurrencies

www.beginnersguidetocryptocurrencies.com

INTRODUCTION

This book, and the accompanying website, were created to be comprehensive learning tools for newcomers to the cryptocurrency space. Cryptocurrencies are going to become an increasingly important part of our society and daily lives in the coming years. At the time of publishing this 2020 edition of the book, the cryptocurrency ecosystem is still relatively young. Although Bitcoin is now more than ten years old, it will still be a few more years before the world sees mass adoption of cryptocurrencies by consumers. If you're reading this book, you can consider yourself to be an early adopter. You'll be well ahead of the curve when mainstream society starts using crypto on a daily basis.

These resources are designed for people with a general interest in learning about cryptocurrency and the potential risks and rewards that come with investing and using various cryptocurrencies. The authors of this book have two main goals. We wish to provide a general education on cryptocurrencies to those who are interested. We also wish to inform our readers on how to minimize risks, both in the form of scams and of hacks. When it comes to cryptocurrencies, there won't be any government agencies protecting you or your assets. You are your own bank, and the importance of following proper security precautions cannot be over-emphasized.

This book will not encourage you to invest in any specific cryptocurrencies, or even recommend that you invest in the cryptocurrency sector in general. Our goal is to give you an understanding of how cryptocurrencies will be and can be used as a type of money. However, this same education will be useful to those of you who are considering cryptocurrencies as an investment. Should you decide to follow that path, we can only recommend that you consider crypto to be a useful part of a balanced portfolio that might also include stocks, bonds, savings, commodities, and real estate. The cryptocurrency markets have traditionally been incredibly volatiles. Many fortunes have been made, and lost. Never invest more than you can afford to lose.

We have a request for you. Yes, for you. We've published this book and are distributing the digital editions at no cost. In return, can you do us a favour? After you're done reading the book, if you like what you read, please share your digital copy of the book with one or two friends. That's it. We're not trying to make money from book sales. We just want to make people comfortable with using cryptocurrencies, and help protect newcomers from making costly mistakes. Thanks for sharing our work.

And now, let's start to learn.

Section 1 – The Basics

WHAT ARE CRYPTOCURRENCIES?

A cryptocurrency is a digital currency. You can think of it in terms of digital and virtual money. No physical coins or paper bills exist for any cryptocurrencies. Cryptocurrencies exist only in a digital format. Some people say that cryptocurrencies are stored "in the blockchain," but a blockchain is a digital file, not a physical object. You can think of your money as existing either online or in a computer. The concept of non-physical currency may seem confusing, but today, the majority of money in currencies we are familiar with is already digital. When people refer to cash, they refer to the physical form of a currency, including coins and banknotes. In the United States, barely ten percent of all US dollars (USD) exist in the physical form of bills and coins. Almost ninety percent exists only in computers, in chequing accounts and in investment accounts and things like that.

A common criticism faced by cryptocurrencies is based on the fact that they are not backed by any physical asset. Of course, this can be argued to be true for most currencies around the world today. Again, using the United States as an example, that country dropped the gold standard in 1971, which means that the federal reserve no longer guarantees that US dollars are backed by that particular financial asset.

Some people argue that even though a national (fiat) currency is not backed by physical assets, it is backed by a government and by the rule of law.

This is true, but by the same argument, cryptocurrencies are backed by the rule of code. Computers aren't emotional, so the computer code acts as both a security mechanism and a court of law, whereby decisions (computations) are rendered consistently, and almost instantly. When it comes to value, it is fair to argue that the only true "value" of a currency is based upon what people, as individuals, believe it is worth. You can say that value is the ratio of exchange between any two goods, and money measures that value. But money by itself isn't worth anything unless people decide to agree that it is worth something.

The same applies to cryptocurrencies. If people decide that a single unit of a particular type of cryptocurrency is worth four chickens, and is willing to give up their cryptocurrency in return for four chickens, or sell their four chickens for that one unit of cryptocurrency, then two individuals have come to an agreement about the value of that cryptocurrency. This value fluctuates almost constantly, as people around the world buy and sell their cryptocurrencies, trading them for different types of fiat (traditional) currencies, or for other cryptocurrencies. Cryptocurrency exchanges help facilitate this trade, and websites such as www.livecoinwatch.com or www.coinmarketcap.com provide the current comparative value of different cryptocurrencies based upon what people are willing to buy and sell them for. Thankfully, most users and traders of cryptocurrencies think of their value in relation to other cryptocurrencies and fiat currencies, not in relation to chickens.

When early adopters of cryptocurrencies talk about their various projects, they often refer to things like "blockchains" and "mining" and "hash algorithms." If you're a member of the general public, you probably have no idea what some of these terms mean. In fact, your eyes may be glazing over just reading them. Don't panic. You don't necessarily need to understand any of these terms in great detail, any more than you need to understand how the

U.S. Mint in Philadelphia makes sure that every quarter produced has a heads side and a tails side. We will try to give you an overview of what everything means, and you can take from it what you will. If you're thinking simply about investing a few hundred dollars into Bitcoin and holding on to it for a few years, you may be fine just reading through all of chapters of this book quite quickly, to get a superficial overview. If you're curious about the exact technologies underpinning various alternative cryptocurrencies to Bitcoin, we'll give you a general overview and give you some guidelines for the many hundreds of hours of additional research that you'll need to carry out in order to get a comprehensive understanding of the various technologies used by different projects.

Unfortunately, there is a lot of confusion surrounding cryptocurrencies. Hopefully, this book and website can help alleviate some of that confusion. Many members of the general public have a fundamental lack of understanding about the basic workings of cryptocurrencies, because these cryptocurrencies have not yet achieved mainstream adoption. Not even close! Above and beyond that, there is some semantic confusion relating to the term "cryptocurrency." The term has been adopted and used to refer to thousands of digital projects, most of which are not even intended to function as currencies. We'll try to address that confusion, and give you more of a fundamental understanding of different cryptocurrencies and other projects that are mislabelled as cryptocurrencies.

CRYPTOGRAPHY

When you were young, you may have pretended that you were a spy, and exchanged secret messages with friends by using codes or ciphers. Cryptography refers to methods of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptocurrencies are intended to have value, and if everyone was able to access any amount of cryptocurrency without passing any sort of security test, then there would be no way to figure out who owns what. Therefore, whenever you buy or are given cryptocurrency, you are given a "private key" to unlock it. Nobody else on Earth should have your key or keys (if you hold multiple cryptocurrencies), and you should never share your keys with anyone else, period. This is the first principle to owning cryptocurrency: You don’t own the crypto if you don’t own the private keys.

Let us reiterate this, because it is so important: Do not share your private keys with anyone! You are your own bank, and you should not leave these keys anywhere that someone could find them or use them. This rule should also apply to friends and family in most cases. If you don’t trust your half-brother to refrain from helping himself to some cash out of the wallet that you left on the kitchen table, then you certainly shouldn’t trust him with knowing what your private keys are, or where to find them. There have been many heartbreaking stories about relationships that went sour, where one partner disappeared into the night with the other partner’s private keys and money.

Incidentally, private keys are not physical keys. They're just very long and complex passwords. Public keys are similar, although you'll soon begin to think of public keys as more like an account number than a password. Private keys for many cryptocurrencies are more than forty or fifty digits long, so they would be almost impossible to guess, even by a supercomputer making thousands or millions of guesses per second. We'll go into a lot more detail about private keys and public keys later in this book. Incidentally, we'll often interchange the terms public key and public address, and make it sound like they are the same thing. Technically, they're slightly different, even though they mean the same thing. Again, we'll discuss that later in the book.

BITCOIN

Bitcoin was the first major form of cryptocurrency and continues to dominate the market. It may always be the main cryptocurrency in the future, but it’s also possible that it could someday lose its position at the top of the charts to a younger and better cryptocurrency. For now though, think of it as the “elephant in the room.” Even if you have no intention of ever buying or using any Bitcoin, it’s impossible to ignore if you want to understand cryptocurrencies properly.

Bitcoin was "designed" by an anonymous person (or people) under the name of Satoshi Nakamoto. In 2008, Nakamoto published a "white paper" (an academic article) that explained the possible structuring of a global virtual currency. The currency would be decentralized, meaning that it would not be controlled by any one country, institution, or person, and it would operate independently of any central bank. It would operate through a peer-to-peer network system, meaning that it would simultaneously exist in computers all over the world. The peer-to-peer network ensures security from hackers, thieves or terrorists wishing to steal, move, or destroy currency.

Cryptography is a field relating to writing and solving secure codes. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The Bitcoin network (and all subsequent cryptocurrencies) rely on complex cryptography to ensure that they are secure. This helps to ensure that users do not face the risk of theft as long as they keep their “password” (their private key) secure.

BLOCKCHAIN

Let’s try to explain blockchain in one paragraph. First of all, we should clarify that having a complete professional understanding of blockchain technology is not critical for gaining a basic understanding of how various cryptoassets work. However, it’s helpful to acquire a general background as cryptocurrencies are almost always built on a blockchain framework.

A blockchain is a public database. A blockchain acts as a ledger which contains all the transaction data from anyone who uses or has ever used the cryptocurrency in question. Each “block” in a blockchain is made up of data and computer code. Think of a block as one link in a chain, although in the case of a blockchain, it’s a digital chain instead of one that is made out of metal. Every transaction that ever takes place anywhere in the world gets added to a new "block" in the digital chain. Every few seconds or minutes, a new block is created on the chain, in order to keep storing additional transactions. These blocks (the entire chain of them) are stored permanently by tens of thousands of computers around the world, so there will always be a historical record of every transaction. Some blockchains (such as the one used by Bitcoin) already have millions of blocks, but that’s ok. Blockchains are usually designed to allow an infinite number of blocks, so they can exist and grow forever. There is no effective way to hide, edit, or destroy these records, because they are on too many different computers, in too many countries, belonging to many different individuals. Even a nuclear conflict or an asteroid impact probably couldn’t wipe out a widely distributed blockchain such as Bitcoin’s, unless it destroyed basically every living person on Earth.

If you’ve heard of Bitcoin or other cryptocurrencies, then it’s almost inevitable that you’ve already heard the term "blockchain." Blockchain technology was in the news a lot in 2016 and 2017 as the “next big thing” in computing technology and corporate efficiency. Understanding exactly how blockchain technology works is not critical if you want to invest in (or use) cryptocurrencies. An analogy would be that you can learn to drive a car without understanding the compression/decompression cycles in a four-stroke engine. However, understanding the very basics of what blockchain means will help you to assess and evaluate various types of cryptoasset projects. We will give you a very basic overview of blockchain technology. However, if you’re serious about investing in cryptoassets, we highly encourage you to do further research. You can find some starter links on our website.

What is Blockchain Technology?

Once again, a blockchain is essentially a giant database, or a collection of information. However, it is a specialized type of database, because the information within the blockchain is immutable, which means that it can’t be altered. In some cases, immutability would be a major disadvantage for a database. For most databases, it is a huge advantage to be able to edit information stored in the database. However, blockchains are intended to target a specific need, namely that users can be 100% certain that the information stored in the blockchain is the correct original information. It is impossible for anyone to edit information that has already been stored on a blockchain. All users are able to trust the contents of the blockchain, even if they don’t trust (or know the exact identity of) people that they’re transacting with.

Think of a blockchain as a series of filing cabinets in a long row in a giant warehouse. Incidentally, these filing cabinets are made of transparent materials, so anybody can look inside them and see the contents (even though they are “locked” so nobody can add or remove files). We’ll look at the Bitcoin blockchain to explain the specifications of this row of filing cabinets. Different blockchains for different cryptocurrencies can have slightly different specifications, such as the amount of time that is allowed to elapse before a new block is created, or the size of each block. Incidentally, blocks on some blockchains don’t necessarily always have to be the same size, and blocks don’t necessarily have to be “full” before they are added to the blockchain. Each different type of blockchain might have its own rules in those respects.

Let’s get back to our Bitcoin analogy. Looking at our row of filing cabinets, the very first filing cabinet was delivered to the warehouse on January 9th, 2009. This was when the first Bitcoin block was mined. The original Bitcoin developers decided that each new block should be mined (created) approximately ten minutes apart. However, mining a block on a blockchain involves having computers solve mathematical equations of varying difficulty. These blocks aren’t "released" or created exactly every ten minutes. Because there is some uncertainty in solving the mining equations, computers might take slightly longer, or slightly less time, before they correctly solve the equations. As such, the ten minute block time may be thought of as a "long term average.”

Similarly, let’s go back to our assumption that we’re getting filing cabinets delivered to our warehouse. We tell the delivery company that we would like them to bring us a new filing cabinet every ten minutes, but since a large fleet of drivers is involved in this operation, the exact amount of time between new filing cabinet deliveries varies slightly. Some delivery drivers will drive more quickly than others. Some will hit red lights. Occasionally, a truck will break down and there's a long delay before our next filing cabinet arrives. But on average, every ten minutes, a new filing cabinet arrives and gets added to the end of our row of filing cabinets.

You may wonder what's in our filing cabinets. Well, we're going to store transactions in them. Also, don't forget that our filing cabinets are made of a transparent material, so anyone can see what's inside of them. Let's pretend that every time a Bitcoin transaction occurs, the details are recorded on a piece of paper, and that piece of paper ends up getting stored in the most recent filing cabinet in our warehouse. A Bitcoin transaction, which occurs when one user sends some Bitcoin to another user, is a "public" transaction. Everyone in the world can see the details of the transaction, if you know where to look on the internet. There are websites called "blockchain explorers" which allow you to look into blocks (our filing cabinets) and to examine every transaction. The Bitcoin blockchain is a public ledger, so anyone with internet access can examine the information contained in any block. Information that is visible includes the Bitcoin address (wallet) that sends a transaction, the address (wallet) that receives that same transaction, and the amount of Bitcoin being transferred.

However, even though we can see the addresses (wallets) that send and receive the Bitcoin, we don't necessarily know exactly who owns those wallets. The inherent privacy of a Bitcoin wallet address comes from the lack of personal identification details associated with the wallets. You can't look into a wallet and see information that identifies the real-world identity of the owner. A real-world wallet might contain a piece of paper that says, "This wallet belongs to Jeffrey Simpson of 1234 Main Street, Topeka, Kansas." Your digital wallet contains no such identifiers. Nobody will ever know that you "own" a specific Bitcoin wallet (address) unless you tell them that it's yours.

Despite the lack of personal information, it is sometimes possible to identify who owns an address/wallet. If you're getting a pizza delivered, and the pizza guy accepts Bitcoin, then when you send him the Bitcoin for your pizza, he now knows your Bitcoin wallet address, because he can use a blockchain explorer to see what address the Bitcoin came from. This means that he can see how much Bitcoin is remaining in your wallet. So even though the wallet address by itself doesn't reveal the identity of the person who owns it, it's possible to figure out who owns a particular wallet if you can connect certain transactions to real-world identities.

Maybe the pizza delivery guy is a disreputable character, and he has some friends who are criminals looking for rich targets. The pizza guy tells his friends, "Hey, I just delivered a pizza to a guy at 1234 Main Street who has a Bitcoin wallet worth $200,000." This risk, which comes with having a public blockchain, is of concern to a lot of people. Think of it as a necessary evil. There are both advantages and disadvantages to the fact that transaction data is visible to anyone who knows where to look. For example, if you're a business transacting in Bitcoin, and one of your competitors is spying on you, they can probably figure out your wallet address or addresses with some quick and simple corporate espionage. From there, they could see your financial balance, and they could see where you're making payments to other Bitcoin addresses. Maybe some of those payments are going to wallets that are known to belong to certain suppliers, and this is useful information for your competitor. Although this sort of scenario sounds far-fetched, there are currently several companies around the world that perform blockchain analysis. They've managed to trace transactions to and from individuals, throughout the blockchain, and there is already strong speculation that nearly every Bitcoin address owner in the world has been identified by these companies. Who can use this information? Well, for starters, governments would be very interested in this information, to ensure that people aren't using cryptocurrencies to evade taxes.

Let's get back to blockchain and to our row of filing cabinets. Every filing cabinet (block in the blockchain) is able to store some records of Bitcoin transactions. In fact, some blockchains can store much more than transaction data. Some blockchains might be designed to store real estate deeds, or peoples' last will and testaments, or dental records. Blockchains could store music or video data, in order to establish copyright. And does a block have to be full before it is added to the blockchain? No, it doesn't. It's possible to add a partly-full block to the blockchain, or even an empty block. Many of the earliest Bitcoin blocks were empty blocks due to the lack of users.

It's important to understand that a new transaction or data can ONLY be stored in the most recent block or filing cabinet. You can't add it to a previous block, even if a previous block was empty and had lots of room. We already mentioned that a blockchain is designed to be immutable, and information stored on/in the chain cannot be edited. In terms of the blockchain, this rule is impossible to break. A new transaction can ONLY be included in the most recent block. The computer coding that creates the blockchain was written in such a way that it is completely impossible to alter a previous block. All you can do is look at that older block and see what it contains. So let's pretend that when a new filing cabinet is added to the end of our row, it gets "locked" in such a way that we can still see information inside it (because it is transparent), but we can't remove or change that information anymore.

Over time, our row of filing cabinets is getting longer, as the blockchain grows longer. And transactions start happening more frequently, because more people around the world are using Bitcoin. Our filing cabinets aren't huge. Each one is only capable of holding so many transactions. If we try to put too many pieces of paper in any individual filing cabinet, we won't be able to fit any more, because that particular cabinet is too full. The blocks on the Bitcoin blockchain are the same way. Let's pretend that each of our filing cabinets is large enough to hold a little over two thousand pieces of paper, or a little over two thousand transactions. Each block on the current Bitcoin blockchain can also hold slightly more than two thousand transactions. If a new block is mined roughly every ten minutes, that means there are an average of around 600 seconds between blocks. If people around the world are making more than a few Bitcoin transactions per second, the blocks are going to be pretty full. In fact, sometimes, people are making too many transactions to fit in one block. In these cases, it is common for some of the transactions to have to wait for the next block. The same thing is happening in our warehouse. If there are too many pieces of paper (transactions) to fit into the most recent filing cabinet, we have to wait for the next empty filing cabinet to be delivered. We can't store transactions in older filing cabinets, even if they weren't filled, because of the rule that says we can't change/edit the contents of older filing cabinets. Remember again that our blockchain is "immutable" or unchangeable.

Let's talk some more about the immutability of the blockchain. Immutability allows for every coin ever made/mined to be traced from its original to present holder. If a specific Bitcoin was mined in 2009, and was part of 150 transactions since it was created, then every single one of those 150 transactions can be seen in various parts of the blockchain. Just like every American dollar bill has a serial number on it, each Bitcoin (and fraction of a Bitcoin) is unique. Of course, that's where the similarity between Bitcoin and paper money ends, because there is no collection of records that traces the path of every individual dollar bill from the time it was printed to its present holder.

Incidentally, at this point, it’s probably important to clarify that Bitcoins don’t have to be traded in whole units. It’s possible to buy half of a Bitcoin, or a quarter of a Bitcoin. In fact, it’s possible to buy 0.00734825 Bitcoins, or any other fraction of a Bitcoin. Although a US dollar can be traded in portions of up to two decimal places or one hundredth of a dollar (one cent), a Bitcoin can be traded in portions of up to eight decimal places. This amount, which represents one hundred millionth of a Bitcoin, is referred to as a "satoshi." So 0.00734825 BTC is equivalent to 734,825 satoshis. Some people think that they can’t afford to invest in Bitcoin, because a single Bitcoin is far too expensive for them. However, because you can buy fractions of a Bitcoin (or almost any other cryptocurrency), it’s still easy to invest an amount like $50 or $100 into Bitcoin. Incidentally, even for fractions of a Bitcoin, some people use the plural form of the word, and others use the singular. So some people might say, “I have 0.3 Bitcoin,” and other might say, “I have 0.3 Bitcoins.”

You’re probably wondering what kind of security we have in our warehouse? What’s protecting our row of filing cabinets, to ensure that nobody can steal them, or open them and change information? Cryptography and decentralization deal with these concerns. First of all, our warehouse is not the only place in the world that has all the information stored in our filing cabinets. Let’s pretend that every time we add a new filing cabinet, and fill it with transactions, all of our partners around the world ask for copies of the information in the cabinets, and they create their own duplicate versions. So there are "copies" of all of the filing cabinets in our warehouse being created in locations all around the world. The same thing happens with blockchain, although all the copies of the blockchain are just stored as data files on computers around the world. Anyone can download and store a copy of the blockchain. This ensures that thousands of copies of the blockchain exist all over the world. The blockchain cannot be destroyed unless all of those copies all over the world were to be destroyed. If a fire burned down our warehouse, the information would still be safe as there are many backup locations around the world. If someone's computer crashed and the blockchain was wiped off their hard drive, the blockchain would remain intact because there are thousands of other copies on other computers. You'd almost have to destroy the entire planet to get rid of every copy.

How do we know with absolute certainty that the blocks in our blockchain contain the same information as when they were first written? How do we know that information in the blocks hasn't been changed? We'll keep this simple for now, and say that basically, the integrity of the information stored in the blockchain may be verified by comparing records in different computers. If you're ok with knowing this, you don't have to understand exactly how it works.

In more advanced technological terms, cryptography works to ensure the integrity of the blockchain. Every time a new block is created, a cryptographic hash function is applied to it producing a "hash value". This value can be seen as a completely unique alphanumeric string summarizing the contents of the block, which partially acts as a password and verification technique. The string of characters in the hash value is very complex, and is derived based on the given hash function and the contents of the block. If you were to be able to change one number or letter or byte that is contained in a block, the hash value for that block would change completely. We'll talk more about this later. For now, you can assume that you can create a hash value from any collection of information, and that each hash value is completely unique. Also, it is essentially impossible for two different records, files, or documents to have the same hash value, because the hash values are such complex numbers.

Having a hash associated with each block means that the validity of the block can be confirmed by anyone. There are lots of free websites available that allow you to enter a block of text or other information, and the website calculates the hash value of that data for you. If anyone else applies the hash function to the exact same collection of data, they will get exactly the same result. We could submit a file or block containing the complete works of the Encyclopedia Brittanica to such a website, and calculate the hash value for it. If you did the same thing, you would get exactly the same hash value, and then you'd know that your information is an exact duplicate of mine. However, if even one tiny part of the information changed, such as there was an extra space in one sentence somewhere, the hash value would be completely different, and you'd know that you don't have an exact duplicate of my information.

As each block is added to the blockchain, the hash value of the contents is also recorded on the chain. That way, people around the world can check the hash value of their version of each block, and make sure that the hash value is the same as for everyone else around the world. If it wasn't the same, you'd know that the content of that block on your chain is not the same as all the others, and therefore, your version of the blockchain is not correct. Don't worry, the computer code does this process automatically, so you don't have to check every block as it gets added to your copy of the blockchain.

It's important to remember that even a tiny change in the contents of a block results in a completely different hash for that block. It's even more important to understand that each new block "builds" upon the previous block, because the hash from the previous block gets included in the information going into the current block. This is critical in the concept of creating a blockchain. When a hash is calculated for a new block, that new hash is partially dependent on the hash of the previous block, since the hash value of the previous block is included with the information in the new block. This complex interaction of the contents of each block ensures that the contents of previous blocks cannot be changed. If someone tried to change an old block, the hash value for that old block would be incorrect, and therefore the hash values for all additional blocks in that copy of the blockchain would also be incorrect. That copy of the blockchain would then be known to be invalid because information was changed.

Hopefully this explanation has given you a basic understanding of the blockchain. It's a series of blocks being built up over time. Every block, unless it happens to be an empty block, will include some sort of information (or in the case of cryptocurrencies, transactional data for that cryptocurrency) which can never be changed once these blocks are created or finalized. The information in every block, going all the way back to the first block that was made or mined when the blockchain was created, can be viewed by the public.

Incidentally, even an "empty" block is not empty. It may not contain any transaction data, but it would still contain the hash value of the previous block, to maintain the integrity and continuity of the blockchain.

In review, a cryptocurrency blockchain is a digitized, decentralized, public ledger of all transactions for a specific cryptocurrency. Depending on the cryptocurrency, some aspects of the blockchain may differ, but its general functions remains the same. For example, blocks on the Litecoin blockchain are mined approximately every 2.5 minutes, blocks on the Monero blockchain are mined approximately every 2 minutes, and blocks on the Ethereum blockchain are mined approximately every 14 seconds. In terms of size, Bitcoin and Litecoin have fixed block sizes, but Monero has a flexible block size, so every block can be a different size. Monero's blocks differ further as they have privacy features preventing the public from being able to see the size and the senders/receivers associated with a given transaction, but that's a story for a different part of this book. The important point is that every cryptocurrency's blockchain can have significantly different characteristics.

The focus of this chapter has been upon cryptocurrencies or other types of cryptoassets which create new blocks by "mining" (solving extremely complex mathematical equations). Some blockchains take different approaches than mining, such as having systems whereby new blocks are released on a specific time-based schedule, without miners needing to perform any complex calculations to release them. The inner workings of blockchains differ from project to project. There are lots of other things which can vary from project to project. In fact, a few cryptoassets don't even use sequential blockchains to store data, and instead rely on things like Directed Acyclic Graphs (DAG's). Iota and Nano are two good examples of cryptos that use this structure. A DAG is sort of like a three-dimensional and non-sequential blockchain, but not really. Let's just focus on blockchains for now.

CRYPTOCURRENCIES VS. CRYPTOASSETS

Let's try to use more accurate terminology right from the start. We may be swimming against the stream by attempting to correct terminology that is already entrenched around the globe, but it can't hurt to try. Rather than describing all digital cryptology-related and blockchain-related projects as cryptocurrencies, let's call them cryptoassets. That's a broad, generic term that can encompass all such projects, because not everything that is commonly referred to as a cryptocurrency is intended to be used as a currency.

Within the broad category of cryptoassets, we will focus on three main sub-categories: cryptocurrencies, platforms, and utility projects. There are certainly several other sub-categories, although we'll stick with these basic categories for now. A lot of people tend to use the slang term "crypto" to refer to all cryptography-related and blockchain-related projects. Since cryptoasset can be shortened to crypto, we think this is a good word to use. However, remember that a lot of people will continue to use the term "cryptocurrency" to refer to all types of cryptoassets, including those projects that don't function specifically as digital currencies. That's fine, we won't judge anyone for this semantic error.

Cryptocurrencies

Pure cryptocurrencies are digital blockchain-based projects, whose basic trading units (usually called coins) are solely intended to be used as a form of online currency. They aren't used for smart contracts, they aren't utility tokens, and they aren't platforms. They're intended to function specifically as digital money, as an alternative to traditional fiat (national) currencies. Bitcoin is the most well-known of the digital cryptocurrencies and accounts for more than half of the total overall market capitalization of all of the thousands of different cryptoasset projects combined (as of early 2020). Other examples of pure cryptocurrencies include Litecoin, Vertcoin, Monero, Dash, Ripple, all the various members of the Bitcoin family, and more. If you're trying to think of a simple way to describe pure cryptocurrencies, think of them as being "just" digital money, and nothing else.

Platforms

Crypto platforms are digital and blockchain-based. These projects invariably allow various types of "smart contracts" and other blockchain-based utility projects to be built upon their framework. Crypto platforms aren't exactly a computer language, and they aren't exactly like a computer, but a good analogy is that they're very similar to being a blockchain-based "virtual computer." Developers are able to use them as the framework or backbone upon which they are able to "write" or build/code other projects, without having to start their projects from scratch. Examples of crypto platforms include Ethereum, Ark, Neo, Lisk, and more. Many of the utility projects that we will discuss shortly are built upon these platforms. Each of these platforms has its own coin or platform token which is used as a unit of trade within the platform. These tokens trade on crypto exchanges in the same way that pure cryptocurrencies are traded. However, the purpose of the tokens varies depending on the platform. Sometimes it isn't even necessary to own any tokens to use those platforms. We'll get more into that later.

Utility Projects

A lot of blockchain projects are built upon existing platforms, rather than being built from scratch. Building a project on top of an existing platform (such as the Ethereum platform or the Neo platform) drastically reduces development time and costs. Imagine this as an analogy: You want to raise funds for a small project. In order to do this, you create a website through which you describe your project, advertise it, and collect money from funders. You have two options: First, you could build your website from scratch, you could talk to payment processors about integrating financial systems into the site to collect money, and you could spend money on advertising and promotion by talking to Google and Facebook and other giants. Of course, these are a lot of separate steps, each of which requires a lot of research and learning. These steps additionally rely on a lot of outside experts, some of which eat up some of the funds that you're trying to raise. However, as an alternative to the DIY approach, you could use an existing platform (such as Kickstarter), through which you can easily advertise and fund your project. In the world of cryptoassets, platforms such as Ethereum and Ark and Lisk and Neo give you a starting foundation. You can build your crypto project upon the framework of an existing project much more quickly than building it from scratch.

It's important to understand what a Dapp is. A Decentralized Application (Dapp) is any software or application that, instead of being contained on a single central computer(s), runs its backend code on a decentralized peer-to-peer network. The use of a peer-to-peer network eliminates a point-of-failure risk. Even if some “peers” in the network fail, many other peers are still able to provide the code necessary for the application to keep functioning. Think of all of these utility projects that we just talked about as being types of Dapps, running code that depends on a crypto platform.

Privacy

One of the best parts of blockchain technology is that it is a permanent, immutable, public ledger. The information associated with all Bitcoin transactions throughout history is, and always will be, visible on the public blockchain available to anyone. The same applies for almost every other cryptoasset. This is important for accounting, auditing, and verification. However, this feature is considered to be a drawback for some people.

When we say "public," it is important to note that Bitcoin accounts (addresses) are just numbers, and don’t have the owner’s personal identification information stored in them. Unless you know who owns the keys to a specific wallet address, you can’t easily tell who owns the assets in that address. In this sense, there is some inherent privacy to Bitcoin. However, remember that all transaction histories can be traced throughout the entire blockchain. If you interact with someone who sends you cryptoassets, you’ll be able to see their wallet address, and they’ll be able to see yours. This means that you can also see the balance in their wallet, and you can trace any other transactions that they’ve made in the past (and vice versa).

Blockchain analysis companies have done a very good job of analyzing the entire global public ledger for many cryptocurrencies, and have managed to tie a lot of real-world identities to various addresses. The government knows this. Don't ever assume that your cryptocurrency transactions are completely private.

Several coins do exist which have certain technological features that partially or completely hide the information associated with all transactions, with varying degrees of success. These cryptos are commonly referred to as "Privacy Coins." Monero and Z-Cash are two great examples. You probably shouldn't assume that any transaction made with these coins will remain completely private in the future, simply because someone may someday figure out a way to decrypt and expose the blockchain records for those projects. However, this may be irrelevant to many people, unless you're a criminal and are trying to hide your funds. For most of these semi-private coins, partial privacy is adequate for almost all users. Most people are not engaged in nefarious activities. Instead, they just want some basic privacy, such as not wanting the pizza delivery person to know how much money is stored in their wallet. We think this is a legitimate concern. We'll go into more detail about this elsewhere in this book.

EXCHANGES

The crypto markets are still in a relatively early stage, making it difficult to buy and sell cryptocurrencies and related assets. Beyond the obvious technological barriers, there are a lot of scams, which makes it increasingly risky to invest. This chapter will provide some general guidelines about investing your money safely. We recommend that you do not just jump in and buy any cryptocurrencies until you become thoroughly familiar with the information contained in this book.

Warnings and Scams

Before educating you about legitimate ways of buying assets on cryptoasset exchanges, we should warn you about ways NOT to buy crypto: Don’t buy crypto from eBay, don’t buy crypto from CraigsList, don’t buy crypto from people advertising in newspapers or on posters. In rare cases, you may find legitimate sellers on these sites, but the majority of the deals you will find are either highly overpriced or outright scams. We’ve seen ads for people who were selling "1 MIOTA" on eBay for over $100 USD, when the market trading price on Binance was only forty cents for a MIOTA. In-person meetings, even in public venues such as libraries and food courts, can lead to a physical safety risk, because malicious persons can figure out your real-world identity for later targeting. Cryptocurrency fan meet-ups and websites such as "Local Bitcoins" have historically provided some legitimate functionality in helping create a market for cryptocurrencies, but it is highly recommended at the present time that anyone who wants to invest should restrict their purchases to legitimate online cryptoasset exchanges. To be honest, even some of the major crypto exchanges have questionable pedigrees.

Online Exchanges

As with many other types of businesses, there are reputable cryptoasset exchanges, and there are exchanges which often face technological issues (or which have terrible customer support for when things go wrong). In addition to researching the cryptoassets that you want to buy, it is important to research the exchanges that you will use to buy them. Exchanges can be located almost anywhere in the world, and there are some decentralized exchanges that aren't really based in any one specific country. Unlikely traditional stock exchanges, which have regular set trading hours, all crypto exchanges remain open 24 hours per day. Crypto never sleeps.

Broadly speaking, it is useful to start by breaking down online exchanges into two groups: fiat gateway exchanges and pure crypto trading exchanges. A gateway exchange allows you to deposit traditional fiat money into the exchange. Some of the gateway exchanges allow only the deposit of US dollars or Euros. Other gateway exchanges allow a wide variety of fiat currencies to fund future purchases of cryptos. You'll have to do some research into which exchanges are most suitable for use as a gateway fiat exchange for the country that you live in. Coinbase is one of the most well-known gateway exchanges. It is based in the United States, but accepts currencies from quite a few countries around the world. Depending on your location, you may be allowed to deposit funds by wire transfer, credit card, bank card, or other means. The length of time that it takes for these various funding methods to be processed will vary significantly, as do the fees associated with each type of funding method.

Throughout most of 2017, Coinbase only offered trading in three types of cryptoassets: Bitcoin, Ethereum, and Litecoin. If you wanted to invest in a different type of cryptocurrency, you needed to get an account on a second exchange. A few years later, Coinbase now offers trading in several additional cryptos, but the selection is still quite limited.

Let's pretend that you want to buy a certain type of cryptocurrency, a fictitious crypto called ExampleCoin which is only traded on a single exchange, Bittrex. Bittrex is another exchange based in the United States, however, when it started out, it was not a fiat gateway exchange. Bittrex now allows fiat transactions, but for the sake of this example, let's pretend that it is still 2017 and Bittrex doesn't touch fiat. At the time, it was not possible to add traditional fiat funds to Bittrex, or to withdraw fiat funds to your bank account. The only thing that Bittrex allowed you to do was to trade between different types of cryptoassets.

Until recently, Bittrex was a pure crypto trading exchange and despite this limitation, Bittrex was quite useful. It offered trading for hundreds of cryptoassets. There are still many examples of pure crypto exchanges around the world that don't touch fiat, usually because regulatory oversight becomes much more stringent when fiat money is involved.

Right now, Bitcoin is the de facto standard within the cryptocurrency world, so most of the cryptos traded on Bittrex (and all similar exchanges) are traded in terms of Bitcoin value rather than dollar value. If a crypto can be traded on an exchange for another crypto, it is referred to as a trading pair. As such, if you can buy and sell ExampleCoin in terms of Bitcoin, then the exchange is said to have a ExampleCoin/Bitcoin trading pair. The majority of cryptocurrencies in the world are set up in trading pairs with Bitcoin. Less frequently, other trading pairs are available on some exchanges, although this type of diversity is growing. Some exchanges allow less well-known cryptos to be traded in terms of Ethereum (ETH) or Litecoin (LTC) or Tether (USDT). As the markets continue to mature, the public will see more and more trading pairs added to various exchanges, which will be a good thing. Flexibility is useful.

Let's assume that you want to buy ExampleCoin. At this point, let's assume that you've deposited fiat funds to your gateway exchange such as Coinbase. The next step is to buy some Bitcoin, and transfer that Bitcoin from your gateway exchange to the pure crypto trading exchange. In this case, you would buy some Bitcoin on Coinbase, and then send your Bitcoin from your Coinbase BTC wallet to your Bittrex BTC wallet. The terms may vary from exchange to exchange. For example, your exchange may say that you are "withdrawing" Bitcoin rather than "sending" Bitcoin. It's important to remember that in order to initiate a transaction, you always do it from the "sending" exchange. In other words, in this example, to transfer Bitcoin from Coinbase to Bittrex, you make the transaction happen by sending it from Coinbase, not by requesting it on Bittrex.

It is extremely important to note that every wallet on every exchange is designed ONLY to hold one specific type of crypto. If you have an account on Coinbase, and you own both Bitcoin and Litecoin, they are NOT stored in the same wallet. You'll have a Bitcoin wallet with one address, and a Litecoin wallet with a different address. This is extremely important to note as it IS possible to send some types of cryptocurrencies to wallets for different cryptos. If you make this mistake, you will lose your crypto, as there is no way to reverse the transaction and no way to recover it! It is therefore important to be very careful when sending a specific type of cryptocurrency to a different wallet or address (the terms are synonymous). You need to be absolutely certain that you're sending it to the proper type of wallet. Never send Litecoin to a Bitcoin wallet, or Bitcoin to an Ethereum wallet, or anything like that. If you do, you'll end up with nothing.

You can easily have multiple wallets for a specific type of crypto. There is no cost to setting up wallets (except for a few rare cryptos that require a minimum balance in your wallet). It is no problem for you to have three Bitcoin wallets on three different exchanges, plus four paper Bitcoin wallets, plus a hardware wallet. As long as you can keep track of your private keys for each wallet, you can have as many as you want. Also, once you have an account on a cryptocurrency exchange, you probably have access to wallets for every type of crypto that the exchange can trade. So for example, you will have a Bitcoin wallet on Bittrex, and a separate Ethereum wallet on Bittrex, and a separate Litecoin wallet on Bittrex, and so on. Finally, on many exchanges, you can have multiple wallets set up for a single type of crypto. So for example, some exchanges may allow you to have seven separate Bitcoin wallets, if that's what you want. We'll go into a lot more detail about wallets soon.

Once you've successfully moved your Bitcoin to the second exchange, you can use that Bitcoin to buy your ExampleCoin. The first couple of times that you move Bitcoin from your fiat gateway exchange to a different exchange, you'll be very nervous. You'll wonder why the transaction isn't happening immediately. Bitcoin is especially slow to transfer, so it may even be a few hours before your transaction is processed. This is a weakness that affects some cryptocurrencies more than others.

You know that Bitcoin has an average block mining time of about ten minutes, so you're probably wondering why a transaction could take longer than ten minutes. One possibility is that your transaction may not get included in the next block to get mined, especially if there are a large number of global transactions occurring simultaneously. Another possibility is that the miners, by random chance, might take much longer than ten minutes to find the next block. We've occasionally seen blocks that took more than sixty minutes to be mined (and we've also seen blocks that only took a few seconds).

Moreover, with respect to exchanges, once your transaction does get into a block, that block still requires multiple "confirmations." This means that the exchange doesn't necessarily believe that your Bitcoin transaction is legitimate until it is buried a few layers deep into the blockchain. Each time a new block is mined, it acts as another confirmation or layer being piled on top of all older blocks, including the block with your specific transaction. Every new block that gets added to a blockchain enhances the legitimacy and security of all older blocks. This is because as more blocks get added, the possibility of a temporary “accidental fork” diminishes, which makes the exchange more confident that your transaction was legitimate. The number of transaction confirmations required for various cryptos will vary from exchange to exchange, and furthermore, will depend upon the particular crypto. Most exchanges require five or six confirmations before they’ll view your transaction as legitimate. Let’s say that you move some Bitcoin and it gets included in the very next block to be mined. Despite that, you may have to wait for five or six more blocks to be mined (at an average of about ten minutes apiece) before your assets are "approved" (show up in your trading account) on your second exchange. On a positive note, once your transaction has appeared in a block, you’ll usually get a notice on your destination exchange to reassure you that the transaction is in progress. In the case of Bittrex, it may list your incoming Bitcoins in a "pending deposits" column.

Different exchanges allow different types of orders, including "market" orders and "limit" orders. A “market buy” order allows you to buy Bitcoin immediately at the lowest price that any of the sellers on the exchange is willing to accept for their Bitcoin. A “market sell” order allows you to sell immediately at the highest price that any of the buyers on the exchange are willing to pay to obtain Bitcoin. Market orders, regardless of whether they are buys or sells, will always get filled immediately (as long as there are any opposing sell or buy orders on the exchange). The drawback is that the price at which your market order gets filled may not be quite what you hoped. Market orders are good if you’re in a hurry, because they are filled almost instantly, although there may be a slight discount to the “best price” that you might have been able to get otherwise, had you been more patient.

Limit orders are good for patient traders. A limit order is more restrictive. Limit buy orders require a trader to specify a “limit,” or maximum amount they are willing to pay to make a purchase. Limit sell orders require a trader to specify a limit for the lowest price at which they are willing to sell their coins or securities. Your limit orders will never be executed if no opposing buyer/seller is willing to meet your terms. For example, let's pretend that we've just placed a limit order to buy a security at $100 per coin. Our order is referred to as a "bid" order. It's like an auction, because we're willing to pay up to $100 per coin (we also specify exactly how many coins we're willing to buy at that price). At the moment, let's assume that most of the sellers using the exchange have placed orders that show they aren't willing to sell their coins for less than $104 (they are using limit sell orders, also referred to as "asks"). However, there is one seller who is willing to sell his coins for $102 (let's call this person Brad). In this example, nobody has placed any "market" orders, and all of the buyers and sellers on the order book have placed "limit" orders. Therefore, there is a gap between the highest outstanding bid (our bid at $100) and the lowest ask (Brad's ask at $102), so for the time being, no orders can be matched and no trades will be executed. Remember that our order won't be filled until someone finally comes along who is willing to sell their coins for $100 each (our bid price).

If someone else (Charlie) came in and placed an order that showed that he was willing to buy coins at $101, then Charlie's order wouldn't get filled either. That's because the lowest "ask" or selling price is still $102, and Charlie is only willing to pay $101. However, if someone else comes along who is willing to sell for $101 or lower, then Charlie's order will get filled.

If someone had come in and said that that they were willing to sell for $100, then Charlie's order would still be filled before ours, even though we placed our order first. This is because the exchange makes sure that people always get the best price possible. A hierarchy exists for the buy and sell orders based upon first-come, first-serve at every unique price level, but when the price levels vary, then a higher bid or lower ask gets priority. Charlie's bid of $101 is “better” for a seller than our bid of $100, so his order is prioritized. If we had both bid the same amount, then our order (the earliest) would have been prioritized.

This has been a very quick overview of the difference between market and limit orders, and you should do additional research before starting to do any active trading. In fact, we urge you to finish reading this entire book (and make sure you understand it completely) before you make any purchase decisions that might put your hard-earned money at risk. We also highly recommend that you buy a book that teaches the basics of trading on conventional stock exchanges, because the processes are almost exactly the same.

Once you’ve bought the coins that you wanted (ExampleCoin), you have to make a decision as to what to do with them. Should you leave them on the exchange, or move them to a personal wallet? Leaving your coins on an exchange is simple, and exchanges are generally secure, but there is still a significant risk. Crypto exchanges are very big targets for hackers, due to the enormous sums of money involved. There have been several recent notable examples of exchanges being hacked, resulting in users losing the coins that the exchanges were holding for them. You can read more about this in the Notable Hacks chapter. Remember, when your crypto is on an exchange, the exchange holds and controls the private keys to the wallets containing your crypto. Unless you have your crypto in a private wallet of your own, not on an exchange, you aren’t in control of your own assets. This is a security risk. There’s a famous phrase to describe this: “Not your keys, not your coins.”

Every wallet, whether it’s on an exchange, on a physical device that you own, in an online wallet, or in a paper wallet, will require a password to open it. This password is called a "private key." When you leave your coins on an exchange, you are trusting the exchange to take care of your private keys for you. This involves a risk. Although the risk may not be huge, especially for the more reputable exchanges, it is still a non-zero risk. If you don't control your private keys, or if anyone has access to your private keys, then you're at risk. Risk-averse investors should almost always move their coins into a personal wallet of some type. This is especially true if you're holding what, to you, is a significant amount of crypto. The only exception to this rule might be if you meet all three of the following conditions: (1) You're using a very reputable exchange, such as Coinbase; (2) You are dealing with small dollar amounts, so your financial stability wouldn't be at risk if you somehow lost your investment; and (3) Your technology comfort level with using wallets is low, and you're nervous that you'll screw something up if you try to create and use an off-exchange wallet. Otherwise, if you feel comfortable with the technology, we always recommend moving your assets off the exchange.

Unfortunately, risks exist in moving your coins to a personal wallet. You can find more information in the Wallets chapter, but some of the risks involve user error, sending crypto to the wrong type of wallet, losing your private key, getting hacked, and more. If you are moving coins from an exchange to a wallet of your own, we suggest that you "practice" first. Set up your wallet, and when you make your first transfer, only send a very small amount of your cryptocurrency to the wallet, to make sure that the wallet works. If your transaction wasn't successful, you'll be glad that you didn't send everything you own, and you'll have the opportunity to do some trouble-shooting.

There's a chance that certain cryptocurrency exchanges that you want to use are based in countries other than the one you live in. While you should always use caution when researching exchanges, don't assume that an exchange from another country is useless to you. The authors of this book are Canadians, based in Canada, but have used an American exchange (for funding) and have traded cryptocurrencies on exchanges based in more than half a dozen other countries.

Cryptocurrencies know no international boundaries. You can send cryptocurrencies to any part of the globe where there is an internet connection. Unfortunately, some exchanges impose user restrictions based upon nationality. For example, the Bitfinex exchange does not allow customers from the United States, due to the strict regulations that American authorities have put into place. Within the United States, residents of certain states are prohibited from trading on certain US-based exchanges. Depending on where you live, cryptocurrencies can be classified by your government under different asset classes (currency, commodity, property, etc.) and the taxation status for buying and selling may also vary. You should always do research, before buying and selling, so you understand the tax laws that may apply in your country. This may affect the way that you plan your trading activities and record-keeping. You should always keep an exact record of every buy or sell transaction involving any type of cryptocurrency, in case the tax authorities in your country request documentation of your trading activities. We'll talk more about this in the chapter about taxes.

In terms of assessing which exchanges are the safest to use, there are several things that you can consider. What is the reputation of the exchange on social media sites such as Reddit? Do customers seem to run into a lot of problems, and does the support team for the exchange respond satisfactorily and in a timely manner? What country is the exchange based in, and does it have any specific restrictions for users of your country? If the exchange is based in a different country, you will probably have fewer options for recourse if something goes wrong. What is the overall average daily volume of the exchange? The top five exchanges globally are probably safer to use than smaller exchanges, based simply on the logic that these exchanges have grown because customers are satisfied with their trading experiences (let's ignore the potential phenomenon of wash trading for the moment). Does the exchange that you're researching allow trading of the specific cryptoassets that you're interested in? There's no point setting up an account on Binance if, for example, you want to buy ExampleCoin and Binance doesn't offer trading in ExampleCoin.

No matter which exchange you use, there's a chance that they may want some sort of identity verification. This may surprise you, and you may be reluctant to provide such identification. If you are suspicious about submitting your personal identity information to strangers who are running sketchy cryptocurrency exchanges in foreign countries, that's a good thing! You **should** be suspicious. Be suspicious of everything related to crypto. However, it is very common for exchanges to require identity verification before they allow you to start trading. Be prepared to submit documents such as the following: A scan/photo of both sides of your driver's license or passport; something that confirms your address (such as a bank statement or pay stub or utility bill); and a photo of yourself, holding the ID that you are submitting, with a handwritten sign that has the name of the exchange and the date that you are submitting the documentation. We're not kidding. Certain countries (especially the United States) have regulations relating to KYC (Know Your Customer) and AML (Anti-Money Laundering). Exchanges generally prefer to meet those rules even when they aren't located in the United States. If you are working with a gateway exchange that allows you to deposit or withdraw fiat currency, you may need to provide some information to confirm that you control the bank account from/to which funds are being transferred.

As already mentioned, for further research about trading cryptocurrencies, we recommend that you study some basic guides to trading stocks on traditional exchanges. That process is extremely similar to trading on crypto exchanges, so the only hard part is understanding and working with the technical steps required for maximizing your security precautions and storing your assets safely. We have several chapters in this book that go into those topics in more detail.

UNDERSTANDING WALLETS

Ensuring the safe and secure storage of your digital coins/assets is a top priority in cryptoasset investing. You can spend all the time you need doing research to find the perfect asset to invest in, and you can go through the process of funding an exchange and buying the asset, but if you can't store your asset safely, you may end up wasting your time and money. There are an incredible number of scams online, and the risk of being hacked is also significant. Right now, there are probably people all over the world who are trying to hack into your computer, to see if you have any crypto that they can steal. It sounds far-fetched, but it is very true!

As a precaution, ensure that you read through all the pages in the Security section of this book before you actually set up a wallet. It is also important to remember that sending any crypto to a wallet designed for a different type of crypto will result in a loss of your assets, without any warnings. Protect your money. You are your own bank.

In this chapter, we will explore the two categories of storage (hot vs. cold) and we will start to gain an understanding of various types of wallets (desktop, mobile, hardware, paper). As mentioned, no matter what type of wallet you decide to use, you need to protect your private keys, and make sure that nobody has access to them.

Cold Storage vs Hot Storage

Cold storage refers to a wallet of any type (be it physical, software, or paper) that is not connected to the internet. Having a cold storage wallet is the ultimate protection against online hacking. If your assets are not connected online, a thief cannot steal them unless he steals the actual physical wallet or gets a copy of your private key(s).

Hot storage refers to a wallet of any type that is connected to the internet. A hot wallet implies a higher risk of theft. A remote hacker may be able to penetrate your internet connection, your computer, and your security protocols, and then gain access to your assets.

Cold storage may be the safest option, but it is not convenient, especially if you actually want to use your cryptocurrencies. Cold wallets are still useful as they can always be used to receive funds. This can be done by anyone around the world if they know the public address for your wallet, or your public key. However, the removal of coins from a cold wallet by anybody, including the owner, requires knowing the private key for the wallet. This is why you should NEVER share your private key(s) with anybody, for any reason.

Hot storage is riskier, but with proper precautions to avoid being scammed or hacked, the risks can be minimized. Hot storage is more functional if you intend to use your cryptocurrencies. A common strategy is to store the majority of your assets securely in some type of cold storage while also storing small amounts of cryptocurrencies in a separate hot wallet (mobile or desktop wallets) for day-to-day use. This would be similar to the approach that many people have used historically with their fiat currencies. Most of their money is stored relatively safely in a bank account, with some cash available in a purse or wallet for daily spending purposes.

Exchange Wallets

With an account on a cryptoasset exchange, you'll be given wallets on the exchange for every single cryptoasset that is traded on the exchange. Often, this happens automatically and won't cost you anything. Some exchanges automatically assign you a wallet for each currency, while others will only assign you wallets for the specific assets that you are holding or trading. In the latter case, the exchange will automatically create a wallet for you when you buy some of that particular crypto. In a case where you're importing an asset to an exchange from an external wallet, you may have to click a "generate wallet" button so that the exchange will know that you need a new public address for that particular type of crypto. Most exchanges will let you create a new wallet address at any time, which is useful if you don't want to re-use a specific wallet address that you have already been using. After all, the number of wallet addresses available for most cryptocurrencies is much greater than the number of grains of sand on all the beaches on our planet, so they'll never run out of possible unique wallet addresses.

On an exchange, the public address for your wallet is sometimes displayed on the screen when you click on a price quote or the information page for any asset or security. In other cases, you may have to click on a "wallet information" tab to find your public address.

Individual wallet addresses on every exchange (and most other types of wallets too) are designed ONLY to hold one specific type of cryptoasset. Is this the third time that we've said this? Yes, but that's because we can't emphasize this strongly enough. A lot of people forget this restriction and accidentally send coins to the wrong type of wallet, and lose their crypto. If you have an account on an exchange, and you have some Bitcoin and some Litecoin in your account, they will NEVER be stored in the same wallet.

Instead, you will have a Bitcoin wallet with one address and a separate Litecoin wallet with a different address. This is extremely important. Inexperienced users often try to send one type of cryptocurrency to a wallet designed for a different type of crypto. When this happens, the sent funds are lost and cannot be recovered.

Having said that, certain wallets occasionally have the capacity to accept multiple currencies. This usually occurs with "platform" cryptoassets and their associated utility tokens. For example, Ethereum is a platform cryptoasset. It functions as a cryptocurrency, but it also acts as a platform or framework upon which developers can create other blockchain projects, which can then have their own tokens. An example of this is the Golem Network (GNT) on the Ethereum platform. Wallets designed specifically for a cryptoasset platform can usually hold both the platform coin (Ether, which has the symbol ETH) and any of the utility tokens associated with that platform. Sometimes, this process is very simple and seamless, and other times, certain information has to be added manually in order for the token to be recognized in the wallet. There is a type of wallet called “My Ether Wallet” (often abbreviated as MEW) which is an example of this. A single MEW wallet can simultaneously hold ETH, GNT, and numerous other Ethereum-based tokens. This can be useful, but before you go rushing off to set up a MEW wallet, make sure that you are on the legitimate site. There are imposter sites out there which are scams. If you accidentally use a wallet from a scam site, you will lose your funds.

Some exchanges offer multiple types of wallets. A "trading" wallet is the most common default, even if it isn’t named as such. “Margin” wallets are possible when an account is authorized to do margin trading (high risk, not recommended for anyone except professional traders). “Vault" wallets are sometimes offered for longer-term security. These Vault wallets are intentionally designed to make it difficult to retrieve your coins, which helps to minimize the risk of being hacked. Removing coins from a vault wallet often involves passing additional security tests and undergoing a wait period of 24 hours. If an attacker begins the process of trying to remove coins from your vault, you will be notified. Hopefully you'll have lots of time to notify the exchange and let them know to prevent the illegitimate withdrawal.

Cryptoasset exchanges usually have highly competent IT staff who are dedicated to protecting the security of your assets. Infosec (information security) is a high priority for exchanges. However, some exchanges have failed to protect their assets adequately. Cryptoasset exchanges are targeted relentlessly by hackers due to the staggering amounts of money that they hold or control. Because they are such obvious targets, it is risky to keep your money or store your crypto assets on an exchange. In recent years, there have been a series of high profile exchange hacks resulting in the bankruptcy of a few exchanges and losses of hundreds of millions of dollars to account holders. We recommend that you DO NOT hold your assets on an exchange. After all, you don't control your private keys for an exchange wallet. And if you don't own your private keys, you don't own your crypto.

Unfortunately, holding assets in your own wallets also presents significant risks from hacking, scams, and even from user error. If you are not comfortable using technology and computers, if you're only storing very small amounts of crypto, or if you are worried that your internet connection and/or computer could be compromised by hackers or malware, leaving your assets on an exchange may be an acceptable risk. You should always read through the Exchange Security and the Scams chapters of this book before you make that decision.

Desktop Wallets

Desktop wallets are software programs written for any of the major operating systems (Windows, Mac, Linux) which allow you to store your crypto on your personal computer. Typically, these wallets never transmit your private keys over the internet, which implies a low hacking risk. Unfortunately, there are forms of malware (such as keylogger malware) which can record your private key when you enter it into your computer, and then transmit that information to a hacker in another part of the world. As such, if you don't have a clean and uninfected computer, there is still a risk that you could lose your private keys.

It is also possible for hackers to break into your WiFi connection and see the contents of your computer. If you keep your private keys on your computer, especially if they are stored in any common type of unencrypted text file, you are at risk of being hacked. That is why it is important to have a secure internet connection, and why you shouldn't store your private keys on your computer. If you absolutely must store your keys on your laptop, it is important that you keep them in an encrypted file. A common password-protected Microsoft Office file is better than plaintext, but it is still risky. Your best bet is to learn how to use free encryption software such as GPG.

To mitigate the risks of desktop wallet or home computer hacks, remember that a secure internet connection is the first line of defense. The second line of defense is a computer that is not compromised. Windows machines and iOS machines are both more vulnerable to hacking than Linux machines, although even Linux systems can be susceptible to some malicious actions.

If you're using a desktop software wallet, always make sure you are using the wallet software that is recommended by the developers of your cryptocurrency. Never use any third-party wallets that are not endorsed by cryptoasset developers. We know of dozens of compromised or malicious wallet software programs which have caused users to lose their investments.

Mobile Wallets

Mobile wallets are software apps written for any of the major mobile platforms (Android, iOS, Windows) which allow you to store your coins on your mobile device, including both phones and tablets. These wallets are especially convenient for day-to-day shopping and transactions. Your mobile device can easily display a QR code on the screen which represents the public address of your wallet. Another user can scan that QR code and send coins directly to you from their own mobile device. Your mobile device can scan QR codes at stores and send crypto to those addresses. There are various "tap and pay" apps available now which allow your device to scan public wallet addresses and then send crypto to those addresses using near-field technology. Every week, more crypto-related apps are being developed and deployed. Cryptocurrency use is predicted to explode between 2020 and 2024.

It is important to note that mobile devices are generally less secure than desktop devices in terms of overall security from hacking, but also due to the risk of losing your phone. For this reason, most people do not store significant amounts of cryptocurrency in mobile wallets. Wise crypto enthusiasts are likely to put major investments into long term cold storage, moderate amounts into desktop wallets, and small amounts into their mobile wallet (which they can replenish periodically) for everyday use. The widespread public adoption of cryptocurrencies has already started in a few countries, and real-world cryptocurrency usage is growing rapidly around the globe.

When using a mobile wallet application, ensure that it is one which has been recommended by the developers of your cryptocurrency. Never use any third-party wallet apps that are not endorsed by the official development team for your cryptoasset, and always check that you are installing the correct app, rather than an imitation. Never store significant amounts of coins on your mobile apps. There have already been a large number of malicious wallet apps which have caused users to lose their investments.

Paper Wallets

A paper wallet is probably the safest type of cold storage, as long as nobody knows or gains access to your private key. To create a paper wallet, you download software which will generate the wallet. Never generate a paper wallet online, or directly from a website. Legitimate resources will recommend that you download their software and use it while offline. Unfortunately, it is still possible for a hacker to create a website and software that creates an offline wallet, but then stores a copy of your private key somewhere in the system and sends it to the hacker at a later time. Therefore, never use any paper wallet generator websites/programs that are not endorsed by the official development team for your cryptoasset. Also, be aware of imitation websites that look similar to legitimate websites, which try to lure in unsuspecting users. Knowing the correct address for a website, and typing that directly into the URL line on your browser, is always much safer than doing a search and clicking on a link. Some malicious websites can show up in advertisements at the top of search results on major search engines such as Google or Bing.

You may wonder how a paper wallet can store assets? And what happens if the paper wallet catches on fire? Well, the assets are not stored in or on the piece of paper. The piece of paper is just a symbolic printout which tells you the public address that is used when you or other people deposit funds to the wallet, and the private key that you need to remove or transfer funds out of the wallet. Once you know the information from the piece of paper, you can destroy it. Of course, that's very risky, because there is almost no chance that you'll be able to successfully memorize your private key. Most people will therefore store a copy of their paper wallet in a safe in their house, or in a safety deposit box. It's probably best to store the document in at least two locations, in case your house burns down. However, if you have too many copies, and some of them are in locations which are not secure, there is a higher risk that someone can get a copy of your private key and empty your wallet.

Some people also turn their paper wallet into a PDF and store it on their computer. This is very risky. If your computer becomes compromised, hackers will be able to read your private key from that document. It is even risky to print a paper wallet from any sort of WiFi-connected or networked printer, because the printer will temporarily store a copy of the document in its storage memory. It might be possible for someone to steal the printer, tear it apart, remove the storage media, and recover previously printed documents, long after you've printed your paper wallet. It is even more likely that someone might be able to hack into your networked printer remotely, and scan through the document cache. Sigh. There are so many risks.

We believe that paper wallets ARE the safest type of long term storage, but that you should take certain security precautions to minimize risks. Rather than printing out copies of your paper wallet, it may be more prudent to copy the public and private key information onto a couple of USB keys or portable flash drives, and then to encrypt those entire drives using a password that nobody but you knows, then to store those keys in two separate hidden and secure locations. Ultimately, the absolutely safest approach, for the superparanoid, would be this: Create your paper wallets on an air-gapped computer (one that isn't connected to the internet), using a Linux operating system, then encrypt and store your keys as we just described. This should improve the security of your assets from "piggy bank" levels to "Fort Knox" levels. About the only way to improve your security beyond that would be to find and use an air-gapped computer that hasn't been connected to the internet since before 2009, before crypto was created (and therefore before malware was created to target crypto users).

Hardware Wallets

Various types of hardware wallets exist. Many of these wallets can store multiple unrelated cryptocurrencies, although to be clear, this is only possible because the device (the hardware wallet) has room to store several different software wallets on it. Your various cryptoassets will not be stored within a single wallet on the device.

A hardware wallet may look similar to a USB key, or it may perhaps be a small mobile device with a screen, similar to a small music player. Some of the main hardware wallet providers at the current time are Ledger, Trezor, and KeepKey. Some of these companies offer multiple types of devices.

If you are going to buy a hardware wallet, ALWAYS buy it directly from the manufacturer. No matter how impatient you are with backlogged orders at the manufacturers, and no matter how much of a price discount you might find from an alternate supplier, you should never buy a hardware wallet from eBay, CraigsList, Amazon, or any other source. To be fair, there are a few authorized third-party resellers who use these sites legitimately, but there are also a LOT of compromised wallets being sold through various eCommerce platforms, and a lot of users have lost their investments by putting them into an insecure wallet. The basic methodology for this scam is that the person selling you the wallet (often repackaged to look like it has never been opened) now knows the private key to the wallet, so once you deposit your cryptoassets into the wallet, the scammer can steal your coins. This has happened to a huge number of unsuspecting victims! Protect yourself by buying directly from the manufacturer.

A hardware wallet can function in different ways. Even if it is connected to a computer which is online, you can consider it to be cold storage. Private keys are maintained in a secure offline environment on the hardware wallet, and they are fully protected even if the device is plugged into a malware-infected computer. If you generate and store your private keys offline, using a hardware wallet, hackers should have no way of getting at your cryptoassets. Hackers would have to steal the hardware wallet itself to do that, but even then, it can be protected with a PIN code. You don't necessarily need to worry about your hardware wallet getting stolen, lost or damaged either. You can create a secret backup code, which can be used to retrieve your cryptoassets. Of course, that secret backup code can be a weak link in your security protocols, because it needs to be kept just as secure as a private key.

Not all cryptoasset project coins or tokens can be stored on hardware wallets. Typically, only a few dozen of the most well-known cryptos are supported. However, despite the price, a hardware wallet is a very good option to protect your investments.

KEYS

You’ve already heard us talking about public addresses, public keys, and private keys. In this chapter we will try to explain them in detail. You can think of a public address as being somewhat similar to a bank account number. In the case of cryptoassets, which rely on a public blockchain, anyone with an account number can view the balance (amount of crypto stored) in an account. A public address is thus used to receive funds OR to see the balance in an account. A private key, on the other hand, is like a password. If you have the private key to an address, you are allowed to make transactions (send assets) from that address. You may also hear reference to things like "seeds" and "pass phrases," and we’ll explain those in this chapter.

People often talk about something called a public key. Often, this term is used interchangeably with public address. However, despite representing the same information, the definitions of these terms differ on a technical level. We will explain that later in this chapter. For now, if you ever see or hear a reference to a public key, you can assume that it is essentially synonymous with the public address.

This chapter may cause some confusion, because we’re going to go into some information that is more technical than the average user may need to understand. If you go to the “Public & Private Keys” page on our website, there’s a short video at the bottom of the page which provides a sufficient overview on the topics. The most important thing to gain from this chapter is a general understanding of the difference between public addresses and private keys, and an understanding that you must never share your private keys with anyone.

Public Keys

To begin, what does a public key look like? A real public key is usually a long alphanumeric string consisting of hexadecimal characters. Hexadecimal characters are restricted to the digits 0 through 9 and the letters A through F. You may wonder why hexadecimal characters are used. Why not just use numbers? Or if we need to use letters, why not use the whole alphabet instead of just including the letters A through F? The answer is simple, but would make more sense to a mathematician or a computer programmer. Hexadecimal notation is commonly used in computer programming and related fields. Hexadecimal is the numbering system for base 16. We're used to base 10 (decimal) numbering, which probably arose naturally because our ancestors had ten fingers and ten toes, and were used to counting on them. But for a computer, the inherent numbering system is base 2 (binary). Base 16 is a natural extension of binary. We have an appendix at the back of this book to explain hexadecimal numbering in more detail, if you're curious. But you don't really need to understand it fully in order to work with crypto. Just take our word that base 16 is fairly useful for computers.

Let's get back to public keys. Here is an example of what a public key might look like. This is a real public key (slightly different from the public address) for a real Litecoin wallet. When expressed in text form, the public key is:

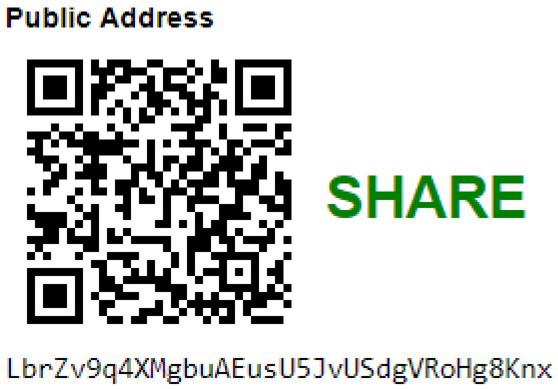
0437F40BE1827A7F5FF4C1ADA993F76313D1B7278FBC55123782C7C926CEAA6B5E8A9F05FC40BD6EC995C955511576C22E7CA396F2EEB73871DD34217B6CC2D7A5

As mentioned, this public key represents a wallet address. It's fairly long, isn't it? It would be impossible for most people to memorize that address. Having a bank account number which is 130 characters long would undoubtedly prove to be inconvenient. Imagine how long the lineups would be at the bank if you had to give the bank clerk an account number that is 130 characters long. That wouldn't be suitable or convenient for regular daily use. The same thing is true when you have a cryptocurrency wallet address which is that lengthy. To make public keys more user-friendly, this problem is solved by shortening the public key to about a quarter of its original length, making it much easier to work with. The shortened version of a public key is known as the public address, which we'll cover next.

Public Address

What does a public address look like? Unlike a public key, a public address is not restricted to hexadecimal characters. It usually takes the form of an alphanumeric string. Quite often, every letter of the alphabet and every digit could be present in a single address. Letters may be either uppercase or lowercase (or both) which means that there are sixty-two possible options for any specific character in the key (26 capital letters, 26 lowercase letters, and 10 numerical digits). The case of a letter is important. A lower case letter is not treated the same way as a capitalized version of the same letter. Not every cryptocurrency allows all sixty-two alphanumeric characters to be used in a public address. Some cryptos have restrictions, for various reasons. Depending on what crypto you're using, your public addresses may have different structures, such as using only capital letters or only allowing one of the ten digits.

Here is an example of what a public address might look like. This is a real public address for a Litecoin wallet. When expressed in text form, the public address is: **LbrZv9q4XMgbuAEusU5JvUSdgVRoHg8Knx**.



Public Address

LbrZv9q4XMgbuAEusU5JvUSdgVRoHg8Knx

Do not send any funds to this wallet! You will lose your money. This wallet address is not intended for you to send us a donation or a tip! Anybody who reads this book will soon have the ability to remove any funds that were deposited into this wallet.

The black and white pattern that you see above is called a Quick Response code (or QR code). A QR is a barcode which can be scanned using a dedicated QR scanner, or by using a QR scanner app on a smartphone with built-in camera. You may not have known that a barcode doesn't have to be composed solely of thick and thin lines, but can instead be pixelated like a QR code. Anyway, this particular QR provides a barcode representation of the exact same string of text as our public address. QR codes exist to present the same information in a different format that's both easier to work with and more accessible. It is much more efficient to scan a QR code using your smartphone than it is for you to type out a few dozen characters without any typos. It is also much easier for your smartphone to scan a QR code correctly than it is for your phone to scan and correctly understand a string of text or letters.

Some types of public addresses have certain conventions. Bitcoin public addresses are up to 34 alphanumeric characters long (sometimes slightly shorter) and always start with the digit 1. Litecoin addresses are always to up 34 characters long (alphanumeric), but they always start with an uppercase letter L. Iota's addresses use any of the 26 letters (uppercase only) and the digit 9, allowing for 27 options for each character in the key. Incidentally, Iota's key is 81 characters long, which is much longer than the keys for Bitcoin or Litecoin or most other cryptocurrencies.

Public Address vs Public Key

Despite appearing radically different, the public address shown above corresponds to the public key described in the previous section. As mentioned, the shorter length of this public address makes it more convenient and user-friendly than the public key. Unfortunately, a lot of people refer [incorrectly] to the public address as being a public key. We can sympathize. We've already implied the same thing earlier in this book. We won't judge you for using the two terms interchangeably, but at least now you know that there is a very important technical difference between the two, even if they are intended to represent the exact same information.

As mentioned, if you know a public address or key, you can see the balance of any crypto that might be stored in that address. This is due to the fact that each blockchain is set up as a public ledger. There are advantages and disadvantages to this system. Let's review those advantages and disadvantages. An advantage is that the public ledger is a permanent and immutable (unchangeable) record of all the transactions that have ever occurred. As such, you don't have to worry that someone has changed or edited any of the past transactions, therefore you know that the information on the blockchain is correct. This is extremely important when it comes to accounting, the keeping of financial records, and a trust of previous transactions. Incidentally, don’t forget that financial records are not the only information that can be stored on a blockchain.

Of course, as we mentioned earlier in the book, a public ledger also presents some disadvantages. One such disadvantage is that anybody who knows a wallet address can see the amount of money in that wallet. They may not know who owns the wallet, but the contents of the wallet can’t be hidden. All transactions are traceable. If you make a transaction from your wallet to a stranger’s wallet, that stranger now knows the address of your wallet (and can thus see the contents). This is a potential security risk.

Let’s get technical for just a moment. Although the public address and public key represent the same information, they obviously look very different. They have different combinations of letters and numbers, and one is much longer than the other. How can they mean the same thing?

A public address is derived from a hashing algorithm which has been applied to the public key. A hashing algorithm is a one-way street in terms of cryptography.   With a public key, it is possible to quickly produce a public address, but it is essentially impossible to work backwards to figure out the public key with just a public address. This is important in terms of data security. We’re not going to explain why it’s essentially impossible to reverse-engineer the hashing algorithm; you’ll just have to trust us that it can’t be done. We have an appendix about hashing if you’d like to learn some of the slightly more technical details. You don’t need to know exactly how it’s done though; you just need to know that it works.

There has been some worry that at some point in the future it might become possible for someone to "crack" a public key and derive the private key from it. Specifically, people are worried that quantum computers might be able to accomplish this task. The probability of this happening any time soon is extremely low, because our current supercomputers aren't powerful enough to crack keys (and if they were, they'd be put to better uses than cracking a single wallet address). However, in a theoretical sense, if it was possible to somehow crack a public key to derive a private key to the same wallet, the funds stored in wallets would be vulnerable to theft. The use of a public address rather than a public key acts like an extra locked door at the entrance to your house. Of course, there's still a drawback. When you send any crypto from a wallet (you do a spend), your public key rather than public address is revealed on the blockchain. At that point, you no longer have the advantage of that extra "locked door" for thieves to penetrate. Essentially then, the extra layer of security provided by using a public address instead of a public key is only valid for a wallet that has only ever received (and never spent) any crypto.

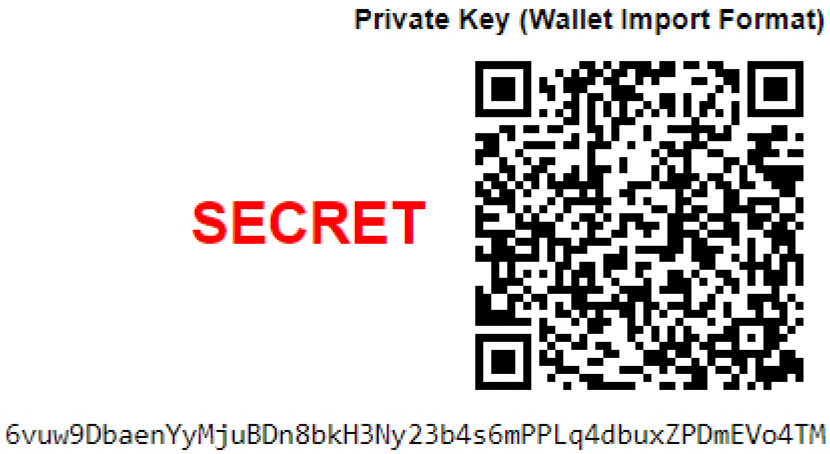
People talk a lot about whether cryptocurrency systems could fall apart when quantum computers eventually become a reality. You may be reassured to know that quantum computers are believed to be *possibly* capable of deriving the private key from a public key, but not capable of deriving a private key from the hash of the public key (the public address). The authors of this book don't worry about quantum computers. Once quantum computers eventually become a reality, they'll probably be put to much more important uses than opening peoples' wallets. Also, certain cryptocurrencies have been specifically designed to be "quantum resistant." I guess we'll see how that plays out someday.

Private Keys

A private key has the same general appearance as a public key and without context, telling the two apart is extremely difficult. Private keys however, often tend to be longer than public keys.

Here is an example of what a private key may look like in a mainstream WIF text format. WIF stands for Wallet Import Format. This is a real private key (password) for a Litecoin wallet (we presume that the wallet is empty). The private key for this wallet is:

6vuw9DbaenYyMjuBDn8bkH3Ny23b4s6mPPLq4dbuxZPDm EVo4TM.



Private Key (Wallet Import Format)

SECRET

6vuw9DbaenYyMjuBDn8bkH3Ny23b4s6mPPLq4dbuxZPDmEVo4TM

What are private keys used for? As previously mentioned, you can think of a private key as a password to a digital account, or you could think of it as a key to a locked cabinet. A private key grants you access to the funds found within its associated wallet, and that specific wallet is identified by a public key (or public address).

With your private key, you don't need to know your public key. This differs slightly from the concept of a bank account. If you go to a bank, you need to know your account number. Simply presenting your password to a teller without your account number would not grant you access to your account. On a blockchain, the information pertaining to both the account number *and* its password are embedded within the private key. If you were hypothetically able to do this at a bank, you could tell the bank teller that your password is "Heather120482" and the teller would be able to say, "Oh, of course, that password is for account number 7285-28-002765." In other words, comparing a bank account and password to a public address and private key is not a perfect analogy.

It is important to note that each wallet has its own distinct private key. A private key only opens one wallet. Not surprisingly, you cannot use a private key for a Bitcoin wallet on a Litecoin wallet, because it would not be the correct private key.

You should NEVER share your private key with anyone, no matter what the circumstances are. The private key posted on this page leads to an empty wallet. If you own any Litecoin and are inclined to make a test transaction, you could send a minuscule amount to that wallet. You could use a blockchain explorer to watch the transfer. Having said that, we do not recommend that you try that, as we do not accept donations, and we don't monitor that wallet. Anyone who reads this page has the capacity to unlock the wallet in question and remove any funds that are in it.

View-Only Keys

Currently, Monero is sometimes reputed to be the only completely private cryptocurrency, although certain other privacy coins also make the same boast. Monero is so private that even with the public key of a Monero wallet, you can't see the amount of funds in the wallet. This presents a challenge in the case where a party to a transaction would like to show the other party the contents of their wallets, but doesn't want to share their private key and risk losing funds. To resolve this challenge, every Monero wallet has a “view-only” key, in addition to the public and private keys. A view-only key allows someone to access a wallet and “view” its contents without providing any other information on the wallet. View-only keys are irrelevant to the majority of cryptoassets currently available.

Pass Phrase

A pass phrase is a more complex (and consequently more secure) version of a password. Pass phrases, unlike passwords, are generally allowed to include spaces. As such, even a simple pass phrase usually provides much more security than a traditional password, due to its length. You may be surprised by this, but a comprehensive pass phrase such as "I like to eat chocolate chip cookies" is incredibly more difficult for a supercomputer to crack by using brute force methods than a shorter arbitrary password such as "Y8s9aJ#&@"

Every password or pass phrase becomes more secure and harder to crack when you make it longer. Adding even a single extra character to an existing password usually makes it at least seventy times more difficult to crack, especially if you’re using random characters. Although a pass phrase that is a sentence in English might not have the advantages of being comprised of “completely random” characters, the extra length should make up for that. Add some random punctuation and numbers to your pass phrase, and you get top marks for great security.

Some websites allow the use of pass phrases in place of simple passwords. This is good. Any website administrator whose site doesn’t allow for passwords that are at least 32 characters long is in need of some computer security lessons. The ability to use long pass phrases on websites will become increasingly common in the future.

Certain hardware cryptocurrency wallets allow the use of pass phrases as a security measure. In these cases, a pass phrase acts as more than just a fancy PIN number to access the device. The pass phrase is required to access the wallet accounts on the device, rather than just to access the device itself. The pass phrase is not actually stored on the device. If your device was stolen and "taken apart" in a lab, the thieves would be unable to get into your crypto wallets because they wouldn't know the pass phrase. This is due to the way a pass phrase is processed. Rather than being stored on the wallet, an algorithm processes the pass phrase information that you enter, and that processed information is what allows your crypto accounts to be unlocked. Therefore, a thief would need to have both the physical device AND the pass phrase for the device, in order to access your money.

Some pass phrases for certain cryptocurrencies are designed intentionally to work universally across all devices or websites (but only to unlock one specific wallet, of course). This is ok, as they are incredibly complex. Using a unique 25-word pass phrase on a different device is mathematically much, much more secure than signing into a bank account from a different device.

A pass phrase can consist of a “seed phrase” plus an extra word that acts as a password to that seed phrase. Next, we will examine seed phrases.

Seeds

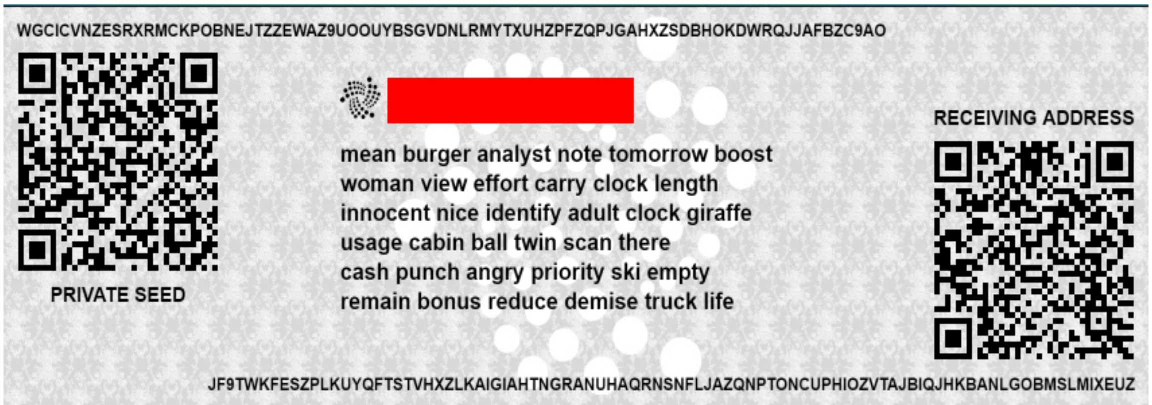
We will preface this section with a piece of advice. This is one of the Golden Rules of crypto security: Never generate a seed (or private key) from an online website! This is a certain way to lose all of your money. Many of the websites that generate seeds are compromised, and your seed or private key will also be sent to a malicious actor, who will wait until you have deposited some crypto into a wallet. After you've done so, he/she will steal it. Believe us, we know of several people that this has happened to!

A seed phrase is a specific collection of common words, in a particular order, which acts as a complex password. Why use a seed instead of a private key? The answer is simple: It is because it is easier to type into a computer than a long private key. Some people just like to use common everyday words to access their wallets, instead of complex alphanumeric strings. Iota is one of the cryptocurrencies that uses seeds, so for the next couple pages, we'll talk mostly about how seeds work within that particular cryptocurrency. However, Iota is certainly not the only crypto that uses seeds, so this knowledge will be useful for many other crypto projects too.

Seed phrases can have any number of words, but they commonly consists of 12 or 24 word seeds. Unlike a pass phrase that might be used to get into a wallet or website, a seed phrase generates a specific public and private key. Here's an example of a 36-word seed phrase generated for an Iota wallet: *"mean burger analyst note tomorrow boost woman view effort carry clock length innocent nice identify adult clock giraffe usage cabin ball twin scan there cash punch angry priority ski empty remain bonus reduce demise truck life."* By using that combination of 36 words, which must be used in that particular order, the following seed is created:

JF9TWKFESZPLKUYQFTSTVHXZLKAIGIAHTNGRANUHAQRNS NFLJAZQNPTONCUPHIOZVTAJBIQJHKBANLGOBMSLMIXEUZ

Here's a screenshot of the wallet information created when this seed phrase and seed were generated:



WGCICVNZESRXRMCKPOBNEJTZZEWAZ9UOOUYBSGVDNLRMYTXUHZPFZQPJGAHXZSDBHOKDWRQJJAFBZC9AO

[redacted]

mean burger analyst note tomorrow boost
woman view effort carry clock length
innocent nice identify adult clock giraffe
usage cabin ball twin scan there
cash punch angry priority ski empty
remain bonus reduce demise truck life

PRIVATE SEED

RECEIVING ADDRESS

JF9TWKFESZPLKUYQFTSTVHXZLKAIGIAHTNGRANUHAQRNSNFLJAZQNPTONCUPHIOZVTAJBIQJHKBANLGOBMSLMIXEUZ

Note that in this particular example, we generated a "real" seed, but we did it from a website that is reputed to be a scam site after many Redditors have reported losing funds. This is why we blocked out the identifier URL with the red stripe. Do not send funds to this wallet address. You will lose them. This is not a wallet that the authors are using or monitoring, and we do not accept donations.

As noted in other sections, scam websites are abundant for almost every type of cryptocurrency. Never trust a site to keep your funds safe without doing exhaustive research. A good resource in determining the safety of any particular website is the official subReddit for that cryptoasset, where you can find resources listed on the sidebar. The moderators of every crypto subReddit generally work hard to ensure that only sites believed to be safe and legitimate are listed on their resource pages. Even so, scam websites sometimes trick Reddit moderators. Ultimately, you should only use resources that are endorsed directly by the official development team for your cryptocurrency.

Assuming that this wallet was legitimate, the seed phrase and seed generated for this wallet will open a specific wallet which has the following “receive address”:

JF9TWKFESZPLKUYQFTSTVHXZLKAIGIAHTNGRANUHAQRNS NFLJAZQNPTONCUPHIOZVTAJBIQJHKBANLGOBMSLMIXEUZ

This receive address is comparable to a public key for the wallet.

It is important to understand that a seed phrase is not actually the same as a private key. This is because a seed phrase allows for the generation of a number of equally valid private keys. We bet that you were surprised by this! A seed phrase, which is sometimes called a “word seed,” is simply a more human-readable way of expressing a "root private key." The 36 words that we used in the example above, when repeated in that exact sequential order, will always generate the exact same root private key.

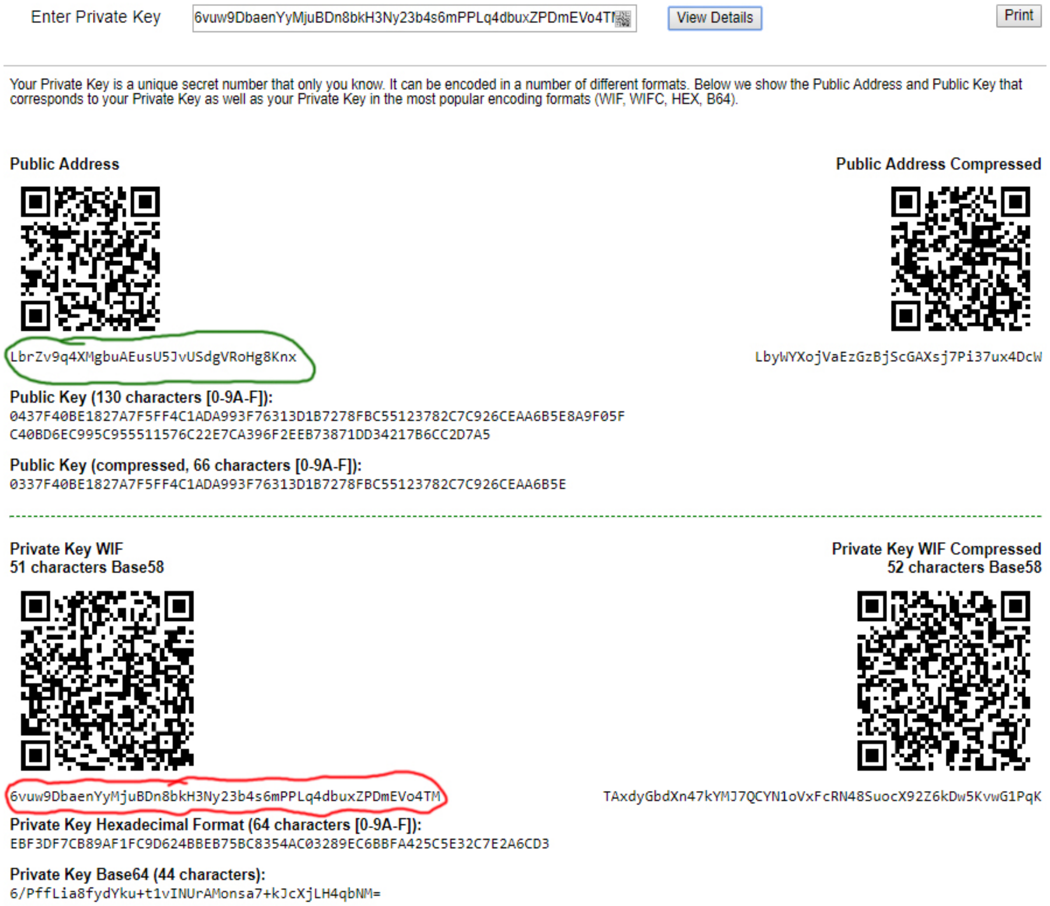
Now you’re probably confused by the reference to a “root” private key, since that term wasn’t mentioned earlier. A root private key is used to generate other private keys for other wallet addresses. All of your addresses will still have different private keys, but they can all be restored by the single main root private key which comes from your seed phrase. This is probably more than a basic crypto enthusiast needs to learn right now, so just keep this in mind for later.

A seed phrase may also be described as a recovery phrase, as the seed phrase offers the means to recover (remove) your funds from your wallet.

Additional Technical Information for Advanced Users

In addition to regular public addresses and private keys which come in the expected and familiar text format, there exist variations of these strings in different data formats and of different field lengths. There can be compressed and uncompressed seeds. There can be different encryption standards used when generating these keys. These are confusing concepts, so don’t worry if they don’t entirely make sense. We’re about to delve into the realm of math and computer science, so all that matters is that you understand the difference between public and private keys. If you don't understand the additional technical information in the rest of this chapter, it's ok. You can just skip ahead to the next chapter if you'd prefer.

Here are some additional details associated with the wallet shown above.



Enter Private Key 6vuw9DbaenYyMjuBDn8bkH3Ny23b4s6mPPLq4dbuxZPDmEVo4T

Your Private Key is a unique secret number that only you know. It can be encoded in a number of different formats. Below we show the Public Address and Public Key that corresponds to your Private Key as well as your Private Key in the most popular encoding formats (WIF, WIFC, HEX, B64).

Public Address

LbrZv9q4XMgbuAEusU5JvUSdgVRoHg8Knx

Public Address Compressed

LbyWYXojVaEzGzBjScGAXsj7Pi37ux4DcW

Public Key (130 characters [0-9A-F]):

0437F40BE1827A7F5FF4C1ADA993F76313D1B7278FBC55123782C7C926CEAA6B5E8A9F05F
C40BD6EC995C955511576C22E7CA396F2EEB73871DD34217B6CC2D7A5

Public Key (compressed, 66 characters [0-9A-F]):

0337F40BE1827A7F5FF4C1ADA993F76313D1B7278FBC55123782C7C926CEAA6B5E

Private Key WIF
51 characters Base58

6vuw9DbaenYyMjuBDn8bkH3Ny23b4s6mPPLq4dbuxZPDmEVo4TM

Private Key WIF Compressed
52 characters Base58

TAxdyGbdXn47kYMJ7QCYN1oVxFcRN48SuocX92Z6kDw5KvwG1PqK

Private Key Hexadecimal Format (64 characters [0-9A-F]):

EBF3DF7CB89AF1FC9D624BBEB75BC8354AC03289EC6BBFA425C5E32C7E2A6CD3

Private Key Base64 (44 characters):

6/PffLia8fydYku+t1vINUrAMonsa7+kJcXjLH4qbNM=

First, it is important to grasp that numbers or text strings can be represented in different ways. For example, the number 4 can be represented simply as 4, or it can be represented mathematically as 2*2 or 2^2. If you decide to depart from our conventional base 10 system of mathematical notation, and convert to binary notation, the number 4 (as expressed in base 10) can be represented as "0100".

When you look at the graphics above, the public and private keys are represented in four common notations used for key information. These four notations are called WIF, WIFC, HEX, and B64. Be aware that all four notations express the same string in their respective ways.

WIF stands for Wallet Import Format. This is the traditional format for a key, i.e. an alphanumeric string containing both lower and upper case letters. The WIF version of the private key is **6vuw9DbaenYyMjuBDn8bkH3Ny23b4s6mPPLq4dbuxZPDmEVo4TM**.

WIF keys are 51 characters of the "Base58" character set (more on this below).

WIFC stands for WIF Compressed. The WIFC version of the private key is **TAxdyGbdXn47kYMJ7QCYN1oVxFcRN48SuocX92Z6kDw5KvwG1PqK**.

The format for this key is 52 characters of the "Base58" character set.

HEX stands for Hexadecimal, a base-16 numbering system. The 16 allowed Hexadecimal characters are the digits 0 through 9 and the letters A, B, C, D, E, and F, which represent 10, 11, 12, 13, 14, and 15 respectively. In the above graphic, the private key in hexadecimal format is **EBF3DF7CB89AF1FC9D624BBEB75BC8354AC03289EC6BBFA425C5E32C7E2A6CD3**.

B64 stands for Base 64. The 64 characters allowed are the letters A through Z (capitalized) which represent the numbers 0 through 25, the letters “a” through “z” (lower case) representing the numbers 26 through 51, the digits 0 through 9 representing 52 through 61, the “+” symbol representing 62, and the “/” symbol representing 63. In addition, the equal sign is a permitted character, used for padding. Base 64 is similar to Hexadecimal but is in base 64 rather than base 16. In the above graphic, the private key in B64 format is expressed as:

6/PffLia8fydYku+t1vINUrAMonsa7+kJcXjLH4qbNM=

Base 58 is a group of binary-to-text encoding schemes used to represent large integers as alphanumeric text. It is similar to Base64 but has been modified to avoid both non-alphanumeric characters and letters which might look ambiguous when printed. Thus, it is designed to be easily used for manually entering data or copying from a visual source. In addition, it is easy to copy & paste this information because a double-click will usually select the whole string, without getting fooled by any punctuation that might have been present in B64 format. Base 58 drops six characters from the conventional base 64 character set. The six characters that are dropped are the digit zero, the capital letter "o", the capital of the letter "i", the lowercase of the letter "L", and the "+" and "/" symbols. This method is well-suited to encode large integers, but not very helpful or efficient when trying to encode longer portions of binary data, since it is not an exponential power of 2.

MINING

Different cryptoasset projects have different features affecting asset security, the generation of new assets, and the establishment of consensus or governance mechanisms. Consensus mechanisms refer to systems of rules that let a widely dispersed group of strangers (or computers) come to an agreement about anything. Governance mechanisms enable the same diverse groups of entities to set or amend rules that govern the behaviour of their projects or userbase.

When you research cryptocurrencies, it won't take long before you'll see references to phrases such as Proof of Work (PoW) and Proof of Stake (PoS), with variations on each. Proof of Work and Proof of Stake are the two most common systems that have been adopted by various cryptoasset projects, but in addition to explaining those, we'll mention a few other consensus systems that you might come across.

Mining, and Proof of Work

Mining is the process by which some cryptocurrency transactions are verified as being legitimate transactions, and are then added to the public ledger (the blockchain). Mining is also a means through which new coins may be released for many projects. The mining process generally involves two steps: Compiling recent transactions into blocks, then solving a computationally difficult puzzle. All miners are competing against each other.

The participant (miner) who is first to solve the puzzle wins the right to place the next block on the blockchain, and claims a reward. The reward for "mining" a block is typically a combination of all of the transaction fees associated with the transactions compiled in the block, plus some newly released coins.

Using Bitcoin as an example, the block reward is currently set at (Transaction Fees + 12.50 BTC). Needless to say, when you think about the current price of Bitcoin, it's obvious that you would make a LOT of money if you were able to mine even a single block! The only problem is that there are a very large number of people around the world that you're competing with, so it's very difficult to mine a Bitcoin block these days. Most new Bitcoin blocks today are mined by "Pools," which are collections of thousands of small miners who pool their computing resources together and share the rewards any time their pool is successful at mining a block.

Not every cryptoasset project uses mining to process transactions and to create new coins, but it is one common approach. A "Proof of Work" system is one which relies on mining. In theory, anyone who owns some decent computing hardware and has internet access can participate in mining. In practice, however, mining for some cryptocurrencies has become so challenging that only large-scale mining farms using specialized equipment referred to as ASIC's are now able to mine profitably. This is a "problem" for Bitcoin. Bitcoin mining is no longer attractive (profitable) for small individual miners. However, this "problem" is also something which is very good for Bitcoin itself, and helps to keep Bitcoin secure. We'll explain shortly.

To understand mining you need to understand blockchain technology. More specifically, you need to understand what the "blocks" in the blockchain consist of, in other words, what kind of data and information is contained in each block. A single block contains cryptographic signatures for that block, and also for the transactions within the block. The transactions are collected from the network, typically with a small fee attached. Those fees become a part of the block reward.

In addition, there is usually some kind of difficulty value attached to the solution for the block, which can scale up or down over time. The goal of this difficulty value is to keep the generation rate of new blocks relatively constant. As we've mentioned, the goal for Bitcoin is to generate new blocks approximately once every ten minutes, averaged over long periods of time. If the average time to mine Bitcoin blocks gradually drops to less than ten minutes, the difficulty level increases, to compensate and slow down the miners. If the average time between blocks starts to increase significantly, the difficulty level decreases.

Understanding mining requires an understanding of block rewards. For most coins, block rewards are given to the person/group that finds a valid solution to a cryptographic hashing algorithm. To simplify this, we can say that each block has its own mathematical puzzle that people all around the world are simultaneously trying to solve. The first person or computer that discovers the correct answer "wins" the block as a prize. Only one person (the first to discover the correct solution for the block) gets to collect the reward for that specific block. The system then moves automatically to the next block, and there is no longer any potential value in trying to find the solution to the previous block. Blocks are therefore released sequentially and one at a time as their puzzles are solved.

Solving a block's "puzzle" generally entails having a computer perform a very large number of calculations. Each of these calculations is called a hash. A kilohash (khash) is a thousand hashes. A megahash (mhash) is a million hashes. A gigahash (ghash) is a billion hashes. A terahash (thash) is a trillion hashes. Depending on the particular cryptocurrency, the complexity of the puzzle may require thousands to trillions of guesses before someone solves the puzzle. As more miners start competing to find the solution to the next block in the blockchain, the system eventually adjusts itself so the answer to the next block puzzle becomes harder to solve. This leads to an increase in the number of hashes being performed by all miners. The global hashrate for Bitcoin, the cryptocurrency which currently has the largest amount of miners working on it, is currently extremely high and consumes very large amounts of electricity. The Bitcoin mining system is frequently criticized due to this heavy consumption of our global energy supplies.

As an individual miner, you would have an extremely low chance of solving the puzzle for the next Bitcoin block, due to heavy competition from hundreds of thousands of other miners around the world. You may wonder if you can increase your odds by targeting a block that is a few thousand blocks into the future, and working on that puzzle in advance? No. The solution to each block's puzzle is a mathematical calculation that incorporates the answer to the puzzle from the previous block. Therefore, there is no way to pre-calculate the correct answer for a future block without knowing the solution to the block before it, and by extension, all of the previous blocks before those. There is no way to predict the exact mathematical puzzle for a specific future block until the puzzles are solved for all of the blocks that come before that one. Since there is no way to start working on the puzzle for future blocks, and there is no longer any reward for trying to solve the puzzles for past blocks, every miner concentrates all of their attention on the block that currently needs to be mined (solved mathematically).

Each cryptocurrency has a target for the average block mining time. That average time depends on the design of the cryptocurrency in question. Bitcoin, as mentioned, has an average mining time of approximately ten minutes per block. Litecoin and Vertcoin each have an average mining time of approximately 2.5 minutes per block. Monero has an average mining time of approximately two minutes. Dogecoin has an average mining time of just over one minute. Each cryptocurrency uses a different hashing algorithm with a different cryptographic formula and level of difficulty. Incidentally, we're not going to explain hashing algorithms here, because that topic is quite complex, and would only be of interest to people who are fairly comfortable with math and computers. However, we have an appendix to explain hashing algorithms in the back of this book, which might be of interest to some advanced readers.

For some cryptoassets, mining can be performed by a computer that isn't very powerful, ie. a machine with a fairly low processing capability. There still exist a number of cryptocurrencies that can be mined using CPU's, although this is becoming more uncommon. The CPU is the Central Processing Unit, or "brain" of a computer. For many cryptos now, mining is predominantly done by GPU's (Graphics Processing Units), which are graphics cards with much more computational power than typical CPU's. When a crypto project is "ASIC-resistant," a GPU is the most powerful device which can mine that cryptocurrency effectively. Vertcoin is an example of such a cryptocurrency. Thanks to ASIC-resistant projects, just about anyone with a decent computer (including most gaming rigs) might be able to be a successful miner, potentially earning several dollars per day after factoring in electricity costs. However, electricity costs are the biggest obstacle to successful mining. In many countries, the cost of local electricity makes it impossible to mine any coins profitably.

An ASIC (Application Specific Integrated Circuit) is a type of integrated circuit that is designed and created for a specific application or purpose (in this case the mining of PoW coins). Compared to a general-purpose integrated circuit, an ASIC is faster and more efficient because it is specifically designed to perform one task. ASIC's can be designed for anything ranging from portable audio recording units to image processors in digital cameras. In terms being useful for cryptocurrency mining, they are commonly designed to mine just one specific type of cryptocurrency, and are frequently used for Bitcoin and Litecoin. ASIC's are considered proprietary technology as they are custom-made, and each model is designed specifically by the company that manufactures them. The efficiency of an ASIC compared to that of a CPU or even a GPU has led to criticism of the general suitability of PoW as a consensus mechanism, because ASIC miners have come to dominate the mining industries of certain types of crypto. ASIC's are usually quite expensive, and often become obsolete within several months of being manufactured. There is also a risk to buyers, because if the mining algorithm of your target crypto changes, it renders the ASIC useless. This is a fairly strong deterrent that keeps a lot of small individual investors from purchasing an ASIC. In fact, this possibility may also be a deterrent that keeps some companies from developing ASIC's for certain cryptos. For example, Monero appears to be changing its mining algorithm approximately once every six to twelve months, in an attempt to prevent companies from developing ASIC's. The reason for this is that the Monero community wants to keep mining accessible to smaller players, ie. individuals with home computers who are interested in mining.

STAKING/FORGING

Forging is a similar process to mining. However, forging occurs in a Proof of Stake system. In a Proof of Stake system, the creator of the next block is chosen via various combinations of random selection and wealth or age. The "wealth" (size of holdings) and "age" (duration that holdings have been sitting in a wallet) are two main characteristics of the stake. Once the creator of the next block on the blockchain is chosen "randomly" by the forging algorithm, the assigned creator automatically "forges" or creates the block. Whereas mining is a race, with people competing to find the next block, the process of forging is a "random probability" process. Once a creator for a block has been determined, there is no longer any competition, which means that staking is not characterized by the same massive consumption of resources (computers and electricity) that characterizes mining.

Proof of Stake (PoS) still involves an algorithm, and has the same purpose as PoW. It just uses a different process/approach to picking who creates the next block. PoS systems have no block reward. Instead, the creators of blocks only receive the transaction fees in those blocks. The creators of blocks in a PoS system are called Forgers rather than Miners.

While PoS systems still require minor calculations to determine who will forge the next block, the amount of work is miniscule compared to that in a PoW system. Proof of Stake is much more environmentally friendly than Proof of Work, because it consumes much less electricity. If the cyptoinvesting public moves in a "greener" direction, the demand (and market prices) for cryptos that don't depend on Proof of Work will increase. The market has already shown some acknowledgement of this potential trend. For instance, Ethereum's eventual goal is to switch from a Proof of Work system to a more environmentally responsible Proof of Stake system.

Delegated Proof of Stake (DPOS) is a variation on the PoS system. In such a system, a specific number of delegates are responsible for the control of governance mechanisms. Rather than every single holder of a cryptocurrency having a vote in governance (which is both inefficient and difficult to manage), all holders of a cryptoasset assign their voting rights to specific delegates to vote on their behalf. The chosen group of delegates (which varies by cryptoasset) votes on behalf of the entire community.

This situation can be compared to that of holding a traditional stock that pays dividends. Over time, the investor slowly receives additional coins. These "dividends" are either of the original type of staked crypto, or of an alternative crypto that may be used in conjunction with the staked crypto. This passive income can be viewed as an asset distribution and slowly increases the stakeholder's position.

Some well-known cyptoassets that use Proof of Stake include Dash, Pivx, Stratis, OKCash, and Neo. For some of these cryptos, the asset dividends are the core tokens of that project. With Neo, any investor who holds their coins in an appropriate wallet will slowly collect (earn) a different secondary token called Gas.

An example of a cryptoasset that uses a Delegated Proof of Stake system would be the Ark platform. Investors who hold Ark in their wallets will gradually receive additional Ark coins over time. Ark uses a system of 51 delegates for governance issues.

OTHER CONSENSUS SYSTEMS

Although PoW and PoS are currently the two most commonly used types of consensus systems, there are other systems which distribute rewards and act as verification mechanisms for various cryptoassets. Let's examine a few other consensus systems.

Proof of Authority (PoA)

Proof of Authority is a system that can act as a replacement for PoW. It can be effective for private chain setups and is suitable for centralized blockchain projects. PoA does not depend on nodes solving arbitrarily difficult mathematical problems. Instead, it uses a set of "authorities." Authorities are nodes which are explicitly allowed to create new blocks and secure the blockchain. The chain has to be signed off by the majority of authorities, at which point it becomes a part of the permanent record. This makes it easy to maintain a private chain and keep the block issuers accountable. In an enterprise/consortium setting, there are no disadvantages to using a PoA network over a PoW. Proof of Authority is more secure and less computationally intensive. Since blocks are released at specific time intervals, it is more predictable. However, Proof of Authority is not a commonly used system for large public or decentralized cryptoasset projects.

Proof of Burn (PoB)

Proof of Burn is a method for distributed consensus which is not used as commonly as PoW or PoS. In Proof of Burn, miners show proof that they “burned” coins or tokens by sending them to a verified “unspendable address.” Any burned coins can therefore never be used again in the future, because they are sitting in an address from which they can’t be accessed/moved/spent. Burning coins is expensive on an individual level, just like Proof of Work, but it consumes no resources other than the burned underlying asset. Many PoB cryptocurrencies work by burning separate PoW cryptocurrencies, so the ultimate source of scarcity remains the PoW efforts in those other cryptocurrencies. For example, SlimCoin uses a PoB system, and Bitcoin is the currency burned in that system. Binance also burns some of their BNB coins periodically, to help support the value of the remaining coins in circulation.

Proof of Research (PoR)

Proof of Research is a system in which each participant contributes to research by performing computations in the network. Gridcoin, which is associated with the BOINC network, is a good example of this type of system. Incidentally, if you don’t know what the BOINC network is, you should look it up. It has been running for a few decades with dozens of projects around the world, and offers people all over the world the opportunity to donate computer resources from dormant home computers to the scientific community, by having those computers perform calculations for a variety of projects related to math, astronomy, chemistry, biology, geology, medicine, and other sciences. If you’re not interested in setting up your home desktop computer system for cryptocurrency mining, and your computer usually sits overnight with the power on, you should consider installing the BOINC client and contributing to global scientific research.

The network average in a PoR system is similar to difficulty in PoW mining. As the network average hashrate rises, it becomes increasingly difficult to achieve the same "magnitude" (share of the overall hashrate). As such, increasing your computational contribution is necessary to continue to earn the same reward. When the price of a PoR-based cryptoasset rises significantly and more computing power is brought in (raising the overall network hashrate), it becomes harder for a single entity with a constant rate of research contributions to get the same reward.

There are many other unique and esoteric consensus systems that have been developed for various cryptocurrencies. What are some other systems that you’ve heard of, which you think should be included in a future edition of this book? If you have any suggestions, send a DM to CanadianCryptoGuy on Reddit.

CHALLENGES FOR CRYPTOCURRENCY ADOPTION

There are a number of challenges that cryptocurrencies in general must overcome before they will be able to reach mainstream penetration and become useful for the majority of people on a global scale. Here is an outline of what we believe to be seven of the biggest challenges facing cryptocurrencies today.

Difficult to Purchase - It is difficult for many people to buy cryptocurrencies. The safest and most cost-effective place to purchase cryptocurrencies is on professional exchanges, and any time that crypto prices are in a sustained uptrend, many of those exchanges are overwhelmed with requests for new accounts thanks to a global demand which their server infrastructure is unable to handle. In addition, many global citizens face barriers due to age, geographic restrictions, and identity verification, which prohibit them from simply signing up for accounts on some of these exchanges. Alternative methods for purchasing exist, but often they entail extreme fees (ie. Bitcoin ATM's) or they turn out to be scams (buying on eBay or Craigslist). Although the advent of cryptocurrencies may eventually increase financial opportunities and freedom for billions of "unbanked" people around the world, their lack of direct access to buying cryptos is a significant barrier.

Ease of Use - At the present time, it is too difficult to use cryptocurrencies. Storing cryptoassets on exchanges is risky, as many have been hacked. It is possible to move assets from exchanges into various types of wallets: hardware, desktop, mobile, or paper. However, the process of moving assets from exchanges to various types of wallets often requires a level of technical competence which exceeds that of the general public. Many people have fallen victim to scams or hacks, or have made simple mistakes during transfers, leading to loss of funds.

Energy Consumption - Cryptocurrency mining is a very energy-intensive and wasteful process which is proving to be a growing environmental concern. Luckily, there are other low-energy consensus mechanisms which can replace mining.

Merchant Acceptance - Not enough merchants accept various cryptocurrencies as a means of exchange for their goods and services. What's the point of having a currency if you can't spend it?

Fees - Cryptocurrencies need to have extremely low fees in order to disrupt the existing financial system. This challenge has been dealt with by a fairly large number of cryptocurrencies, some of which have fees of less than a penny per transaction. A few are even feeless. However, this continues to be a challenge as some of the main cryptocurrencies require large fees. For example, depending on the global transaction rate at the time, a single Bitcoin transaction can sometimes cost several dollars, which is completely untenable and runs counter to one of the main points of using cryptocurrencies. Also, many people are forced to pay exorbitant fees when converting fiat to crypto.

Scalability - To be truly useful and to satisfy long-term global demand, cryptocurrencies will eventually have to be able to process many thousands of transactions per second. A few are currently capable of scaling to that level, but the majority cannot. Bitcoin is currently only able to process approximately seven transactions per second, which is completely insufficient for mainstream acceptance. Visa, the credit card company, averages many thousands of transactions per second. Ultimately, for a cryptocurrency to be truly useful for everyday purchases on a global scale, it would have to be able to execute tens of thousands of transactions per second (unless it was a niche cryptoasset used for a specific purpose, rather than intended as a general currency).

Security - As mentioned above, the world of cryptocurrencies and cryptoassets is full of scammers and hackers, who have individually and collectively discovered hundreds of ways to steal funds from unsuspecting users. The community needs to work together and move toward better education, self-regulation, and security protocols, in order to protect users and investors. Every time someone is defrauded or has money stolen, it potentially turns them away from ever using cryptocurrencies again, and decreases the likelihood that their circle of friends/family would feel comfortable using cryptocurrencies. This erosion of public trust is unquestionably one of the biggest risks to long-term adoption.

If you're planning to invest in cryptoassets, you should make time to read this book, several times if necessary, until you understand it completely. After that, branch out and do a lot more research. Once you think you understand how everything works, pick the project or projects that you're interested in, and then spend thirty days watching their pricing moves, and the moves of similar projects. Don't invest before those thirty days are over. After that much time has passed, you'll probably have a sufficient basic understanding of the project, which will prevent you from making any uninformed "wrong" decisions as you start out. Many people make the mistake of becoming interested in a specific crypto project before gaining a true understanding of how it works, but then they are reluctant to admit that they made a mistake, so they hold on to an undesirable asset instead of getting out quickly and moving on to better projects. Don't continue holding assets of an undesirable project, in hopes that it will appreciate in value. Recognize your loss and move on to better opportunities. Don't double down on a bad bet.

Most importantly, a thorough understanding of all the information in the Security section of this book is vital before you begin investing. There is no government body to step in and reimburse you for losses when you make mistakes or fall victim to hackers or scammers. Cryptocurrencies are the wild, wild west of investing. You are your own bank, and nobody else is looking out for you.

Section 2 – Security

RISKS OF INVESTING

All financial markets carry some risk with them. This is the price that must be paid in return for potentially earning a return on your investments. Conversely, one can also say that the return earned on an investment is the reward for taking a risk.

Different markets have different risk profiles. Bond markets are generally the safest, especially because nobody expects an entire country to default on their debt, and the risk of a Fortune 500 company defaulting on a bond issue is also fairly low. Municipalities, smaller companies, and many other types of entities can also issue bonds, although such bonds might be deemed to be more risky. Stock markets are usually even more risky than, with Blue Chip companies being less risky than mid-caps, and penny stocks being high risk. ETF's, Forex, and Derivatives markets all have varying risk profiles. In the end, however, there is no question that Cryptoasset markets may be more volatile and more risky than all other types of financial markets.

There are different reasons why investing in crypto is risky. Some of these factors relate to the market as a whole, and others relate to specific projects. Let's examine some of the potential issues.

Issues that are Internal to Projects

At the most basic level, a cryptoasset project needs to be assessed on a number of levels: Technology, vision, team, financial structure, marketing, and a dozen other factors described in more detail in the “Evaluating a Project” chapter.

A chain is only as strong as its weakest link. Something that goes wrong with any number of aspects of a project can derail that project, and with it, your investment. A project not designed properly for scaling can be strangled as usage ramps up. A mistake in the coding can be discovered years into the project, and exploited by malicious actors. Project milestones can be missed when coding challenges prove to be greater than expected. Key developers can lose interest and move on to more exciting projects. Marketing campaigns can backfire.

Any of the above reasons, and many more, can derail a project internally. When that happens, the trading price can suffer and the market value of your portfolio will diminish, sometimes for extended period of time (or even permanently). There are literally thousands of blockchain projects that have been started over the past few years and which are now defunct, with assets no longer trading on public exchanges. To keep things in perspective, google the “dead coins” website.

Competition with Similar Projects

In any market, the "First Mover" usually has a very strong advantage over other competitors. Imagine how hard it would be now for a new social media platform to dethrone Facebook, or for a new search engine to dethrone Google. Even if the first mover has technology that is inferior to new entrants, their “first mover advantage” is usually enough for the entrenched entity to remain dominant.

Critical mass of users is also important. Some systems are designed to work best when large numbers of people are using them. Think about social venues - a crowd attracts a crowd. People want to go where their friends are. If a technology is not widespread in implementation, its usage will not be widespread either. ExampleCoin could be the most innovative new cryptocurrency on the planet, but if no merchants or service providers accept it, it may never gain traction.

When evaluating a project, technical superiority does not guarantee success. Will the project that you're investing in be able to survive in a crowded and competitive space? History shows us many examples of good technologies that were crowded out by inferior products. Just do some research into Betamax vs VHS as a prime example of a good product that was eventually buried by a competitor.

Market Dominance of Bitcoin

For many years, Bitcoin essentially moved the entire cryptocurrency market space. When Bitcoin went up, the entire market went up. When Bitcoin went down, the entire market went down. Eventually, with a strong rise in the number of alternative cryptoasset projects in 2016 and 2017, the market began to partially decouple from Bitcoin. It was possible to see some periods where investment seemed to flow in a wave between Bitcoin and all other currencies. Sometimes, Bitcoin gained strength (and market share) as alternative projects went down, and at other times, the alternative cryptos seemed to gain strength while Bitcoin went down. However, even today (early 2020), Bitcoin still accounts for more than fifty percent of the global market capitalization of all cryptocurrencies combined.

Another phenomena that started to happen with increasing frequency in 2017 and 2018 was the gradual introduction of more "pairing couples" on cryptoasset exchanges. For years, essentially the only way to buy most alternative cryptos was to purchase them with Bitcoin. However, especially in 2017, some exchanges began to offer trading of alternative small-cap cryptos against other coins (especially ETH, Tether, and LTC), or directly against fiat currencies (especially the USD and EUR). This phenomenon further decoupled the price of Bitcoin from the rest of the crypto marketplace. This overall trend may continue in coming years, as more trading options become available and Bitcoin's dominance is further eroded. Note that this doesn't necessarily mean that Bitcoin will drop in fiat price; it just means that Bitcoin's share of the overall crypto markets may decline in percentage terms. Of course, if you're investing, it's always important to consider the performance of your assets in percentage terms rather than just in absolute terms.

Despite the gradual decoupling of Bitcoin from alternative cryptoassets, all future Bitcoin corrections will almost undoubtedly have a negative effect upon the rest of the market. And Bitcoin is no stranger to corrections! In 2017 alone, Bitcoin went through seven separate notable corrections. Looking at a broader time frame, Bitcoin was at an all-time high of around $1200 USD in late 2013, but then dropped precipitously to around $200 two years later. Obviously, it eventually recovered and surpassed the previous 2013 highs, but it took years. Are you willing and financially able to stomach a drop of 80% of your portfolio value for a period of a few years? Remember, the markets can remain irrational for longer than you can remain solvent.

Regulation of Cryptoassets

At the present time, most governments around the world have almost no idea of how to deal with cryptoassets. This uncertainty remains a common theme whether you're talking about ruling governments, central banks, member banking networks (consumer banking), taxation authorities, or accounting firms.

With respect to national governments, a few countries have actively embraced cryptocurrencies and passed legislation to confirm that investors need not fear government intervention. Japan officially recognizes Bitcoin and digital currencies as a "means of payment that is not a legal currency." Other countries have gone in the opposite direction and have stated that cryptocurrencies are illegal. In Algeria, "The purchase, sale, use and holding of so-called virtual currency is prohibited." To be clear, the status of cryptocurrencies is "legal" in most countries, but don't confuse this with "legal tender." More detailed information about the legal status of cryptocurrencies in various countries can be found on Wikipedia.

In the late summer of 2017, rumours swirled about China banning cryptocurrencies, and the entire cryptoasset markets took an immediate hit, deep into correction territory. The Chinese government subsequently banned citizens from participating in ICO's. That was a wise long-term move, in order to protect citizens from scams. If another major nation such as the United States were to take the same blanket approach to all ICO's, the overall crypto markets would probably crash, and it could take a long time for them to recover. Of course, nobody knows what the risk of this sort of event could be. In fact, there was already a fairly significant crack-down on ICO's in the United States in 2018, and the effects were negative for overall market sentiment.

The proliferation of cryptocurrencies has certainly attracted the attention of central and member banks around the world. It is certainly quite possible that central banks could start creating and issuing their own nationalized cryptocurrencies, with the full support of political powers. Some might even say that such a development is inevitable. Such a move could be embraced by many mainstream consumers, especially if such a currency could be used safely and conveniently within the existing banking systems. Nationalized cryptocurrencies could theoretically draw capital away from existing decentralized global cryptoasset markets.

Regulations about the conversion of fiat to crypto (and vice versa) could have a major negative impact upon the ability of users/investors to embrace crypto in today's fiat-based society. If governments shut down fiat gateway exchanges, or banking systems freeze the ability to transfer fiat to and from known cryptoasset trading entities, that would significantly slow the adoption of cryptocurrencies. Gateway exchanges are the weakest link in the system, and an anti-cryptoasset campaign would almost certainly attempt to target this weakness.

Tax laws, depending on the way they are written, can either encourage or discourage trading or investing in cryptocurrencies. In some countries, every single transaction (including crypto-to-crypto) is treated as a taxable event. In a system where direct fiat equivalents and capital/income gains and losses must be determined for every transaction, and then any applicable foreign exchange rates established simultaneously, it is very difficult for an individual to properly account for trading gains/losses and to maintain compliance within the tax system. Criticizing the relevant taxation authorities for this problem is probably a waste of energy. One solution would be the development of accessible and affordable tax preparation software packages that could factor all necessary data into their calculations, including transactions on foreign exchanges, and therefore facilitate the submission of tax-compliant returns.

If a major global exchange such as Binance or Coinbase wanted to help encourage the global adoption of cryptocurrencies, perhaps they could help sponsor the development of such software. In the meantime, tax treatment is a risk in many countries. As tax authorities continue to gain an understanding of cryptoasset markets, and make decisions about how tax treatments will apply to transactions, there is the potential that future clarifications of taxation regulations in some countries will not be friendly to cryptoasset investors.

Global Economic Factors

Global economic developments can affect your cryptocurrency portfolio. What happens to your portfolio when your national fiat currency gains or loses strength again the US dollar? What happens when the US dollar gains/weakens against all other fiat currencies?

What happens when global geopolitical events affect financial markets? If stock markets go up/down, does this affect cryptoasset markets? What about a major stock market correction like "Black Monday?" In general, the second half of 2017 saw a general “small” outflow from traditional markets into cryptoasset markets, but the transfer of funds turned out to be a significant infusion of capital (due to the much smaller size of the crypto markets in comparison to traditional markets). The same trend may happen again during all future upcycles in the crypto markets. Would financial strengthening of traditional markets slow this transfer of capital? What about bond and forex and derivatives markets, would the same apply?

Do trading prices of various commodity markets have an effect on cryptoassets? In particular, think about the effects of changes in the prices of oil, gold, and silver. Although the relationship between these commodities and crypto is much more tenuous, every action in the global financial system has ripple effects upon all other systems.

If there was another global economic recession similar to the Great Recession of 2008, how would cryptoasset markets react? Would there be a "flight to safety" which would result into money flowing into the cryptoasset markets? Or would margin calls in the traditional markets need to be covered, leading to some crypto investors rapidly selling off crypto assets to meet those stock market margin calls?

How do central bank interest rates, national inflation rates, and national/global GDP rates affect the cryptoasset markets? As cryptoasset markets mature and stabilize over the upcoming ten to twenty years, diminishing volatility will be beneficial to investors. However, at the same time, stronger cryptoasset markets will probably also become more subject to effects based upon the vagaries of external global economic factors.

Evolution of Technology

It is quite possible that much more advanced cryptocurrencies may be designed in the future. If a "Crypto 3.0" comes out, it may become a dominant cryptocurrency which pulls market share and value from all existing cryptos. The risk of obsolescence is significant for many current cryptocurrencies.

Black Swan Events

A "black swan" is an event or occurrence, geopolitical or natural, that deviates beyond what is normally expected of a situation. Black swan events are extremely difficult to predict. Black swan events are infrequent, but often have far-reaching or even global implications. Some geopolitical examples of black swan events have been the tearing down of the Berlin Wall, the fall of Soviet communism, or the Arab Spring uprisings. Some natural examples of black swan events would be the 2004 Indian Ocean tsunami, the 2010

Icelandic volcanic ash clouds that disrupted global air travel, or Hurricane Katrina's effect upon the United States in 2005.

It is sometimes possible to predict potential black swan events, although it is not possible to accurately determine the likelihood that such events could actually happen, or exactly when they might occur. We can think of many possible examples of potential natural black swan events. Major earthquakes in western North America could cause part of California or Vancouver to slide into the ocean. A full collapse of ice shelves in Antarctica could raise global sea levels by several feet and displace billions of humans. A major volcanic eruption could disrupt or prevent regional or global air travel for more than a year. A massive solar flare could knock out half of Earth's satellites and electronic systems. A meteor impact could rival the effects of a global nuclear war. Those are just some possible (but hopefully unlikely) examples.

We can also think of several possible examples of potential geopolitical black swan events. There could be a nuclear exchange between the US and a rogue North Korean regime. The assassination of a major world leader could plunge a country into full-scale civil war. A revelation that life exists on other planets, coupled with communications from an intelligent extra-terrestrial species, would completely change our world.

Black swan events do not necessarily have to have a negative impact on humanity, even though it seems that way based on our possible examples so far. One beneficial potential black swan event would be the discovery of a cheap cold fusion process that would essential give the gift of extremely cheap electricity to all of mankind. This would also disrupt global economic systems, although in a different way than most geopolitical or natural disasters.

Although the number of assorted black swan events that happen in any person's lifetime is quite low, these events invariably have major global repercussions. They would affect global economic systems and financial flows, and could therefore affect your investments. A volcano spewing ash in Iceland probably doesn’t seem like it would have an effect upon your crypto portfolio, but what if your main investment was in a blockchain asset used in the global aviation networks, and global air travel was restricted for several months or longer?

Lateral Thinking

The aim of lateral thinking is to solve problems by using indirect and creative approaches, typically through viewing problems in a new and unusual light. In other words, "think outside the box." If you’d like to read an article that "thinks outside the box" with respect to cryptocurrencies, find an article on Hackernoon entitled, “What Will Bitcoin Look Like in Twenty Years.” The point is that nobody really knows what global financial markets will look like in twenty years.

NOTORIOUS HACKS

There are a lot of different meanings to the term "hacking." Hacks can be positive occurrences, such as smart tricks that help one to perform tasks more efficiently. In the context of this book, however, hacks are malevolent events that compromise someone else’s equipment, assets, or finances. If a clever thief figured out a way to bypass the security of a network or computer system, and managed to steal money or cryptocurrencies from your account, that’s a malevolent or malicious hack.

You’ve probably already wondered about the risk of getting hacked. There are different ways to fall victim to a hack. You could be hacked personally, through someone accessing your phone or computer in person (either in person or over the internet). Our “Smart Computer Practices” chapter helps you mitigate this type of risk. But many cryptoasset holders in the past have fallen victim to broader hacks of third-party infrastructure, which have affected software, exchanges, and even entire crypto projects or platforms. There isn’t much that an individual investor can do to safeguard against such risks, other than to use common sense and minimize the exposure of your assets and holdings to third-party entities. In this chapter, we’ll list a few of the very notable large-scale hacks that have affected large numbers of users.

Mt. Gox Exchange, 2014

Mt. Gox was a Bitcoin exchange based in Japan. It launched in July of 2010, and by 2014 it was handling over 70% of all Bitcoin transactions worldwide, which made it the world's leading Bitcoin exchange.

In February 2014, Mt. Gox suspended trading, closed its website and exchange service, and filed for bankruptcy protection from creditors. In April 2014, the company began liquidation proceedings. The company announced that approximately 850,000 Bitcoins (valued at $450m USD at the time) belonging to customers and the company were missing and likely stolen. Although 200,000 Bitcoins have since been "found", the reasons for the disappearance (theft, fraud, or mismanagement) were initially unclear. New evidence presented in April 2015 by Tokyo security company WizSec led them to conclude that "most or all of the missing Bitcoins were stolen straight out of the Mt. Gox hot wallet, over time, beginning in late 2011." There are approximately 127,000 former Bitcoin holders who are listed as official creditors.

As of November 2017, it appeared that the roughly 200,000 Bitcoins recovered by authorities would be used to reimburse people who lost Bitcoins in the hack. However, it appeared that people who lost Bitcoins would be compensated for the initial value of their investments at the time of the loss, rather than taking any other factors (lost opportunity cost, interest) into account. Since Bitcoin has appreciated so much between 2014 and 2017, the value of the recovered coins greatly exceeds the claims of creditors, which is causing significant concern in the bankruptcy proceedings and among unhappy creditors.

Mark Karples, the CEO and former head of Mt. Gox (who was arrested in Japan in August 2015 by Japanese police and charged with fraud and embezzlement), caused great controversy in November of 2017 when he suggested that he would be setting up an ICO to solicit up to $245m in funds to revive Mt. Gox. It appears that the very unfortunate Mt. Gox story is not yet over.

Cryptsy Exchange, 2014

Once one of the most voluminous exchanges for alternative digital currencies, Cryptsy collapsed in late 2015 after months of escalating service issues. Trading was ultimately suspended in early January of 2016, and just days later, the exchange went offline amid claims of insolvency and concealed theft.

The exchange alleged in an early 2016 blog post that it had been the target of a hack in July 2014, an incident that it said cost approximately 13,000 BTC (valued at $7.5m at the time) and approximately 300,000 LTC (valued at $2.08m at the time). The acknowledgement of insolvency and the hacking claim came after months of customer withdrawal delays, comparisons to the already defunct Mt. Gox exchange, and the filing of a class action lawsuit against the exchange.

The exchange ceased trading permanently by the time that the exchange made that 2016 blog post.

The DAO Hack, 2016

The DAO, which stands for Decentralized Autonomous Organization, was a project based upon the Ethereum platform. The intent of the DAO was to provide an entity which was not tied to any one geographic region, nation, or group of controllers, to act as a form of investor-directed venture fund. Various technology projects needing funding would be listed on the DAO network, in a sort of cookie-cutter approach to helping these projects raise capital, instead of having to create fundraising projects from the ground up. Once a project became part of the DAO, various people could support or fund the project. People who owned DAO tokens essentially acted as investors, advisors, board members, and power brokers, all rolled up into one. Projects that got the most support from DAO token holders would raise the most funds. If the projects turned out to be profitable, DAO token holders got to share in the profits on a basis proportionate to their support for that project.

The DAO was decentralized, so it depended on computer code. Although the code was reviewed after being written (and before being released to the public), it was very complex. Once it was released and initialized, there was no way to edit it or turn it off.

Unfortunately, there turned out to be an exploitable bug in the code for the DAO which allowed a hacker(s) to start siphoning funds from the project. On June 16th, funds started to be drained. Over the next few hours, cryptoassets worth approximately $55m USD (at the time) were moved into the attacker's account. Then the attack stopped, temporarily.

At this point, a group of white-hat (good) hackers realized that the only way to stop the attacker from completely draining the DAO would be to steal the rest of the assets themselves, before the attacker could. Eventually, once they had time to deal with everything, those "stolen" funds could be returned to the rightful owners. They did this.

Meanwhile, a very influential group of Ethereum developers, including the founder, examined options. It became apparent that one option would be to "roll back" the Ethereum blockchain, or more specifically, to change the code so the stolen funds were no longer worth anything. The only problem with this option was that it created an enormous ideological rift in the community. The fact that blockchain cryptocurrencies are "decentralized and immutable, not subject to actions of any specific centralized group of individuals," is a very important fundamental tenet for most cryptoasset developers, investors, and supporters. This option was effective, but it ran completely contrary to the ideals of decentralization and autonomy. In the end, it was decided that recovery of the funds was the most important consideration. The Ethereum blockchain was forked, and the stolen funds became unusable.

Shortly thereafter, a new plot twist surfaced. Although the stolen funds still technically lived in a separate fork of Ethereum (the original blockchain), the lack of any support for that chain should have allowed it to die off immediately. But somehow, suddenly, that separate fork was getting mining support, and stayed live. That original blockchain, dubbed Ethereum Classic, still exists and is still traded today. The value of "Ethereum Classic" is much lower than of the "Ethereum" token, but it does have some support among purists who believe that the blockchain should never have been allowed to be forked in the first place. Although the attackers of the DAO never managed to make off with Ethereum ETH tokens, their Ethereum Classic tokens (representing 30% of the total supply of that currency) remain viable today.

The DAO project was wound down immediately and delisted from exchanges. There are a few links to the DAO story in the Security & Hacking section of the Links page on our website.

Bitfinex Exchange, 2016

Bitfinex is a cryptocurrency exchange that was originally operated out of Beijing, but was subsequently listed as being headquartered in a few other jurisdictions. On August 2nd, 2016, it announced that it had been hacked, and almost 120,000 Bitcoins (valued at $72m USD at the time) had been stolen from random user accounts. Trading on the exchange ceased immediately, although not long afterwards, the exchange opened read-only access so individual users could see if their accounts had been affected.

The amount of the attack, while only about a fifth of the coin volume of the Mt. Gox hack, was significant enough to shock the markets, and Bitcoin prices immediately plummeted by about 10%. The dollar value of the lost Bitcoins was significant enough that the exchange was unable to cover the losses of customers.

In an unprecedented move, while the exchange was still locked down and withdrawals or trades were not possible, Bitfinex stated that they would not allow some individuals to suffer 100% losses while other users didn't suffer any losses, considering that the targeted accounts seemed to be selected randomly. Bitfinex said that to remedy the situation, they would confiscate approximately 36% of the holdings of every investor on the platform, to allow them to balance the losses proportionately between all accounts. Their argument was that if bankruptcy proceedings were to be initiated, the same approximate process would be used to liquidate holdings. At the same time, Bitfinex stated that they would issue tokens to all account holders in proportion to the amounts lost. The eventual goal of the exchange would be to buy back all the tokens at the original value of the losses, once they were able to raise the appropriate amount of funding, and thus fully reimburse all account holders (in the long term).

When these "BFX tokens" were issued and started trading (with a face value of one dollar apiece), the market trading rate dropped to only approximately half of that amount, because token holders were discounting the probability that they would eventually get their money back. However, thirty days after the hack, Bitfinex moved to buy back roughly the first 1.2% of the outstanding tokens. This gave confidence to the markets, so the BFX tokens started trading at a less severe discount, and the global trading price of Bitcoin also started to recover.

Approximately eight months after the hack, Bitfinex was able to buy back the last of the outstanding tokens, and then claimed to have reimbursed everyone for their losses. Of course, this didn't cover interest, lost opportunity costs, or discounts to people who disposed of their BFX tokens prematurely. No information seems to have been made public about the blockchain records of the stolen coins, nor of whether those Bitcoins are being circulated freely today.

CoinDash ICO Hack, 2017

CoinDash is a cryptoasset based social trading platform. It held its ICO in July of 2017. On July 17th, CoinDash reported that its ICO website had been hacked, and that the hackers had substituted a different deposit address than the official ICO wallet. People who were subscribing to the ICO, not realized that they were sending their investments to the wrong deposit address, lost approximately 44,000 Ether (valued at $10m USD at the time).

Parity Wallet Hack(s), 2017

Parity Technologies is a group of developers working on a specific collection of open-source projects. Parity itself, also referred to as the Parity Wallet, is an Ethereum client. It is a free software client that was peer-reviewed. The Parity Wallet allows users to interact with the Ethereum blockchain, and includes all traditional wallet-based functions.

On July 19th, 2017, Parity reported that due to a vulnerability in a version of its wallet software, approximately 150,000 Ether (valued at $30m USD at the time) had been stolen from multi-sig wallets. Parity urged all users with any funds in any multi-sig wallets to move their assets into a different secure address immediately. At the time, it appeared that only three wallets had been compromised, but obviously these three wallets held significant amounts of Ether, and there was a risk that more wallets could be drained at any time.

Fast forward several months to November of 2017. Although the initial hack vulnerability from July had been patched (fixed) very quickly, Parity suddenly found itself in the spotlight again. Shockingly, multi-sig wallets were again found to be vulnerable in a much larger hack.

This second Parity hack might arguably be classified as an "egregious error" rather than a malevolent hack, but the effects were the same. Also, it should be noted that this hack was dissimilar to the other hacks discussed so far, because it did not represent a theft of coins. Rather, due to a "user error," approximately $158m USD of Ethereum tokens were locked up and rendered inaccessible. When the first Parity hack vulnerability had been patched in July, a new exploit had been made possible. Basically, there was a section of "library" code which the wallets depended upon for proper functionality. For some reason, certain users had permissions that allowed them to be able to kill the library process (essentially removing the code). On November 7th, a user actually tried this, ostensibly "not knowing what would happen." After the library was killed, none of the affected multi-sig wallets would work anymore, so the assets in those wallets became permanently frozen. Due to the nature of the code, it wasn’t possible to simply "re-instantiate" the library. At the present time, those assets still remain frozen and inaccessible.

Certain analysts who have studied the online logs of the unknown user who killed the library routine have suggested that the act may have been deliberate, or more specifically, a very expensive prank. The user in question who triggered the freeze deleted all of his accounts almost immediately after killing the library.

NiceHash Mining Network Hack, 2017

NiceHash is a cryptocurrency mining marketplace, which acts as a service for miners to rent out their hash rate to others. On December 6th, 2017, their Bitcoin wallet was emptied, resulting in a collective loss of 4736 BTC (valued at $62m USD at the time).

The company made a statement which included, "Importantly, our payment system was compromised and the contents of the NiceHash Bitcoin wallet have been stolen. We are working to verify the precise number of BTC taken. Clearly, this is a matter of deep concern and we are working hard to rectify the matter in the coming days."

YouBit Exchange, 2017

On December 19th, the South Korea based YouBit exchange was hacked, with the thieves stealing approximately 20% of the platform's cryptoasset holdings. It was the second successful attack on the exchange that year, with cyber-thieves having made off with $35 million dollars of Bitcoin in a hack earlier the same year, in April 2017.

The second (larger) attack proved to be too much for the exchange, which was forced to declare bankruptcy almost immediately.

Coincheck Exchange, 2018

At the time, this hack was the largest cryptocurrency hack in history. The Coincheck exchange is located in Tokyo. In late January of 2018, hackers broke into a hot wallet on the exchange, and stole 500 million Nem (XEM) tokens.

The exchange admitted full responsibility for the breach, and conceded that they should not have had so many coins stored in hot storage. The exchange has indicated that it will reimburse all accounts who suffered losses (many of the coins actually belonged to the exchange itself). In the meantime, all of the stolen funds have been flagged, in an attempt to make them untradeable in the future. Most exchanges that have Nem pairings have already indicated that they will permanently block any trading of the flagged stolen coins, as has ShapeShift.

Bitgrail Exchange, 2018

This Italian exchange was the main trading platform for the popular Nano (formerly RaiBlocks) project. The developers of the project endorsed this exchange.

In early February of 2018, after several weeks of throttled or shut-down withdrawals, the exchange stopped trading funds. Previously, the exchange owner (Francesco Firano) had said that the reason for the withdrawal restrictions was due to a new need to comply with KYC requirements. However, on February 8th, he revealed in conversations with developers at Nano that the Nano wallets on his exchange had a serious deficiency: 15m coins were "held" in theory, but there were only 4m actual coins in the exchange wallets. He alleged that the problem was due to either a hack or due to a coding problem in the Nano technology.

After that, it became apparent to users that funds had probably been missing for several weeks, and that Francesco had been using this time to try to cover up and resolve the problem. Although some users were able to convert a portion of their assets to Bitcoin (at a loss) and remove their funds from the exchange, many other users' assets were frozen and could not be recovered.

A criminal investigation resulted. It appeared likely that this could have been either an intentional criminal act by the exchange owner, or gross negligence (rather than a problem with Nano itself). Certainly, the problems appear to have originated with the exchange, rather than with the Nano code. It is believed that user losses, based upon the market price at the time, may have been as much as approximately $157 million USD.

QuadrigaCX, 2019

Quadriga was a well-known Canadian exchange that commenced operations on a very small scale in late 2013. In late 2018, the administrator of the exchange (Gerald Cotten) was reported to have passed away suddenly while building an orphanage in India. The exchange kept accepting new deposits until almost the end of January of 2019, but was not paying out investors. The exchange then announced that they were filing for creditor protection at the end of that month, and investors today are still owed nearly a quarter billion dollars.

Rumours continue to swirl around this set of events. This probably wasn't a hack, but was it a case of intentional fraud? Did Cotten disappear on purpose, and run with clients' funds? If that's the case, then that's a bold strategy Cotten – let's see how that works out for you. Did Cotten's alleged untimely death suddenly expose a massive ponzi scheme? It's even possible that the exchange was hacked and that Cotten had covered it up, to protect his reputation. Investors may never know the truth.

Other Hacks

The list of hacks noted above is just a small sampling of some of the more notorious hacks that have taken place in the cryptoasset world. The take-away lesson here is that you can never be too careful about the security of your investments. If major exchanges with highly skilled InfoSec defense teams can be hacked, then you can too, if you're not careful.

SCAMS & PONZI SCHEMES

"If you didn't expect to find snakes in the grass, then you shouldn't have left the parking lot."

Cryptocurrency markets are the wild, wild west of the financial world. The number of scams in the cryptoasset space is simply staggering. Face it, anywhere there's money, there are people trying to take your money. Thousands of criminals and dishonest people are using all sorts of different schemes to successfully steal funds from unsuspecting investors. Unfortunately, the low education level in the cryptoasset markets, combined with the ability to confuse people with fancy-sounding high-tech terminology, is a perfect breeding ground for fraud.

We'd like to start by saying that you should ONLY ever buy coins from legitimate cryptocurrency exchanges. Don't buy crypto from eBay, CraigsList, personal ads, social media promotions, or any other sort of facility that isn't a major cryptocurrency exchange. Even a lot of the smaller and mid-sized exchanges are highly risky, while a few others are outright frauds. Don't buy crypto from strangers at one-on-one meet-ups. Never click on an advertisement in search results that takes you to an exchange website. Always use a safe bookmark or type in the exchange URL directly, to make sure you're not on a cloned site designed for phishing. Markups and fees at cryptocurrency ATM's are ridiculously high. Many sites where you can buy cryptocurrencies "directly" are scams. There are many sites designed to look exactly like official sites for a cryptoasset, but which are run by scam artists waiting to take your money. Some ICO's, even if they happen to be legal in your jurisdiction, are big scams. Many cryptoassets marketed as "the next big cryptocurrency" are garbage projects.

Falling victim to a scam is different than getting hacked, although the end result can be the same. We'll use this chapter to give you some background about some of the scam projects that have fooled investors. Also, near the end of this chapter, we'll give you what is probably the most important part of this book: A list of generic scams to be aware of. If you read nothing else, at least skip through to that section and review it carefully. And by the way, never ever use a website to generate a seed or a private key.

Trust Nothing Without Verification

A scam is a fraudulent act or activity, usually set up purposefully to take money away from an unsuspecting victim. A ponzi scheme is 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 from financial trading.

The first step to protecting yourself against fraud is to be aware that within the cryptoasset space, probably more so than in any other financial markets, there are a huge number of criminals and malicious actors who will try to separate you from your money. If you understand this, hopefully you'll be cautious with the investments that you make, and with the handling of your assets. The best approach for investing in crypto is "trust nothing without verification." A few hours of research can prevent the loss of hundreds or thousands of dollars of investments.

When it comes to scams relating to specific cryptoassets, some online communities have created their own sets of resources to help ensure that unsuspecting investors do not get scammed. In particular, some Reddit communities have pages that list all known and suspected scams. Here's an example for the Monero cryptocurrency:

https://www.reddit.com/r/Monero/wiki/avoid

Before investing in a particular cryptoasset, you should always try to find a similar page to that one, and learn everything possible about which resources to avoid. This precaution will help you avoid scam websites, non-validated wallets, and unsecure generation of seeds or private keys. Time spent on education and research is unquestionably worth every minute that you put into it. If you understand some historical scams and current attack vectors, you'll drastically reduce the chance that you'll become a victim.

Examples of Cryptoasset Projects that were Scams

Confido - Confido was an Ethereum-based token which raised about $375m USD, but then suddenly, announced that due to "legal problems," they were cancelling the project. All traces of their social media and web presence were erased, and the market cap of the coin collapsed. At the time of writing this, there have been no updates about the project.

Monero Gold - This was a token based upon a common scheme whereby the scammers link the name of a well-known and legitimate project to a "new fork" by adding a second name, such as Cash, Gold, Diamond, or Platinum.

REcoin - REcoin was a project which was allegedly going to invest in real estate deals. It was shut down by the United States SEC in 2017.

OneCoin - This project was marketed as a Bitcoin alternative, until it ran afoul of authorities who realized that it was not a legitimate project.

BitConnect - BitConnect had all the characteristics of a classic Ponzi scheme. For instance, investors' funds were locked into the project for a period of time before the investment could be unwound. As many people predicted, this project crashed in early 2018.

MyCoin - This was a cloud-mining contract site, rather than just a cryptocurrency. It shut down and took investors' funds.

RedChain - This was just one typical example of any large number of ICO scams (which is why they should be regulated).

Links that provide more information about all of the above projects can be found on the "Scams" page of our website. Also, be aware that this is just a very short list that we've come up with, to help emphasize that you can never be too safe. You need to do a LOT of research before you invest in any project, and your best approach is to treat everything with a very critical eye (ie. guilty until proven innocent). There are hundreds of other examples of cryptoasset projects that turned out to be scams or ponzi schemes. Literally hundreds. If you don't believe us, go to the DeadCoin website and check out their Scams section.

Some of the Top Scam Tricks to Avoid

Online Seed Generators: Many, many investors have fallen victim to this scam, for many different currencies. Make sure that you never generate a seed using an online seed generator. Many of these are fake pages set up by criminals. Even taking some of them offline doesn't give you a safe seed, because some of these scam sites simply "generate" a seed offline by picking a seed from a list of compromised seeds that a scammer has created. Only use seed generators that are offline AND that are specifically endorsed by the developers of the project. Incidentally, never trust links on Wikipedia pages either, as a number of scammers have added links to malicious seed generators on various Wikipedia pages.

Fake Websites: If you search for various websites that allow you to buy cryptocurrencies, chances are high that some of the top results will be fake or imitation sites which will take your funds, and you'll never see your money again. This is especially the case with imitation cryptocurrency exchange websites. For example, the major global trading exchange, Binance, only has one site at Binance.com, but if you do a google search, you may find six to eight "fake" Binance sites that have slight variations on the URL for the real website. Be on the lookout for character substitutions in the URL's for the sites, such as a capitalized "i" that replaces the lowercase letter "L", or non-Roman characters in the URL. The simplest way to avoid this scam is to do research to confirm the legitimate URL for the site that you're looking for, then to enter it in your browser as a "safe cryptocurrency bookmark" list. From that point on, ONLY visit the site by going through that bookmark. Of course, someone could create malware that looks for browser bookmarks to major exchanges and edits them, so always do a close visual check on the URL after you reach the site. This doesn't just apply to exchange websites. For example, mymonero.com is the legitimate website for monero wallets. The following are all fake sites: mymonero.co, mymonero.eu, my-monero.org, etc. And wait, did you believe us when we just said that mymonero.com is the legitimate website? If so, you should start reading this chapter again from the beginning. Don't trust us. Don't trust anyone. Do the necessary research to verify everything yourself, before assuming that it is safe.

Fake Google Ads: Related to the above point, you'll probably see fake advertising at the top of search results, which leads you to fake websites. The best option to avoid this is to install a script blocker or ad blocker extension to your browser, such as "ublock origin." A second safe practice is to ensure that you never click on any of these ads. It is very rare for a major reputable cryptoasset exchange to use advertising to attract customers.

Imitation Projects: A common scheme for scammers who have a background in coding, or who merely spend a few hundred dollars to hire a developer for a few hours, is to create a cryptocurrency of their own which links the name of a well-known and legitimate project to their scam crypto, by adding a second name such as Cash, Gold, Diamond, or Platinum. You'll hear of projects such as Neo Gold, Bitcoin Diamond, Bitcoin Silver, and others that are scams trying to capitalize upon the market recognition of the original projects. Stay away from all of these.

Third-Party Resellers of Wallets: If you're buying a hardware wallet such as a Ledger or Trezor, always buy it directly from the manufacturer (or directly from an authorized reseller who is promoted on the Ledger/Trezor websites). Even if there's an extensive wait time due to a back-log of orders, we recommend that you don't purchase from websites such as eBay or Amazon. While the actual devices are difficult to tamper with, and the safety factor should be high if you wipe the device upon receiving it then create your own seeds or private keys, there have been numerous cases of people losing all of their funds because they fell victim to the "pre-configured wallet" scam. If you're going to store hundreds or thousands of dollars on a device that you bought in the mail, there is no reason not to be patient and order directly from the manufacturer, to be safe.

Third-Party Software Wallets: Many people have created wallets that can store a single cryptoasset, or multiple cryptos. However, thousands of investors around the world have lost coins from some of these wallets. If you do google searches, you'll see many stories of heartache from users of wallets produced by Coinomi, Exodus, Jaxx, and others. If you're using a desktop or mobile wallet, the safest solution is always to go to the project's official web page, and use only the wallet(s) that the developers of the project recommend. If this is inconvenient because you need thirty different software wallets to hold thirty different coins, have patience with being inconvenienced. Security should always trump convenience.

Mobile Wallets on App Stores: Despite careful review of apps by Apple and Google, some malicious wallet apps occasionally manage to make it onto the app stores for short periods of time. If you're searching for a specific app, always make absolutely sure that you're downloading the legitimate app, and not a scam.

Websites Asking for Private Keys: Don't ever give up your private key. If you don't own your key, you don't own your crypto. Also, if you're using a blockchain explorer to check the status of funds in your wallet, make sure you always use the public address for the search string, not your private key!

Social Media "Good Samaritans": Many users of social media platforms such as Reddit will give advice to less experienced crypto investors, and usually with good intentions. However, an anonymous user will sometimes offer advice that looks legitimate, but that has a slight twist to it. For example, we've seen posts from throwaway accounts where a user offered advice to help someone deposit coins to the "user's wallet," but then provided the address of a different wallet in the post, hoping that an unsuspecting user would naively send money to the wrong wallet.

Social Media "Sob Stories": Many people like to talk about stories of heartache or bad luck on social media sites. Some of these stories are completely legitimate. However, some of the authors of these stories have "reluctantly" added donation addresses after pressure from sympathizers who want to help out. And unfortunately, some of these stories have later turned out to be completely false. If you want to give money to a stranger on the internet, because it makes you feel better about helping out someone who is down on their luck, we recommend instead that you donate crypto to a legitimate charity such as the Water Project, or to other organizations such as Wikipedia or the Electronic Frontier Foundation or The Internet Archive.

Social Media "Crowd Support": If you want to create a scam crypto project, a key step in the process of luring victims is to create a fake online support community. It isn't hard to create a number of fake social media accounts that can pop up to support or shill a project. It's also pretty easy to hire a bunch of real-world people to participate in a scam. Let's say that you're going to create a scam crypto and you've created a very detailed [private] road map which leads to your eventual exit scam. If your eventual payout is tens of millions of dollars, it's easy to spend ten or twenty thousand dollars to convince legitimate and unsuspecting social media account holders to make posts talking about how ground-breaking and revolutionary your project is. It's also easy to create a bunch of sleeper accounts on sites like Reddit (and even on sites such as Facebook that require more verification) and activate them to support your project. Someone with a trained eye can usually figure out with relative accuracy which accounts are legitimate and which are not, but fake social media accounts are sometimes getting much more difficult to spot. Unsuspecting victims are frequently tricked by this "grassroots support" and throw money at fake projects. Thousands of investors are tricked by crypto project exit scams every month. Never trust the advice of a stranger on the internet. Do your own research before putting a single dollar into a project. If it seems too good to be true, it probably is.

Final Thoughts

Again, if you’re trying to use a website or a wallet associated with a crypto project, always make sure you’re using the resources that are officially endorsed by the official development team of that project. Most cryptoasset subReddit pages have a sidebar that lists the resources that the developers of that project believe to be safe.

SMART COMPUTER PRACTICES

There are a number of very smart computer practices that you can follow in order to minimize your risk of getting hacked, or of accidentally making a mistake of your own that causes you to lose access to some of your assets. Losing access to assets that are sitting in your wallet, because you've lost your private key, is just as final and devastating as outright theft. We have a number of suggestions about smart computing practices in this chapter. However, proper security is not just a set of practices or guidelines: It's a mindset.

If your crypto portfolio is small, you may think that computer security is unimportant. However, your personal identification data is incredibly important too, and usually much more valuable than whatever amount of cash you have sitting in a savings account. Protecting your online identity from being compromised is important in case you have a valuable portfolio in the future, but also simply because being the victim of identity theft is incredibly frustrating and difficult to fix.

You may feel that achieving perfect computer security is impossible, and believe that you're wasting your time because a determined hacker will be able to hack you anyway. Remember that skilled hackers will usually target the easiest victim first, to pick the "low-hanging fruit." Let's put it this way: A skilled intruder can still break into your locked house, by picking the lock or smashing down the front door. That doesn't keep you from taking simple precautions such as locking the door, in hopes that an intruder will look for an easier house to break into somewhere else. Even if your digital security precautions are not perfect, they help make it harder, more inconvenient, or more expensive for someone to hack you.

As you read through this chapter, you may quickly feel overwhelmed if you're not already technically literate when it comes to computers. That's ok. Start learning slowly and implement our suggestions. Baby steps. Let's get started.

Security Through Obscurity

Be aware that some hackers or thieves target victims randomly, while others target specific victims. If you are known to have wealth or cryptocurrency holdings, you're more of a target, even if people don't know how much money you have invested. Therefore, the number one rule in cryptocurrency security is to be discrete about it. If people don't know that you own any cryptocurrency, they'll be less likely to try to hack you, or to try to physically steal your assets!

If you regularly post on Reddit, and you're going to start posting in crypto forums, create a throwaway account that you use exclusively for conversations that mention crypto. This way, you're less likely to have your real-world identity tied to crypto. Use a separate browser for your two identities, so you're less likely to make an accidental post while logged in with the wrong username.

Although thousands of people have been hacked because of weak internet security (which we'll address shortly), there are also a significant number of people who have had cryptoassets stolen by boyfriends, girlfriends, family, and associates. In some of those cases (especially with family members or Significant Others), better security practices should have been in place. In many cases though, the assets would not have been stolen if the first place if the thief hadn't known that the victim owned any cryptocurrencies. So no matter how much you might want to brag about your crypto earnings and holdings, it may be smarter for you to keep that information completely to yourself. Probably the only person who should know about your cryptoasset holdings is your accountant, unless you share finances with your spouse. Remember the first rule of Fight Club: Don't talk about Fight Club.

Setting Up a New Email Address

If you use a single email address for all of your online interactions, and you use the internet frequently, chances are high that at some point your email address (and a password) will be lost in a data breach from some random website that you've used in the past. For starters, if you want to know if this has ever happened to you in the past, you can check the "Have I Been Pwned?" website. But even if your email address hasn't been associated with a data breach or hack at any point, it's highly likely that your email has ended up on a number of spam email lists. No matter how carefully you approach internet security, it is almost inevitable.

Hackers will take email lists, and try to find vulnerable emails to compromise. For example, a hacker could buy an email list of a million random email addresses, then try to sign in to a popular cryptocurrency exchange with every one of those email addresses (using an automated computer script to perform the work). If the exchange gives a message such as "your password is incorrect" rather than "your email address was not found," then the hacker can quickly compile a new shorter list of addresses for all of the emails that apparently have crypto trading accounts on that exchange. The next step is to focus on cracking the password, and that's a surprisingly easy process.

There's a simple solution to deal with all of this: Create a unique new email address for every banking and crypto website that you use! It's easy, and it's free. For example, if your name is Clayton Holmwood, and your real-life email address is **claytonholmwood@gmail.com**, you could create **cholm814hK372@gmail.com** for your Chase Manhattan banking account, **cholm924uM261@gmail.com** for your Coinbase account, and **cholm285Wy925@gmail.com** for your Bittrex account. If you do this, and you NEVER use those extra email addresses for anything other than accessing their one associated financial account in question, those addresses will never end up on a hacker's list, and the chance of someone guessing that such an email address even exists is astronomically low. Your email address won't be hacked if nobody else knows that it exists!

Make sure you enable Two Factor Authentication on each email address (which we'll explain shortly). Incidentally, we picked Clayton Holmwood from a random name generator website. Our apologies to anyone with that name who might end up reading this book.

Basic Password Security

The number of poor passwords being used by the general population is just staggering. Even after years of education about the importance of computer security, many people still choose passwords such as "1234" or "password," or things like their spouse's name. Or a family member's name. Or a pet's name with a couple digits added. "Social engineering" hackers rely on this kind of foolish approach to computer security. So the very first step to better security is to always pick a password composed of random alphanumeric characters.

Always try to include a mix of characters that includes at least one of each of the following types of character: A capital letter, a lower case letter, a digit, and a punctuation mark. By doing this, a hacker who is trying to use a powerful computer to "brute force" a password will need to try approximately 72 different options for each character, instead of just 26 options when someone sticks only to lower case letters. In a very simple four-character password, a full alphanumeric password with punctuation options gives rise to almost 26.9 million different possible passwords, rather than just 450,000 choices if the user sticks with just lowercase letters.

When it comes to passwords, length matters. As the length of the password increases, your password quickly becomes exponentially more secure. By using the four types of characters mentioned above, every single extra digit that you add to a password makes it 72 times more complex. Let's look at an example where somebody is trying to be proactive, and makes a password of twelve random lowercase letters. It would take a supercomputer a moderately long time to crack this, because there are about 95 quadrillion different options. But by using a mix of the four character types, you instead have 1.94 x $10^{\wedge 22}$ different options. If you don't know math, don't worry. Let's just say that this number is about twenty million times as hard to guess as the other 12-letter password that used only lowercase letters. If a website allows it, the authors of this book always prefer to use passwords that are between twenty and thirty characters long. Nobody will EVER guess those. Even someone in the future with a quantum computer would probably just walk away and find something better to do.

Always use a different password on EVERY website. This is extremely important. It's also very hard. People like to pick passwords that they can remember. Picking a password that you can remember is extremely poor computer security. If you find that this is too much of a challenge for you, you can always pick one easy "throwaway" password for all of the common public sites that you visit, a fairly complex (and unique) password for your email, and a complex (and unique) password for each financial, crypto, and banking site. Yes, it's annoying to have to remember and secure all of these passwords. But it's also annoying to open up your bank account or your crypto wallet and find that it's empty.

In some cases, keeping track of your passwords is very challenging. For instance, we regularly visit over two hundred different websites. We have different random passwords on every one of those websites! One good way to keep track of everything is to use a "password manager." Just make sure that you keep two backups of the data file from your password manager. A paper backup of the master password is important, and a digital backup of the entire data file is important. Make sure those are stored in a very secure location, preferably with a copy off-site in case your home burns down. Another option is to create a text file of all your passwords, then to encrypt that file using encryption software such as GPG (and of course, store a backup of that encrypted file someplace secure).

You may think that a password manager is risky, because if someone gets your master password, they'll then have access to every one of the sites that you visit. Yes, we acknowledge that this is a risk. However, since a password manager allows you to use different passwords on every website, at least you're lowering your risk portfolio with respect to third-party hacks of those websites.

At this point, you may be thinking that this is a lot of overkill. However, for proper computer security, you need to put in some serious work. Even if you can't do everything that we've suggested above, do as much as you can.

Following good computer security protocols is a pain in the ass. But it would be much worse for you to have your identity stolen, or your financial assets stolen.

An alternative to random characters in your passwords, if a website allows for a long password (say 30 characters or more), is to type in a phrase. This type of phrase is often referred to as a pass phrase. A good pass phrase can be easier for you to remember than groups of random characters, but if it is fairly long, it is very effective at preventing brute force attacks, especially if the phrase is unique to a single website. An example of such a phrase could be, "ihatethecolorofmyneighborshouse" or anything like that. That password, due to its length, is an extremely secure password as long as you don't use it on more than one site, although unfortunately, many websites don't allow passwords to be that long. But that's changing slowly! Whenever we discover a website that doesn't allow passwords of at least 32 characters in length, we email the administrator of that site and respectfully suggest that they change their code to allow for longer passwords.

It goes without saying that if you write down a list of passwords on a piece of paper, and leave it in a desk by your computer, you're putting yourself at risk. If the passwords are complex, as outlined above, you've probably protected yourself again online hackers. However, you can still be vulnerable if a physical intruder or a family member finds that list. At the very least, hide it in a book somewhere. And again, have a backup copy in a sealed envelope in a safety deposit box or similar secure off-site location, in case of a fire or other natural disaster. Literally millions of dollars of cryptocurrencies have been irretrievably lost in events such as the California wildfires, simply because people didn't keep backups in secure off-site locations.

Two Factor Authentication (2FA)

Two factor authentication is a security protocol whereby in order to access a system, a user must have more than just a username and password. The user must also possess a second form of identification or verification to make it more difficult for anyone else to bypass the password security for the account. 2FA is usually tied to a physical device that a person carries with them, such as a special type of USB key, or a cell phone that can receive a text message, or a mobile device with an “authenticator app” that provides time-based authentication codes.

We need to be very clear about one big risk immediately. Text-based (SMS) authentication is slightly better than not having any 2FA at all, but it is still highly risky! Hackers are frequently able to trick mobile service providers into allowing a person’s phone number to be "ported" to a different phone. This even happens (surprisingly often) when an account is flagged with a "do not port" instruction given by the customer, and sometimes even when a provider has a house rule to restrict porting. Remember that a lot of mobile phone company employees don’t really care about a stranger’s security, or they fall victim to a good social engineering attack. Perhaps a hacker calls the Support department and has your name and basic identity information on hand (which is easy to find on the internet), and she gives a story such as, "Help, I dropped my phone in the toilet earlier today, and just bought a new phone, and I need to get my old number back as quickly as possible because my daughter is expecting a baby right now, and she’s already in the hospital in Dallas!" If the hacker can provide all of the basic personal details for the account, such as the address and phone number and birthdate, chances are high that the phone number will be compromised.

Once a phone has been ported to a new number, the hacker can make phone calls and send/receive texts using your number. Even worse, any text-based 2FA is immediately broken. If the hacker has also figured out your email, then he/she can log in. The 2FA service will send an authentication text, and the hacker then bypasses the 2FA and accesses your account. You're screwed. This is why SMS-based 2FA is a very risky security protocol.

To be fair, 2FA in general is not weak. In fact, it's highly recommended. However, having "device-based" 2FA is exponentially more secure than SMS-based 2FA. By far the most common type of device-based 2FA is to use an authentication app, such as Google Authenticator or Authy. Both of these are highly rated. If you're downloading either from an app store, be absolutely certain that you're downloading the legitimate app, rather than an imposter!

The way that an authentication app works is this: When you turn on 2FA for a website that you use, such as Gmail or a cryptocurrency exchange, the website will generate a unique key for you. That key will be presented on the screen in two formats: A text based version, and a QR code version. Basically, the code will look like a short private key, so it might hypothetically look something like this: XY4HF78HS93LKV82934H12PA. You can then open the authentication app on your phone, and either scan the QR code with the phone's camera, or manually type in the text version of the key. The key is then permanently hidden in your device. You may have to type in a name for the website associated with the key (to clarify exactly which site the authentication codes are for), since the authentication app can simultaneously hold many different keys for a number of different websites. So for example, you might want to label a certain authentication key as "personal gmail account," and a second key as "gmail account for coinbase account," and you might label another key as "coinbase account." From that point on, whenever you have your authentication app running, a six digit number will be displayed in large text for each different website’s key that you have entered. Every website’s key will be a different six-digit code number. There will be a small thirty-second countdown timer beside your code, and after the clock has run out, a new (different) six-digit code will be displayed. Your six-digit code is ONLY valid for the duration of the thirty-second clock. So when you go to sign into a website on which you’ve enabled 2FA, you’ll typically enter your username and password, then you’ll be taken to a second screen which asks you to enter your authentication code. Bring up your codes on your phone. It takes a few seconds to type in the code, so if your thirty-second timer is almost expired, wait a few seconds until a fresh code comes up. Once that new code is displayed on your phone, type the six digits into the website, and as long as the code on your phone is correct, you’ll be allowed to log in.

With device-based 2FA, even if a hacker on the other side of the world knows your email address, and knows the password for your account, they won’t be able to get into your account unless they physically have your phone in their possession. Of course, losing your phone is a big risk. If someone finds your phone, they’ll have your authentication codes. However, they presumably won’t know your password (unless you’ve stored it in your phone, which is risky), so they still wouldn’t be able to access your 2FA-enabled account.

The biggest risk with enabling 2FA is that many people have lost their phones, or had phones stolen, or dropped their phone in a toilet. In all of these cases, you may have a big problem because you no longer have access to your authentication codes. In some rare cases, website Support teams have eventually agreed to turn off 2FA, but this process usually involves weeks of delays and submitting a large amount of documentation to reassure the website support staff that it’s really you, trying to get into your own account, rather than a hacker. Some website support teams simply refuse to assist cases like this. And for some websites, if you didn't provide extensive documentation (like photos of driver's license or passport) when you signed up, they have no way to match your request to the account. You don't want to be put into this position. Thankfully, there's a backup option.

2FA can be enabled on multiple devices. For instance, if you have a spare older cell phone, you can enable 2FA on that phone too. After you've done that, lock it in a safe and forget about it. The phone doesn't even need to have an active mobile connection. You can set it up using a WiFi connection, and once the authentication app is running, it doesn't even need the WiFi connection anymore. The only trick is that when you're trying to set up multiple devices with Google Authenticator, you currently have to enter the initial authentication key manually on each device, because if you do it by scanning the QR code, the app immediately moves on to the next screen and doesn't let you scan the code with a second device. This leads to the next important security step: Save a copy of your initial setup key.

There is no time limit on the time that you're given to manually enter your authentication key, if you are adding a new website to the app. Nor is there any limit to the number of devices that you can add the key to (remember, you can add the key to an offline phone). If you want to create a backup by adding your 2FA key to a second older phone that's stored in a safe in your bedroom, or in a safety deposit box at your local bank, that's great. But you can also simply store all of your text 2FA Other people prefer to store their backup codes on a USB key that they store in a safety deposit box. Some people even go to the precaution of encrypting that key.

If you've decided to add 2FA to a backup phone, and you've already set it up on your existing phone at a previous time, you might have a temporary setback. If you scanned the QR code when you activated 2FA, you probably didn't also write down the text version of the code, so you probably don't know your authentication key for manual entry. In that case, you can log in to the website(s) in question, turn OFF your 2FA temporarily, then turn it right back on. The website will then generate a new and different authentication key for you. This will render your old key on your old phone useless, so the next step is to delete that old key from your phone. At this point, you can write down your text version of the new authentication key, and manually enter it into both devices.

There's one last important thing to remember. On most phones, if you lose/upgrade the phone, and restore all your apps to a new phone using a backup app/system, all of your old apps (including your authentication app) will usually be restored on the new device in a seamless automatic process. Many of your passwords will also be transferred to your new device. However, even though the authentication apps may be reinstalled automatically, your authentication keys are NEVER moved and cannot be recovered. This is why it's really important to save a backup of your original authentication keys in a secure location. If you've lost access to your old phone, and don't have your authentication keys backed up somewhere, you're probably screwed.

Transactions Over WiFi, and Using VPN's

Using public WiFi is risky. Whether you're in an airport, coffee shop, or hotel, there's always a chance that there could be a hacker within WiFi range, casually checking out activity on the network. Remote attacks are also possible. If you're frequently in situations like this, we recommend that you use a VPN service to help protect your wireless communications. The problem, however, is that there are literally thousands of VPN's out there, and many of them are not really that secure. In fact, some VPN's may even be worse than an unencrypted connection, especially if you happen to live in a relatively non-hostile WiFi zone in a remote small town with nobody around you! We recommend that you do a lot of research before picking a VPN. Be careful, because many of the top-ranked online articles that review VPN's are sponsored by some of the VPN's themselves, so they might be very biased. Check out a wide variety of reviews before you make a decision.

We feel very reluctant to advertise any one particular VPN. However, knowing how daunting a task it is to choose a good VPN, we'll admit that we usually use one called Private Internet Access (PIA). We'll also clarify right now that we have no direct or indirect association with PIA, and we're not receiving any compensation to say that we think they're one of the lesser evils out there.

PIA is not perfect, and depending on your priorities, you may find other providers that you prefer. So far though, PIA has been pretty good for us. Having said that, nothing is without risk. What if an employee at your VPN service is a hacker, and is able to monitor traffic passing through your secure connection? What if someone else sitting nearby in the same coffee shop is skilled enough to get around the VPN's security connection? What if the VPN you're using temporary drops the connection and goes to unsecure traffic, and you don't notice? These are all non-zero risks. Hopefully the chances of getting hacked in any of these ways are not very high, but you can never be too safe. Treat public WiFi connections as an unacceptably hostile environment.

For us, the best security approach is to make sure that we never access financial or crypto accounts from public WiFi. Try to make sure that you only access these sites on a secure home-based connection. Even if you're accessing important sites through your phone's cellular connection, there is a slight risk. It's possible for hackers to do packet sniffing, to observe internet traffic passing through a network. It's even possible (and not that expensive) for hackers to spoof a cell tower, which means that all of your mobile data transits through their compromised pipeline before connecting to a real tower. If they're doing that and they see your passwords or your private keys going by, you could be compromised. Thankfully, for some crypto-related services (such as mobile or desktop wallets), the private key never actually leaves your device, so it can't be seen passing through the internet. In this case, if you're able to create the private key on a secure and clean device which is offline, you're probably fairly safe.

If you're going to store crypto on a mobile device, and the monetary value is more than just "petty cash," maybe you should consider buying a cheap new-in-the-box phone and don't add ANY apps other than your crypto wallet to that phone. Even though mobile devices are generally less secure than desktop devices, a brand-new phone with no past usage may be much safer to use than your two-year old laptop that might have picked up malware from one or two of the thousands of sites that you've visited. Buying a new low-end $99 phone may be more cost-effective than spending $300 or more on a new laptop that is intended to be used solely for crypto. But then again, if you're going to be storing crypto funds worth much more than that, you shouldn't put yourself at risk just to save a few hundred dollars. This may not apply to you if you're only thinking about investing a few hundred dollars into crypto, and if you can afford to lose that investment. If you're considering investing a few thousand dollars though, you absolutely need to minimize or eliminate any possible attack vectors.

Router security is extremely important. Unfortunately, unless you're very tech-savvy, you'll look at routers as mysterious black boxes. You'll buy a standard consumer router, plug it in, nervously set up a network name and password, and hope it works. However, setting up a secure router is much, much more complicated than that.

There's a great router security site to be found at this link:

https://routersecurity.org

However, don't be disheartened if you go to that site and quickly realize that you're not qualified to do everything that the site suggests. See if you have a tech-savvy friend who can help you out. If you thought that cryptocurrencies were complicated, they've got nothing on router security.

Using a "Clean" Computer

We've already hinted at the value of having a machine that isn't infected with malware or viruses. Having worked in IT, we've frequently been stunned by just how much garbage accumulates on most peoples' computers. The average one-year-old computer is riddled with viruses, spyware, and malware, unless the user is especially security-aware and careful.

For starters, never click on an attachment in an email unless you know exactly what it is. We even question the attachments that come to us in emails from known friends, especially if the file isn't something that we were expecting to receive. Executables are completely off-limits, although most malware doesn't spread that way (at least not since the early 2000's). Documents, spreadsheet files, compressed folders, and some other types of files can contain malicious macros. Even some types of media files are dangerous. If you don't know what it is, don't open it. Even if you trust the source, it is possible that the sender's machine is unknowingly affected.

Email attachments aren't the only risk. Although they used to be the most common attack vector, there are a number of other weaknesses. Malware can be attached to torrents that you download, or hidden in mobile apps that have accidentally been vetted by Google and Apple as "safe" apps. Free software frequently has hidden payloads. And this may really dismay you, but a lot of public web pages have malicious scripts hidden on them. Even legitimate sites carry this risk, because the sites can be hacked and malware added without the sites' owners finding out. Advertising is also a problem, as malware can accompany ads on sites. Do some research into "malvertising," and you'll see what we mean. Frankly, the internet is a terrifying and unsafe playground. The more that you start to learn about these risks, the more surprised you'll be. Incidentally, don't think that if you have a Mac or an iPhone, you're immune. Viruses and malware also exist for Apple's products.

Even if you're not trading cryptoassets, it's very useful to spend time researching ways to prevent your computers and mobile devices from being infected with malware and viruses. This is simply a wise life decision. It's not just crypto that is vulnerable. Your traditional financial assets (online banking) can be vulnerable, and even more importantly, your personal identity information can be stolen. Identity theft is a very serious problem, and if your identity becomes compromised, you're going to have a lot of headaches to deal with in the future. You wouldn't leave a nice sports car parked unlocked in a seedy urban neighbourhood, would you? Then why would you leave your computer open to serious security risks? As mentioned, the internet is a cyber war zone, and good security is a mindset. Know and follow safe computing practices.

Let's assume that your regular computers have the potential for being compromised. What's your best option? Well, if you are tech-savvy, consider setting up, learning, and using a Linux machine. They are far more secure than Windows and Apple systems, and less susceptible to viruses and malware. If you're really comfortable with computer technology, you can even set up a version of a Tails operating system (Linux based) on a portable USB key, which is only ever used on an offline computer. This may be taking security to paranoid levels, but for some people with considerable investments, it's a smart choice. If you're not comfortable with Linux, another option might be to purchase a brand-new "throwaway" laptop (don't throw it away!), and use it specifically for your crypto activities. If you never use it to read emails, and never visit websites other than the half dozen key crypto sites (exchanges) that you may need to use, that laptop should remain fairly safe, especially if it is restricted to a secure home connection.

If you want to be especially cautious, don't even check price quotation websites with your special-purpose computer, not even once. For example, can you imagine the systemic risk to the cryptocurrency ecosystem if hackers were able to successfully embed a malicious keylogger script onto a website such as CoinMarketCap? Think of how many millions of peoples' accounts might be compromised within hours.

Going back to basics, don't click on unknown links on websites either. If you hover over a link with most browsers, the destination URL for that link shows in full text down in the bottom left of your screen (on desktop browsers). Always double-check this critical piece of information before you click. If there's a link on a sketchy website that says "www.bittrex.com" on the screen, but the URL on display in the bottom left says http://www.bitttrex.de then you will know that something fishy is going on, and you can avoid that link.

Be wary of links in Slack channels, and similar chat sites. We find Slack to be particularly bad. If you join a Slack room, you'll often start getting email notifications which say that you "must upgrade XXX to prevent losing coins" or something like that. Trust nothing.

Using Anti-Virus and Anti-Malware Software, and Script Blockers

It goes without saying that your computers or mobile devices should have anti-virus and anti-malware software installed. This is basic Computer Security 101 material. Do some research to figure out which programs are the best. As with most other things, different software packages perform certain tasks better or worse than other packages, so you'll have to figure out what's best for you. Free protection embedded in the operating system of your computer (such as Windows Defender) isn't perfect, but if you keep it updated properly, it may be a viable option. It's certainly better than nothing at all! Set up this software to update its virus and malware definitions (and do a full scan) on a daily basis.

If you're trying to figure out the difference between malware and viruses, a virus is a type of malware, just as a Dodge Dart is a type of automobile. There are lots of different types of malware though, not just viruses. Other types of malware include trojans, worms, adware, keyloggers, and spyware. Being on top of computer security means that you need to understand computers fairly well, and be able to recognize the different risks involved.

One security precaution that we feel is especially important is to ensure that you have a good script blocker extension in your browser. As mentioned earlier, many web pages run scripts. Some do so unknowingly after being hacked. Scripts (active computer code) have the potential to install malware on your computer. When you have a good script blocker installed in your browser, and you visit a website, the script blocker will warn you if the page is trying to run any scripts other than basic safe website languages such as html. The blocker will prevent all scripts from running until you've decided whether they should each individually be allowed to run, or be blocked. You can allow or disallow each script for the current session only, or on a permanent basis. Your choice.

In this day and age, it's inevitable that most complex modern websites will have some scripts on them, and you'll probably have to have a bit of faith. Even most cryptoasset exchanges have scripts on their websites, usually to enhance functionality and security. In general, however, the fewer scripts that you allow, on the fewest number of websites, the safer your computer will be. We've been to sites that are simply ridiculous. A good example would be trying to watch a video on a CNBC website and finding over 70 scripts on a single web page. If it's not necessary, and you're truly concerned about your computer's security, navigate away from that page. You don't really need to watch that video.

Using Encryption

Obviously, one of the first security steps that you should take with any specific device is to make sure that a password is needed to log in to the computer, or a PIN code is needed to get into the mobile device (or preferably, even stronger protection). As with other security matters, a stronger password is significantly more beneficial than a short and simple one.

What would happen to you if your laptop got stolen? Do you have valuable information there that you don't want a thief to have access to? Do you store all your passwords on your laptop? Would someone be able to access all of your email accounts, bank accounts, and crypto accounts? If so, you're exposed to a big risk that you need to deal with!

One option is to make sure that you never let your laptop out of your sight. Of course, this approach isn't convenient. You probably don't want to take your laptop to bed, or to a nice dinner, or into a movie (well, ok, sometimes we do). Let's use a better example: What if you get mugged? Now you have a problem. However, there's a solution: Encryption.

It's possible to buy encryption software that will protect the contents of your laptop or computer. You can encrypt specific files, or you can encrypt specific folders, or you can encrypt the entire device. Be aware that whole-disk encryption is a great solution when you want to protect a single device (which is often going to be the case in the crypto scenarios that we're currently envisioning). However, if you're trying to share encrypted data over the internet with other users, you'll possibly focus on different types of encryption software.

For many years, the PGP/GPG (Pretty Good Protection) software was the gold standard in encryption. It's still a very popular choice, although there are other packages available. Again, do some extensive research to see what package appeals to you, as different packages have different features (such as 2FA or other options). We won't delve into device encryption any further here, but we do strongly recommend that you consider using device encryption if your laptop has sensitive data or gives users access to any type of financial assets. Even if you always leave it at home, you could be vulnerable if there's a break-in.

ADDITIONAL SECURITY FOR PRIVATE KEYS

If you don't own your private keys, you don't own your assets. You should NEVER ever share your private key with anyone.

Do NOT Share Private Keys

Sharing your private key (or keys) is like giving a pile of cash to a stranger and saying, "Here, hold my money while I just go hang out at the local pub." No, actually, that's a bad analogy: A stranger might be honest and not run away with your money. A better way to emphasize this point, which will resonate with people who have little faith in humanity, is to point out that giving other people your private key is about as wise as throwing all of your cash into the ocean, off the back of the Titanic.

Don't give a private key to people who are teaching you how to work with cryptoassets. Don't give a private key to online support staff or exchanges. Don't give a private key to your brother-in-law, or girlfriend, or bank manager. The only way you can keep a private key secure is to make sure that you never share it with anyone. We're not saying that you shouldn't keep a secure backup somewhere! But if you have any significant amount of funds associated with a private key, then the only backup you might want to consider is something along the lines of encrypting it into a digital file that is placed on a USB key locked in a safety deposit box at a bank. You can never be too paranoid.

Do NOT Share Seeds or Seed Phrases

Same thing, same risks, same warnings. The same comments about keeping private keys to yourself also apply to seed phrases, and to the seeds that they generate. If a seed or a seed phrase can unlock your wallet, you need to make sure that nobody else ever has access to this information.

Generating a seed online is as bad as sharing a seed. Why? Because a lot of online seed generators are malicious, and designed by hackers. So even though you might not realize it, you may be sharing your seed with a criminal. Always generate seeds offline, and only with resources endorsed by the official developers of a project.

Do NOT Share Pass Phrases

Are you starting to sense a theme yet? If you use some sort of pass phrase to access a cryptoasset wallet, you should never share that, not even with friends and family. Sharing a pass phrase to a wallet can lead to unexpected loss of funds if someone decides to steal your assets.

Final Thoughts

This is one of the shortest chapters in this book. This was on purpose, so we could get right to the point, and not risk minimizing the importance of the message. When investing in cryptoassets, you are your own bank. Nobody else is looking after your interests. Never forget this lesson. Come back to this book a few weeks after you've read it, and re-read through the Computer

Security and Scams & Ponzi Schemes chapters to make yourself as aware as possible of potential weak links in your personal security protocols.

EXCHANGE SECURITY

Cryptocurrency exchanges are extremely tempting targets for cyber-thieves, as they hold enormous amounts of assets. Most exchanges therefore have highly skilled teams of IT specialists and security defense mechanisms to help guard against hackers, although many exchanges have been proven historically to have had insufficient defense mechanisms in place. In this chapter, we will discuss what you (as an account holder) can expect to encounter in terms of security requirements to open an account on an exchange. We will discuss what happens when an exchange is successfully hacked. And most importantly, we will discuss the issue of whether it is safer to leave your coins on an exchange, or to move them to a hot wallet, or to store them in an offline cold wallet that is completely under your own control.

Opening an Account on an Exchange

The process of setting up an account on a cryptoasset exchange varies from exchange to exchange, and is also affected by the country or countries that the exchange is registered and operating in. However, the overall process is similar on most exchanges.

First, you will need to set up basic account details, such as your email address and choosing a suitable password. In a few minutes, we'll give you some suggestions about "best practices" to follow.

On some exchanges, you may be asked to pick a username. On other exchanges, you may be given something such as a special "Account Number" or "Client ID" that you'll use to sign in.

You'll probably be asked if you want to enable Two Factor Authorization (2FA). It is very important that you do this. Many exchange account holders who haven't taken advantage of 2FA security have had their accounts successfully hacked.

You may be given the option of verifying your real-world identity. In other cases, the exchange will force you to verify your real-world identity. If you're trying to trade on an exchange anonymously, you may prefer not to submit to this verification. However, remember that the majority of blockchain transactions (except perhaps for Monero or Z-Cash) can be traced, so hiding your real identity on your exchange account probably doesn't do any good if government blockchain analysis correlates your identity to a transaction further down the line. Our recommendation is to always take advantage of identity verification if it is an option (unless of course you're a libertarian, which some of you will be).

Verifying your identity is a complex task. You'll need to have a camera that takes good quality digital photos. A high-quality camera on a mobile phone is usually the best option. Most exchanges will ask you to submit at least two types of photos that can confirm your identity. The first photo will be a high quality photograph of a major type of government-issued identity card which includes a photo, date of birth and address information. This ID card must not be expired. Usually, a good photo or color scan of a driver's license or passport is required. If you don't have a driver's license or a passport, you may be out of luck. This will be a barrier to trading for many people. In some cases, a government-issued identity card can replace the driver's license, so for example, you might be able to use a card that shows that you're a member of your country's armed forces.

The second piece of identity verification photo that you'll often be required to submit will be a color photograph of yourself, showing your face clearly, holding the passport or other government document that you submitted in the previous step, and also holding a sign with a piece of paper that clearly shows additional handwritten information (such as your name, the name of the exchange that you're submitting the information to, and the current date). We're not kidding! This can be very tricky, especially if you're by yourself. It's difficult to hold an identity card and a paper sign and take a selfie, all at the same time. By the way, if you're worried about the security of your personal identification information, you should layer some sort of unique watermark onto any ID's that you submit to exchanges, so if something goes wrong in the future, you can at least figure out which exchange caused the leak.

It's very important that the scan/photo of your identification card is high quality and readable. The exchange needs to be able to clearly read the text on the card. It's also very important that the photo of yourself holding supporting documentation is also very clear and high resolution. Make sure that you take the photo in a brightly lit area, to enhance the quality. If someone else can take the photo for you, and you're using a phone, ask them to take the photo with the higher quality camera on the back of the phone, rather than the lower quality camera on the front-facing (selfie) side. If someone else takes the photo, make sure they are close enough to avoid extra "useless space" in the outside portions of the photo. Many people have had their identity verification declined because the photos they submitted were too dark, or of low quality.

In late 2017, most cryptoasset exchanges were facing a huge backlog of support tickets and new account registrations. Some exchanges stopped accepting new account registrations, to allow them to catch up on the backlog and to properly service their existing clients. Thankfully (?) the market price of all cryptocurrencies crashed hard starting in January of 2018, and the amount of new account sign-ups dropped precipitously. Exchanges were able to get their houses in order, and get caught up with all requests for new accounts.

As of today, the process for signing up for a new account is usually fairly quick. On some exchanges, you might be able to get a new account approved within 24 hours or less. On other exchanges though, even though the support pages may say that the verification process will take a few days, expect that in reality, it might take several weeks before your identity verification is processed. Likewise, if you have a problem and need to contact a support team, expect to potentially wait for several weeks for an issue to be resolved. Even today, some of the most "reputable" of licensed (and government-approved) major exchanges (such as Coinbase) may take much longer to respond to some support tickets than they should, which inevitably causes a huge amount of frustration among their user bases.

When picking an exchange to register with, you'll probably want to consider a few different factors. Is the exchange in your own country? If so, it may be easier to get support tickets resolved due to legal options. A customer doesn't have a whole lot of leverage when it comes to an overseas exchange. What are the fees on the exchange? Different exchanges have different fee rates for buying, selling, and transferring cryptos, and for funding the account with fiat or withdrawing fiat. Does the exchange act as a fiat gateway? Some exchanges are crypto only, so no matter if you have an account on one exchange or six, you'll need to ensure that at least one account is on an exchange that takes traditional fiat currency and lets you buy cryptoassets with that fiat money. Does the exchange accept customers from your jurisdiction? American citizens are prevented from opening accounts on a large number of foreign exchanges, for various reasons. Citizens from certain countries, or who have been flagged as "problem individuals" for any of a variety of reasons, may not be able to open accounts on American exchanges such as Coinbase and Bittrex. Does the exchange that you want to use offer trading in the particular cryptoasset(s) that you want to buy? Some exchanges have very limited trading options. For example, if you want to buy a lesser known crypto such as Everex, you won't find it on Coinbase.

It is useful to review customer feedback about various exchanges, by using sources such as Reddit. Most exchanges have their own subReddits on that site. However, it is also important to remember that a person is far more likely to post a negative review than a positive one. That's just human nature. Consider it inevitable that every exchange will have some negative reviews. Also, during any periods when crypto prices are increasing rapidly and new registrations start to shoot up, the number of complaints about even the "best" of the exchanges will no doubt be quite high.

Some of the larger exchanges in the world (in early 2020) as ranked by daily trading volume, include the following: Binance (Hong Kong), Bittrex (US), Bithumb (South Korea), Bitfinex (Hong Kong), Coinbase/GDAX (US), Bitstamp (UK), BitMex (Seychelles), HitBTC (Denmark), Coinone (South Korea), ACX (Australia), and Gemini (US). Always investigate the reputation of an exchange before deciding to trust your funds to that exchange, just as you would research a bank before opening an account. It is common for many cryptoasset investors to open accounts at several exchanges.

Protecting Your Exchange Account

There are five main components to protecting your exchange account: Using a secure and perhaps unique email address, using a strong password, enabling 2FA protection, verifying your identity on the exchange, and following other best practices when it comes to general computer and online security. Most of these items have already been discussed in far more depth in our Computer Security chapter, but we'll do a quick overview here too.

Using a secure email address is important. If someone is trying to hack specifically into your account on an exchange, and have done any social engineering legwork, they'll probably know your usual email address(es) and will presumably attempt to access any potential crypto accounts by using those addresses. One way to mitigate risk in this respect is to have a separate and unique email account for each exchange. For example, an email address such as **cholm78fq9mx2@gmail.com** is much less likely to be hacked than **claytonholmwood@gmail.com**, especially if you don't ever use that more complex special email account on any website other than your cryptocurrency exchange.

A strong password is important. Best practices with respect to having a strong password include the following: A longer password is better, passwords which include capital letters and digits and symbols are better, and having a unique password for every website is better.

Two factor authentication is extremely important. With 2FA enabled, even if your email account AND exchange account password both become compromised, it is much less likely that hackers can access your account because they will essentially need to be in physical possession of your mobile device. However, you should never use SMS texts as your method of 2FA from a mobile device if that can be avoided. Device-based authorization, using an app such as Google Authenticator or Authy, is far more secure.

We've already mentioned that different exchanges have different requirements for opening an account. If verifying your identity is an option, you should consider doing this, even if you don't need to. That way, if you somehow get locked out of your account in the future, you MIGHT be able to convince the exchange support staff to let you back into your account, by providing the same documentation again.

Other best practices for computer security, which will help keep your exchange account secure, include ensuring that your computer is clean of viruses and malware and trojans and keyloggers, ensuring that your connection with your ISP is not being monitored through a compromised WiFi connection or similar attack, and ensuring that any private keys or seeds are stored in encrypted format on your computer.

As mentioned, all of these best practices are explained in much more detail in our Computer Security chapter. There is nothing more frustrating that losing your financial assets to a cyber-criminal. Although it takes time and effort to ensure that you're following the necessary steps for basic computer and internet security, this is one of the most important pieces of groundwork that all potential investors should take care of before putting any funds into purchasing cryptocurrencies.

Storing Assets on an Exchange

Perhaps one of the most contentious questions in cryptocurrency is whether or not it is safe to leave your assets on an exchange. In absolute terms, the answer should be a resounding no. If you don't control your private keys, you don't control your crypto. If your investments are held on an exchange, you don't control the private keys.

Having said that, there are a number of reasons why storing your assets on an exchange might actually be a smarter decision than moving your assets off-exchange to a hot or cold wallet. The decision is not always that simple. For instance, if you're trading frequently, you won't want to move your assets to a wallet, because you'll need to keep them on the exchange.

If the monetary value of your holdings is very small in terms of your own personal wealth, you may prefer the simplicity of keeping your cryptoassets on an exchange. If you can handle the possibility of the exchange being hacked and losing your investment, then keeping assets on an exchange becomes more reasonable. Of course, we can't give you an absolute dollar amount as guidance, because risk tolerance is different for every individual. A wise mantra is to never invest more than you can afford to lose.

There are also significant risks, unfortunately, to moving assets off an exchange and into a wallet. This process should make your assets a lot safer, in practice, but the sad reality is that many people have inadvertently lost their coins this way, either through user error, or from being hacked. A common user error involves sending coins to the wrong type of wallet address, for instance by sending Litecoins to a Bitcoin wallet. A second common user error is losing your private keys. Being hacked is also a risk. This can happen through an insecure internet connection, various types of malware that are installed on your computer, weak security practices, poor security of your private keys, and many other ways. This is probably one of the biggest problems with the cryptoasset markets right now, in that these risks should be negligible. However, they're NOT negligible. Many, many people have lost funds after being hacked, in literally hundreds of different ways.

If you're not fairly technically literate, and you're not comfortable with learning the process of creating paper wallets or desktop/mobile wallets and moving assets, then you may be better off leaving your assets on an exchange. We feel very nervous making this statement, simply because when you're on an exchange, you don't control your private keys. However, we have to accept the reality that some investors have very little IT prowess, and the security of their systems may also be questionable. Many people don't have the skills or motivation to set up a completely clean, sandboxed computer to handle their cryptocurrency trading. If you're using the same machine for your crypto that you do for everyday use, you've exposed yourself to a higher risk profile. If you're using a machine that is shared with family members or friends, that risk profile increases yet again.

Some cryptocurrencies are safer and easier to transfer and move than others. For example, through late 2017, Ark had a reputation as having one of the best wallets in crypto, and we never seemed to hear of anyone having problems with moving coins off an exchange and into the desktop wallet. On the other hand, the vast majority of Iota users had problems with the basic Iota wallet, and with zero balances, and with transactions that needed to be resubmitted or reattached, or that disappeared. Although we were big fans of the Iota technology, we were also quite unimpressed with the user experience in securing our assets. In Iota's defense, the Trinity wallet (which was released in late 2018) is probably one of the best wallets in crypto right now.

Ultimately, when you make a decision about how to store your cryptoassets, it comes down to balancing simplicity against the value of your portfolio, and in comparing risks of an exchange being hacked versus the risks of being hacked as an individual, or of making a mistake with your wallet setup. You also need to understand what options your own cryptoassets have in terms of off-exchange storage, and how secure and user-friendly those options are.

Please make sure you fully understand everything in the Wallets & Security chapter before making a decision to move assets from an exchange.

GOLDEN RULES OF SECURITY

This short chapter highlights some of the most important rules for your safety in cryptoasset investing.

Our “Top Six” Lessons for Crypto Investing

Never Share Your Private Key - If you don’t own your key, you don’t own your coins. Protect your private key like you would protect a pile of cash.

Avoid Online Seed Generators - The vast majority of online seed generators are compromised by hackers. If you need to generate a seed or private key for a paper wallet or certain other type of wallet, always do it with an offline script on a computer that is not connected to the internet. Also, make sure that the script is one that is endorsed by the official developers of the project. Even an offline generator can be dangerous if a criminal sets it up to distribute seeds from a certain small list of pre-populated compromised seeds that he or she has set up.

Don’t Trust Strangers - Many of the people whose advice you read on the internet are, at best, badly misinformed. There is a surfeit of blatantly false information posted on Reddit and other forums. These forums are also populated by large numbers of scammers and hackers. Verify everything before acting upon information that you read from anonymous strangers on the internet.

Use Resources Endorsed by Developers - Don't trust third-party wallets, websites, or any other type of resources found on the internet unless they have been officially endorsed and code-reviewed by the actual developers of the cryptoassets that you are investing in. A good starting point is the "sidebar" in the official Reddit community for a crypto, although some nefarious resources have even snuck into these lists in the past.

Understand Your Investments - If you don't understand the technology, learn the technology. Otherwise, you won't be able to tell when a project description is simply smoke and mirrors. If you don't understand coding, learn to code. It may take a year or more, but it's a great life skill to have.

Learn to Keep your Computers Secure - If you're not fully comfortable with the use of computers, and in knowing how to keep your devices secure, this is another great life skill to have. Computers will only become more prevalent in our society in the future.

Section 3 – Investing in Cryptoassets

EVALUATING A PROJECT

We would like to reiterate that we are not recommending that you invest any funds into cryptocurrencies. However, if you've already decided independently that you're going to invest money into crypto, the least we can do is try to teach you the best ways to avoid making bad investment decisions.

Many people are quickly persuaded to invest in a specific cryptoasset on the spur of the moment, because of a flashy advertisement, or because someone that they trust says that it will be "the next Bitcoin." This is a terrible approach to investing your money. If you're the type of person who goes into a restaurant and compares the price of different entrees on the menu, being aware that your choice will affect the dinner bill by a few dollars, then why would you EVER spontaneously invest hundreds or thousands of dollars into a project that may not even have a working product? And yet, this happens all the time. At some point, the crypto markets will have a big shakeup and a flight to quality (the 2018 crash was not that shakeup). When that happens, unsustainable or technically problematic projects will undergo large-scale devaluations, and only a relatively small number of crypto projects with actual real-world impact will maintain their trading value. Unless you're the sort of person who is comfortable with going to a casino and throwing significant sums of money on the roulette table, you should be very concerned with preservation of capital. The first rule of preservation of capital is to understand what you're investing in. Sadly, too many people are throwing money at weak cryptoasset projects with no real knowledge of how the project works, and whether or not it fills a basic need. Does your project solve a significant problem, or is it just looking for a problem to solve?

Metrics for Analyzing a Cryptoasset Project

The Technology: If the project has a whitepaper, read it. If you don't understand it, read it twice more. If you still don't understand it, at least you've probably learned some things, and at the very least, you probably have a better idea of what the project is all about than you did before going through the whitepaper.

The Vision: Does the project fill a need? Is this a need that couldn't be just as easily filled without blockchain? If the same problem could be solved by using a database instead of blockchain technology, then there may be no need for the project to exist.

The Competition: Is the project revolutionary or a first mover in its space, or is it simply copying a similar crypto project? The first mover will always have an advantage, although in some cases, superior technology can overcome that advantage.

The Project: Is the product/blockchain currently functional? If so, does it work well? If it isn't functional, when is it expected to be ready?

The Team: Who are the developers? Who are the advisors? What are their pedigrees? Can you see real links to their profiles on sites such as LinkedIn, and are you confident that these are real people participating in a real project, or just a bunch of random photos which have been posted to make the project look legitimate? How do they collaborate and move development forward? Is there a foundation or oversight group that is separate from the development group, and if so, how does that relationship function?

The History: How did the project get started? Was it a fork or clone of a different crypto? If so, what makes it different/better? Has the project met past goals and timelines on time and according to community expectations?

The Present: How do original founders/developers/advisors influence the project? What are developers working on at the present time?

The Future: Does the project have a defined roadmap? Are the goals attainable? Are the time frames reasonable? Is there a chance that goals might not be met?

The Financial Structure: Did the project have an ICO? What about pre-sales? Were any coins pre-mined? Do the developers hold coins in escrow that originated at the project's inception? Is there a foundation that defines and controls how funds are collected/allocated/spent? Was venture capital involved? Were there any institutional investments? Does the project rely wholly or partially on donations from the community?

The Marketing Approach: Does the project have a specific marketing team? Is it an in-house team, or a hired PR firm? What social media channels are utilized? What kind of advertising budget is the marketing team working with? What are the specific educational goals of the marketing campaigns that are in place? Have they been effective so far?

The Investors: Is investment open to all investors, or are there geographical restrictions? Are there any restrictions based on KYC regulations, or can people invest anonymously? Does the project have functional paper/desktop/mobile wallets for off-exchange storage?

The Environment: How might future regulatory oversight affect the project, either with respect to regulations affecting cryptoassets in general, or with respect to regulations that could affect specific aspects of this project?

The Potential: What kind of growth potential might this project have, based upon factors such as current price, current coin/token supply, inflation, liquidity, and ease of trading?

Analyzing Your Research

Once you've analyzed the answers to all of the questions above, you need to make a risk assessment of the project. Is this, insofar as crypto projects go, a relatively low risk, medium risk, or high risk? A healthy portfolio will probably have a mix of all three types of projects. There is probably a high chance that a large number of projects will catch your eye. You shouldn't invest in all of them. Unless you have no other job, and can "work" full-time at keeping up with cryptoasset research, we recommend that you hold no more than five to a dozen different types of cryptoassets at any one time. If you have any more than that, you probably don't have time to properly stay on top of research and on-going evaluation of your assets. Every portfolio should be re-evaluated on a regular basis, perhaps once every month to two months.

Don't allow yourself to become overly optimistic. Blockchain will change the world for the better, but we strongly believe that at least ninety-nine percent of crypto projects will probably fail in the long term. The project (or projects) that will become the dominant global cryptocurrency in the future may not even been conceived yet. The problem with looking at the world through rose-coloured glasses is that every red flag just looks like a flag.

We presume that all of your funds will not be invested into cryptoassets. That would be very risky. Just as you should have a diverse crypto portfolio, you should also have a diverse financial portfolio. Consider what portion of assets you should keep in property, real estate, traditional stocks and bonds, precious metals, treasury bills, and of course, in a savings account. We're not suggesting that you need to invest in all of these traditional financial instruments, but we do recommend some diversification. Your investment approach should be based upon your income, your age, and your risk tolerance. At a minimum, always keep enough in a savings account to cover food, housing, and other basic necessities for at least three to four months, in case you lose your job. The crypto markets are known for their gut-wrenching corrections, and when those happen, you don't want to be forced to sell at a loss simply to pay for groceries. A market correction can last much longer than you expect, even if it doesn't make sense. Be prepared for the worst. Remember that the markets can remain irrational longer than you can remain solvent.

Section 4 – Appendices

ABBREVIATIONS

Here are some common abbreviations that have come into use in cryptocurrency ecosystems, within finance/trading in general, and also in the fields of technology and computing as they relate to cryptoassets. If you'd like more information about any of the abbreviations that isn't obvious in meaning, check out the Definitions appendix. We've also included some common slang abbreviations which may be common sense to a generation that grew up on the internet, but which may not be as obvious to people who don't frequent social media sites such as Reddit.

/xxx or **[/xxx] –** A catchall slang to refer to the end of “xxx,” or This was “xxx”

/S - End of sarcasm, or This was sarcasm

ACES - Ark Contract Execution Services

ACH - Automated Clearing House

AFAIK - As Far As I Know

ALT - Alternative Coin (usually refers to any crypto that is not Bitcoin)

AMD – A type of graphics card made by Advanced Micro Devices

API - Application Programming Interface

ATM - Automatic Teller Machine (Bank Machine, Cash Dispenser)

ATM - At The Moment

2FA - Two Factor Authentication

2X - Segwit2x

AML - Anti Money Laundering

AS - Atomic Swaps

ASIC - Application-Specific Integrated Circuit

ATH - All Time High (sometimes also represents, depending on grammatical syntax, At The Height or At The High)

AWS - Amazon Web Services

B2B - Business To Business

BGTC - Beginner's Guide to Cryptocurrencies

BOINC - Berkeley Open Infrastructure for Network Computing

CFB - Come From Beyond

CLI - Command Line Interface

CMC - Coin Market Cap website

CPU - Central Processing Unit

CT - Confidential Transactions

DAG - Directed Acyclic Graph

DAO - Decentralized Autonomous Organization

DAPP - Decentralized Application

dBFT - Distributed Byzantine Fault Tolerance

DCA - Dollar Cost Averaging

DCI - Digital Currency Initiative

DD - Due Diligence

DDOS - Distributed Denial of Service

DEX - Decentralized Exchange

DLT - Distributed Ledger Technology

DNA - Distributed Network Architecture

DNM - Dark Net Market

DOX - Personal Information

DPOS - Delegated Proof of Stake

DYDD - Do Your Due Diligence

DYOR - Do Your Own Research

DPR - Dread Pirate Roberts

ELI5 - Explain Like I'm Five

ERCxx – Various numbered standards for tokens on the Ethereum Network

ERC20 - One very common type of token on the Ethereum Network

EVM - Extended Verification Module

FA - Fundamentals Analysis

FFS - Fee For Service

FFS - For F's Sake

FIAT - Fiat Currency (traditional national currencies)

FINCEN - The [US] Financial Crimes Enforcement Network

FOMO - Fear Of Missing Out

FUD - Fear, Uncertainty, & Doubt

GOX - Mt. Gox Exchange

GPG – A well-known type of encryption software

GPU - Graphical Processing Unit

GTO - Game Theory Optimized

GUI - Graphical User Interface

HDD – Hard Disk Drive

HIBP - Have I Been Pwned? (website)

HODL - Hold (for the Long Term)

HODL - Hang On for Dear Life

HTLC - Hashed Timelock Contract

I2P - Invisible Internet Project

ICO - Initial Coin Offering (crypto tokens)

ICO - Initial Public Offering (stocks)

ICYMI - In Case You Missed It

IIRC - If I Recall Correctly

IKR - I Know, Right?

IMA - Independent Management Architecture

IMHO - In My Humble Opinion

IMO - In My Opinion

ILP - Interledger Protocol

IoT - Internet of Things

IR – Investor Relations

IRL - In Real Life

IRS - Internal Revenue Service (the US taxation authority)

JMO - Just My Opinion

KYC - Know Your Customer

LAMBO - Lamborghini

LCW - Live Coin Watch website

LE - Law Enforcement

LIT - An alternative lightweight Lightning Network developed by the MIT Media Lab

LMK - Let Me Know

LN - Lightning Network

LND - Lightning Network Daemon

LPT - Life Pro Tip

M2M - Machine To Machine

MC - Market Cap

MEW – My Ether Wallet

MITM - Man In The Middle

MM - Market Maker

MMS – Multimedia Text (capable of more content than SMS)

MRW - My Reaction When

N/A - Not Applicable or Not Available

NFC - Near-Field Communication

OC - Overclocking

OG - Original Gangster

OP - Original Poster (used on Reddit and similar social discussion sites)

P2P - Peer To Peer (or Person to Person)

PGP - The "Pretty Good Privacy" encryption standard

PITA - Pain In The Ass

PKI - Public Key Infrastructure

PND - Pump & Dump (also P&D)

POA or PoA - Proof of Authority

POB or PoB - Proof of Brain

POB or PoB - Proof of Burn

POC or PoC - Proof of Concept

POD or PoD - Proof of Devotion

POLO - Poloniex cryptoasset exchange

POR or PoR - Proof of Research

POS or PoS - Proof of Stake

POS - Piece of Shyte

POW or PoW - Proof of Work

PR - Public Relations

PR - Pull Request

PS – Power Supply

PWD - Password

QC - Quantum Computing

QC - Quality Control

QR - Quick Response code

QS - Quantum Supremacy

R&D - Research & Development
RAM – Random Access Memory
SA - Sentiment Analysis
SEC - United States Securities and Exchange Commission
SEGWIT - Segregated Witness
SHUM - Should Have Used Monero
SMS - Standard Messaging Service (traditional text message on mobile device)
SNARK - Succinct Non-Interactive Argument of Knowledge
SPV - Simple Payment Verification
SSD – Solid State Drive
STARK - Scalable Transparent Argument of Knowledge
TA - Technical Analysis
TFW - That Feeling When
TIL - Today I Learned
TLDR - Too Lazy; Didn’t Read
TOD - Time Of Day
TOR - The Onion Router (browser)
TOR - Terms Of Reference
TOX - Peer to Peer encrypted messaging protocols
TPM - Trusted Platform Module
TREX - Bittrex cryptoasset exchange
Ux - User Interface
YOY - Year Over Year
YTD - Year To Date
ZK - Zero Knowledge (as in zk-SNARKS and zk-STARKS)

If you come across an abbreviation that you don’t recognize and it was not on this list, it’s quite possible that it’s a ticker for a particular cryptoasset.

You can try putting it into the search box on Coin Market Cap and see if it shows up as a type of crypto.

DEFINITIONS

Accidental Fork - This happens when two or more blocks are “simultaneously” mined with the same block height, forking the block chain unintentionally. This typically occurs when two or more miners find blocks at nearly the exact same time, although it can also happen as part of an attack. When an accidental fork occurs, one of the forks will almost immediately become dominant through consensus support from network participants, and the non-dominant fork(s) or orphans will fade from use. Although it is common for more than one block to be found "simultaneously" to create such a fork, and network latency can possibly exacerbate the problem, the situation usually resolves almost immediately, with the one being heard first by the network ending up as the "winning" fork.

Airdrop - Occurs when some amount of a coin/token is distributed to the community at no cost, usually to encourage wide distribution and perhaps generate interest in the coin/token. Sometimes a crypto project will airdrop to its own holders, and other times a project will airdrop to holders of a different token. For example, if ExampleCoin wants to raise attention and gain a diverse userbase, it could decide to airdrop 500 ExampleCoin tokens to every person who holds at least 10.0 Ethereum tokens on a certain time/date. The Ethereum blockchain would be analyzed (a snapshot taken) at that exact time, then the developers at ExampleCoin could give 500 ExampleCoins directly to each valid Ethereum holder, by depositing the ExampleCoins directly into their Ethereum wallets (this assumes that ExampleCoin is an ERC-based token that can share a wallet with ETH). Airdrops don't happen too frequently, and when they do, their dollar values usually aren't very significant.

Altcoins - This slang (often shortened to "alts") originally referred to any cryptocurrency or cryptoasset that was not Bitcoin. As the market matures, it is possible that larger projects will start to be referred to as large-cap and mid-cap cryptos (referring to the size of each project's market capitalization), and the term "altcoin" may start to be used more exclusively with lesser-known projects that have smaller market caps. For example, Ethereum is a major and notable project, and may not deserve to be called an altcoin anymore. For now though, most people refer to all cryptos other than Bitcoin as altcoins. An "altcoiner" is someone who invests in or uses crypto, but who prefers to avoid Bitcoin.

Air-Gapped - A computer or other device which is not connected to the internet, making it much less prone to hacking attempts.

Anti Money Laundering (AML) - Regulations that have been put into place by governments to help detect and report suspicious activity relating to any number of financial activities that might include money laundering, terrorist financing, securities fraud, and market manipulation.

API Call – This happens when an API (a software routine) is sent a request to fetch data from another application.

Application Programming Interface - A software intermediary that allows two applications or programs or websites to talk to each other. It is a set of routines, protocols, and tools for building software applications. It is a set of clearly defined methods of communication between various software components.

Application Specific Integrated Circuit (ASIC) - A type of integrated circuit that is designed and created for a specific application or purpose. Compared to a general-purpose integrated circuit, an ASIC can improve processing speed because it is specifically designed to do one thing as efficiently as possible. An ASIC is usually smaller and more efficient than a general purpose integrated circuit, and uses less electricity. The disadvantage of an ASIC is that it can be very expensive to design and manufacture, particularly if only a few units are needed. ASIC's can be designed for everything from portable audio recording units to image processors in digital cameras, but the common use in the cryptoasset ecosystem is for mining certain types of cryptocurrency, especially Bitcoin and Litecoin. Because ASIC's are all custom-made and thus only available to the company that designed them, they are considered to be proprietary technology. Using ASIC's to mine crypto is much more efficient than using CPU's or even GPU's. This has led to some criticism because ASIC miners have come to dominate the mining industry for certain types of crypto. Other types of crypto (such as Vertcoin) have advertised that they are ASIC resistant, by virtue of planning to immediately change mining algorithms if an ASIC is developed for that coin (the intent is to allow users with "just" a GPU to be able to participate in mining for the project). A big risk of owning an ASIC (beside the high cost) is that if the mining algorithm is changed, the ASIC will probably become useless.

Arbitrage - Buying a security in one market and simultaneously selling it in another market at a higher price, profiting from a temporary difference in prices. This is considered riskless profit for the investor/trader. For example, if ExampleCoin can be bought on Bittrex for $7.25 per coin, and people are buying ExampleCoin on Bithumb for $7.80 per coin, it would be possible to almost simultaneously buy on Bittrex and sell on Bithumb for a profit of $0.55 per coin. Of course, other traders around the world usually notice when there is an easy opportunity for arbitrage, so prices start to balance out as the market slowly reacts and eliminates the arbitrage opportunity.

Arise Chikun - A meme (from the Aqua Teen Hunger Force cartoon) that supporters of a crypto (especially Litecoin) like to share when their crypto is trading listlessly and they want it to rise in value. See the meme page on our website for more background information.

Astroturfing - Masking the sponsors of a message (or organization) to make it appear as though it originates from and is supported by a members of a grassroots community.

Atomic Swap - The exchange of one cryptocurrency for another cryptocurrency, without the need to trust a third-party. The objective of atomic swaps (also known as atomic cross-chain trading) is to create interoperability between coins/tokens relating to various cryptoasset projects. Atomic swaps are still a technology in development, however, several simple atomic swaps have been performed, such as between Vertcoin and Litecoin. One group of cryptoassets which should all be able to cross-participate in atomic swaps would include Bitcoin, Bitcoin Cash, Decred, Litecoin, Monacoin, Particl, Vertcoin, and Viacoin, due to their very similar coding frameworks.

Automated Clearing House (ACH) - An electronic network for financial transactions (based in the United States), which processes large volumes of credit and debit transactions in batches. ACH credit transfers include direct deposit, payroll payments, and vendor payments. They frequently tend to be part of a long-term series of transactions between related parties (as opposed to wire transfers, which are usually for infrequent, one-time transfers).

Average Down – To buy additional shares of a security (one which the purchaser already holds) when the price is lower than the purchase price of the earlier securities. This lowers the overall average purchase price per unit.

Bad Actor - A hacker, swindler or some sort of con artist, or any person who has malicious intentions. Also commonly referred to as a malicious actor.

Base Reserve - See "Minimum Balance."

Bear - Someone who is pessimistic about the direction of the markets, ie. anyone who thinks that asset values and/or trading prices will decrease.

Bearish Sentiment - When investors or analysts believe that the price of a security will decrease over time.

Black Swan - An event or occurrence that deviates beyond what is normally expected of a situation and is extremely difficult to predict. Black swan events are typically random, infrequent, and unexpected. Some examples of geopolitical black swans would include the falling of the World Trade Towers on 9/11, and the falling of the Berlin Wall in 1989. Some examples of financial black swans would include the Black Monday crash in October of 1987, or the stock market crash of 1929.

Block - One record within a blockchain. A block will usually contain a hash pointer link to the previous block in the chain, a time stamp, and transaction data (if there were any transactions included in that block). Depending on how the blockchain is set up, blocks can contain additional fields of data such as spurious messages, random numbers, or many other types of information.

Blockchain - A list of records (called blocks) which are linked and secured using cryptography. Each block typically contains a hash pointer (a link to the previous chronological block), a timestamp, and transaction data. Many blockchains grow continuously, regardless of whether or not new information is added (transactions being processed on the chain), so it is possible to have blocks which don't contain any transactions. By design, blockchains are inherently resistant to modification of the data. A blockchain is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way." For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network which collectively adheres to a protocol for validating new blocks. The inability to edit/modify/delete information that has been included in the blockchain means that the blockchain is immutable (unchangeable). Once recorded, the data in any given block cannot be altered retroactively without the alteration of all subsequent blocks, which would be almost impossible because it would require collusion of the majority of network participants.

Breach - A security incident that results in unauthorized access of data, applications, services, networks and/or devices, by getting past their security mechanisms or defenses. A data breach can refer simply to unauthorized access, or also to outright theft and redistribution.

Bulletproof - This is a feature in Monero.

Bull - Someone who is optimistic about the direction of the markets, ie. anyone who thinks that asset values and/or prices will increase.

Bull Run - When prices remain in a general rising trend for a period of days, weeks, or months.

Bullish Sentiment - When investors or analysts believe that the price of a security will increase over time.

Burn - A coin burn (or token burn) occurs when coins are sent to an address or wallet from which nobody is able to retrieve them at the current time, and from which the coins can never be recovered in the future. The coins are therefore lost permanently. This is accomplished by having a deposit address that either has no private key, or that had a private key which was somehow destroyed in a manner that nobody can ever retrieve it. The most common reason to burn existing coins is to increase the value of the remainder of that type of coin. This assumes that the implicit market value of a project (not the approximate market cap based on current trading price of the coin/security) will remain unchanged when a coin burn happens, therefore, the total value of the project will be distributed among a lower number of assets, and each asset will therefore be worth more per unit. If a coin burn happens, it is usually a publicized event initiated by the developers of the project, and a large number of coins/tokens are slated for "destruction" (being made inaccessible) at a specific time and date. Burning of coins also takes place commonly on a much smaller scale in the "Proof of Burn" systems being used by a handful of cryptoassets.

Buy Wall - A buy wall on an exchange is a large order(s) at a certain price that acts as an obstacle, in order to try to restrict the trading price from going down too far. If the buy wall is large enough, there may not be enough sellers to overcome it and push the market price lower. For instance, if a certain large holder wants to support the market value of ExampleCoin at $1 because it has been dropping lately, they might put in a buy order for ten million units of ExampleCoin at $1. It would then take a very large number of disillusioned sellers to eat through the buy offer at that level. This technique, intended to support the security's price for a period of time, can be useful to avoid a psychological/pricing rout which might cause even more damage to a large holder's portfolio in the long term.

Candlesticks - A style of financial chart used to describe price movements of a security, derivative, or currency. Candlesticks reflect the impact of investor sentiment on security prices and are used by technical analysts to determine when to enter or exit a trade. The study of candlestick charting is complex, as there are dozens of patterns that can be identified, and not all patterns give clear signals about market direction. It would be possible to spend months studying candlestick analysis.

Casper - Casper is a Proof of Stake system which is designed as one possible long-term solution for scalability in Ethereum. There would be other advantages to using Casper on Ethereum (as opposed to the current Proof of Work algorithms): Casper would help improve decentralization, enhance economic security, and most importantly, it would be energy efficient.

Central Processing Unit (CPU) - 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 operations specified by the instructions. The CPU is basically the brain of a computer.

Centralization - The opposite of decentralization. Centralization is the concentration of control of an activity or organization under a single authority. Centralized platforms require all data to pass through a singular point. Information can't be sent or received without it going through that single point (which is often a server or hub).

Chain - Short for Blockchain.

Changelly - A trading service which facilitates exchanges between digital currencies. The service offers a wide range of digital currencies to buy and sell but does not provide conversion to or from traditional (fiat) currencies. Changelly aggregates and suggests the best currency rates among the largest crypto trading platforms. Do extensive research before attempting to use Changelly. Many users have reported alleged unresolved problems with this service. We feel that buying and selling crypto on a major licensed exchange is always the safest way to trade. Always avoid gimmick sites, eBay, Craigslist, and other similar methods of purchasing cryptocurrencies. Your money will be safest if you use the top ten globally ranked exchanges.

Churn - In traditional marketing, the churn rate (also known as the rate of attrition) is the percentage of subscribers to a service who discontinue their subscriptions to that service within a given time period. For a company to expand its clientele, its growth rate (as measured by the number of new customers) must exceed its churn rate. When it comes to securities, churn is sometimes be used as a reference to the general turnover in ownership of securities or coins. For example, let's say that going into June of 2018, there are a total of 37,000 Vertcoin holders worldwide. Then there is a period of consolation for two months. During those two months, two thousand Vertcoin holders sell all their holdings and exit the Vertcoin market, but three thousand other people enter the market by buying Vertcoin. That "turnover" in ownership is the churn during the consolidation period. Churning also has a separate technical meaning in terms of securities trading, namely, excessive trading by a broker in a client's account, done principally to generate commissions. This type of churning is an illegal and unethical practice that violates SEC rules and securities laws.

Cipher - A method of hiding words or text with encryption by replacing original letters with other letters, numbers and symbols.

Ciphertext - Text or written information that has been encrypted.

Cloud Mining – Setting up a virtual computer online, using services such as Amazon's AWS, and tasking it to mine cryptocurrencies.

Coblee - Refers to Charlie Lee, the lead developer of the Litecoin project.

Coin Burn - See "Burn."

Cold Wallet - A wallet of any type (be it physical, software, or paper) that is not connected to the internet.

Collar - In traditional stock markets, a collar is an options trading strategy that is constructed by holding shares of the underlying stock while simultaneously buying protective puts and selling call options against that holding. The puts and the calls are both out-of-the-money options having the same expiration month and must be equal in number of contracts. However, in more colloquial terms, a collar can sometimes refer to a tight pricing range that a stock is temporarily trading in due to the presence of large buy and sell walls on either side of the range. For example, if ExampleCoin is trading on an exchange that has a huge buy wall at $5.50 per coin, and another huge sell wall at $6.00 per coin, some people will say that there is a price collar in place between $5.50 and $6.00. The market price won't likely drop below $5.50 because someone is willing to buy a lot, and probably won't rise above $6.00 because someone (possibly the same entity trying to "make a market") is willing to sell a lot. See also the definition of Market Maker.

Colored Coins - A class of methods for associating real world assets with addresses on the Bitcoin network. Examples could be deeds, stocks, bonds or futures. The technology could also be used to track and register intellectual property assets. Although Bitcoin was originally designed to be a currency, its scripting language allows it to store small amounts of metadata on the blockchain, which can be used to represent asset manipulation instructions. The advantage of using Bitcoin's blockchain as the backbone leverages Bitcoin's strengths, such as immutability, non-counterfeitability, ease of transfer, robustness and transparency, thus allowing asset manipulation with unprecedented security and ease. In principle, one can represent asset manipulation data on other blockchains (such as Litecoin), or could use other types of cryptoassets with smart contracts to perform the same function. The term "Colored Coins" is usually associated with implementations that specifically use the Bitcoin blockchain, and which don't issue an auxiliary coin.

Command Line Interface (CLI) - A means of interacting with a computer program where the user (client) issues commands or requests to the software by entering lines of text (command lines). The program which handles the interface is called a command language interpreter, or shell. The text-based interface of a CLI was the traditional means of data entry into a computer for decades after punch-cards stopped being used. Nowadays, it is not common to see a CLI used for interacting with software (unless you're talking to coders and IT specialists who are very comfortable with their machines). Graphical user interfaces (GUI's) are more commonly used in the latest modern operating systems.

Commit - A term used in coding and data management, which means to make a set of tentative changes permanent. After new code is tested and audited, if the developers think it is ready to be introduced into the mainstream product, it gets a commit to become part of the official code for the project.

Consolidation - Describes the movement of a security's price within a well-defined pattern of trading levels. Consolidation is generally regarded as a period of indecision, which ends when the price of the asset moves above or below the prices in the trading pattern. During a consolidation phase, a security is neither continuing nor reversing a larger price trend. Consolidated securities typically trade within limited price ranges and offer relatively few trading opportunities until another pattern emerges. As an example, a crypto may slowly rise from $1 to $5 during August and September, then during October through December it might trade during a tight range of between $5 and $6 for the entire three months. Suddenly, in January it starts moving up (or down) significantly from that range. In this example, the trading during October-December, when it floated between $5 and $6, was the consolidation phase. During the consolidation phase, it is common for a number of holders of the security to sell to new entrants. In that case, the consolidation phase begins to create a new "base" price (average cost base) at which a large part of the market invested. The consolidation phase may also called the congestion phase in some markets. A consolidation phase after a period of rapid increases often allows the market to "catch its breath" and evaluate whether the security is priced fairly.

Crowdsale - See "Initial Coin Offering."

Crypto - Slang shorthand for cryptoasset or cryptocurrency. Most people use it as shorthand for cryptocurrency, but since that's a bit of a misleading term in itself, based on the way it is currently used, you should probably think of the word "crypto" as being shorthand for cryptoassets of any type.

Cryptoasset - The term cryptocurrency frequently gets misused to encompass all types of "coin-like" or "token-like" digital assets. However, a more appropriate term for this would be cryptoasset. Cryptoassets can be broken down into several subcategories, including cryptocurrencies (the pure currencies such as Bitcoin and Litecoin and Ripple), crypto platforms (such as Ethereum, Ark, and Neo), and crypto projects, which often use utility tokens (such as Golem, Siacoin, and OmiseGo). There are also some additional categories for grouping cryptoassets, such as StableCoins.

Cryptography - Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography originally related to creating and breaking codes in written form and in radio transmissions, but in today's world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption).

Cryptojacking - Occurs when a website has an embedded cryptocurrency mining code that makes use of visitor resources without informing them. The process makes the user's machine run more slowly as it ties up system resources (especially CPU cycles and memory).

Cryptosphere - The overall ecosystem that encompasses all activities that take place in the various types of cryptocurrencies, crypto platforms, and other crypto projects. You could call it the cryptoasset "industry" or the cryptoasset "field" or the cryptoasset "market," but in reality, the cryptosphere is a slang term that encompasses all those and more.

Cryptocurrency - This term frequently gets used incorrectly. Technically, a cryptocurrency is a type of cryptoasset that specifically acts or is intended to act purely (or almost purely) as a type of digital currency, rather than as a smart contract or development platform, or as a security token for a project. Some examples of cryptocurrencies include Bitcoin, Litecoin, Vertcoin, Dash, and Ripple.

Daemon - A computer program that runs as a background process, rather than being under the direct control of an interactive user. It typically waits to be activated by the occurrence of a specific event or condition.

Dark Net Market (DNM) - A commercial website on the web that operates via darknets (anonymous or hidden networks) such as Tor or I2P. They function primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, and other illicit goods, in addition to the normal sale of legal products.

Death Spiral - A theoretical catch-22 situation for a PoW cryptocurrency whereby the current difficulty level is set to be fairly high (due to significant historical hashing power devoted to the network), but due to a recent significant drop-off of hash power committed to the network, new blocks become very slow/difficult to mine. This condition can create a negative feedback loop of sorts: Because new blocks are difficult to mine, more hashing power leaves the network, which means that new blocks are mined even more slowly. The system might grind to a halt entirely if the death spiral is not stopped somehow (such as by an adjustment to the difficulty level, to make it easier to mine again).

Decentralization - The opposite of centralization. Decentralization allows the transfer of decision making power and assignment of accountability away from a single administrative center(s) to other locations. The value of decentralization in cryptoassets is that if an asset is not under a centralized authority, then it becomes harder for any specific entities (especially governments or hostile actors) to control the project. With a decentralized project, change can only be effected through consensus.

Decentralized Autonomous Organization (DAO) - The DAO was a digital decentralized autonomous organization and a form of investor-directed venture capital fund, which became notorious due to an Ethereum hack in 2016. The DAO had an objective to provide a new decentralized business model for organizing both commercial and non-profit enterprises. It was instantiated on the Ethereum blockchain, and had no conventional management structure or board of directors. The DAO was crowdfunded via a token sale in early 2016, setting a record for the largest crowdfunding campaign in history. In June 2016, users exploited a vulnerability in the DAO code to enable them to siphon off one third of The DAO's funds to a subsidiary account. On July 20th, 2016, the Ethereum community decided to hard-fork the Ethereum blockchain to restore virtually all funds to the original contract. This was controversial, and led to a fork in Ethereum, where the original unforked blockchain was maintained as Ethereum Classic, thus breaking Ethereum into two separate active blockchains (each with its own cryptocurrency). The DAO was delisted from trading on major exchanges such as Poloniex and Kraken in late 2016. Many people were critical of the hard fork as they pointed out that it did not conform to the tenets underlying a truly decentralized platform. Other people supported the fork as a necessary action to preserve the reputation of the Ethereum project.

Decentralized App (DAPP) - A DApp is any software or application that has its backend code running on a decentralized peer-to-peer network, instead of running on one specific computer or server. This eliminates a point-of-failure risk. Even if some of the network peers go down, many other peers are still able to provide the code for the app to keep functioning.

Decentralized Exchange (DEX) - A crypto exchange in which control of the exchange is decentralized, rather than being maintained by a single entity. A properly created decentralized exchange significantly reduces the chance of users being scammed by malicious actors. The drawback of decentralized exchanges is that they do not offer the ability to trade between fiat currencies and crypto, which means that they cannot act as gateway exchanges.

Delegated Byzantine Fault Tolerance (dBFT) - A type of consensus protocol used in certain Proof of Stake projects such as the Ark platform. The consensus part of the Delegated Byzantine Fault Tolerance protocol occurs through a "gamified" form of block verification among professional node operators. All of these professional nodes are appointed by ordinary nodes through a delegated voting process (in Ark's case, there are 51 nodes or delegates). Each professional node broadcasts its own version of the blockchain to the network. If 66% of the other nodes agree with the information, consensus is achieved. Should this threshold not be met, a different professional node is appointed to broadcast its blockchain version until consensus can be established. This type of system is not a completely decentralized system, but it is not completely centralized either.

Delegated Proof Of Stake (DPOS) - Delegated Proof-of-Stake (DPOS) is the fastest, most flexible, most efficient, and most decentralized consensus model available. This method implements a layer of technological democracy to offset the negative effects of centralization. Basically, everyone who holds tokens on a network gets to vote for delegates, with one vote for each token held. A number of delegates (sometimes called Witnesses) are thus elected to act as representatives for the network, similar to a house of parliament acting on behalf of citizens. The key point is that voting is an ongoing process, and since there are only a certain specific number of top delegates that get to participate in governance of the system, it is possible at any point for voters with enough influence to move a delegate out of the key top ranking group. Delegates are therefore incentivized to act on behalf of the community and their voters. Some crypto projects that use DPOS include Ark, Lisk, EOS, Steem, and BitShares.

Digital Currency Initiative (DCI) - A group at MIT that focuses its research and development upon cryptocurrency and its underlying technologies.

Directed Acyclic Graph (DAG) - A mathematics and computer science construct, which is a finite directed graph with no directed cycles. It consists of finitely many vertices and edges, with each edge directed from one vertex to another, such that there is no way to start at any vertex "v" and follow a consistently-directed sequence of edges that eventually loops back to "v" again. Equivalently, a DAG is a directed graph that has a topological ordering, characterized by a sequence of vertices such that every edge is directed from earlier to later in the sequence. DAG's can model many different kinds of information. The most well-known DAG in the current cryptoasset space is "The Tangle," a DAG used by the Iota project.

Distributed Ledger - A collection of replicated, shared, and synchronized digital information which is spread across multiple sites, countries, or institutions. There is no central administrator or centralised data storage. It is basically a database or collection of records, all of which have been verified as accurate by group consensus, which are stored on a peer-to-peer network that can extend around the globe.

Distributed Ledger Technology (DLT) - Another name for distributed ledgers and blockchain technology.

Distributed Network Architecture (DNA) - The types of systems used in non-centralized computing networks. Cloud computing is a type of distributed network. The internet is a type of distributed network. Telecommunications networks and grid computing networks are types of distributed networks.

Distro - Computer science slang for a “distribution,” ie. a version of a program, app, or software package. It frequently refers to different versions of the Linux operating system, but can also refer to other software.

Dollar Cost Averaging (DCA) - An investment technique of buying a fixed dollar amount of a particular investment on a regular schedule, regardless of the price of the security. The investor purchases more securities when prices are low and fewer securities when prices are high.

Doxxing - To search for and publish private or identifying information about a particular individual on the Internet, typically with malicious intent. A very good common sense security protocol is not to Dox yourself on a public forum, ie. don’t provide personal information which makes it easier for bad actors to identify who you are in real life.

Dread Pirate Roberts (DPR) - A character from a book/movie called "The Princess Bride". This name was used as a pseudonym by Ross Ulbricht, an American former drug trafficker and darknet market operator, who was best known for creating and running the Silk Road website from 2011 until his arrest in 2013.

Dry Powder - Funds (in fiat) which are kept "on the sidelines" in an exchange, so if a particular security drops significantly in price, you have the ability to take advantage of that dip immediately without needing to go through the process of adding funds to the exchange.

Due Diligence (DD) - Comprehensive research and analysis of a business/project/product, which should be undertaken by a prospective buyer, especially to establish the value, risks, and potential profit of purchasing that asset. Crypto investors should always do their due diligence before investing into a project, so they understand exactly what they're getting themselves into, and to ensure that they don't put funds at risk without knowing risk factors involved. Reading comments from anonymous users on 4chan and Reddit does not qualify as professional due diligence. Be prepared to read whitepapers, review websites, read articles and blogs, enter into debate on social media, and study technology/coding (if possible) to ensure that your due diligence and research is of the highest possible standard. It's your money that you're putting at risk.

Dust - Tiny fractions of coins sitting on exchanges (or in wallets) that are too insignificant to be used, either because there isn't enough value there to cover the transaction fee, or because the exchange has minimum value requirements for trades. For example, if you have 0.00002346 ExampleCoin remaining after a specific trade, and that amount is worth the equivalent of 1.6 cents, the exchange probably won't let you do anything with it. Unfortunately, there aren't a lot of ways to sweep up this dust, so it tends to clutter up some peoples' accounts on certain exchanges.

Encoded Listener - An application built using the Ark platform, to aid in SmartBridge communication. An Encoded Listener node is a hub for listening to SmartBridge transactions. Any trading entity (such as Changelly, Shapeshift, Coinbase) can set up an Encoded Listener node, in order to help the network. In fact, anyone at all who wants to help the network may be able to set one up. In exchange for providing this service, they will be able to collect transaction fees for passing data or exchanging currencies via SmartBridge.

Encryption - The process of converting information or data into a code, especially to prevent unauthorized access.

Escrow - A financial arrangement where a third party holds and regulates payment of the funds required for two parties involved in a given transaction. The intent of escrow is that the third party be an independent and unbiased facilitator to the transaction, to ensure that neither of the two main parties to the transaction are cheated. For example, in an online sale, a buyer and seller may not trust each other, but they may trust a specific third party such as a public escrow agency. The buyer gives the funds to the escrow agency, and the escrow agency doesn't release the funds to the seller until the buyer notifies the escrow service that they received the goods/services relating to the transaction. This way, there is no risk to the buyer that the seller will failure to deliver the goods/services (because the seller won't receive money until they’ve done so), and there is no risk to the seller that the buyer won’t pay for the goods/services (because the funding is already sitting with the escrow agent who is ready to pay the seller once the seller’s obligations have been fulfilled). An escrow situation is still not absolutely bulletproof. There have occasionally been scams with escrow agents colluding with one of the parties in the transaction. However, escrow almost always allows a buyer and seller who don’t trust each other to complete a contract with very little risk that either side will be cheated.

Exchange - A business/entity/institution/organization that allows people to buy and sell various types of assets or securities (such as stocks, bonds, foreign exchange currencies, crypto assets, etc.). Traditionally, exchanges were real-world bricks & mortar institutions, although in modern times, all traditional exchanges also have online extensions. Aside from informal person-to-person meet-ups and gatherings to exchange cryptoassets, the vast majority of crypto trading is facilitated by online systems.

Explain Like I’m Five (ELI5) – To put something into layman’s terms, or to “dumb down” the explanation so someone who is very unfamiliar with the topic can still understand the concept.

Exploit - Any software, data, or a sequence of commands (code) that takes advantage of a bug or vulnerability, in order to cause unintended or unanticipated behavior to occur on any type of computerized software or hardware.

Extended Verification Module (EVM) - A security interface feature for some Linux computers that can help to secure the kernel against tampering/hacking.

Faucet - The name given to any website or app which gives away free cryptocurrencies (usually in very tiny amounts). Although these faucets aren't intended as a way for visitors to become rich for free, they can serve a useful function to give users very small amounts of cryptos to play with while experimenting with setting up wallets, etc. Some faucets are sponsored by holders of cryptocurrencies who got into that particular crypto very early in the game, when that particular crypto was very inexpensive. Other faucets are supported by the advertising on their pages.

Fear Of Missing Out (FOMO) – A feeling of apprehension that arises from a belief that others might be having rewarding experiences from which oneself has been excluded, either inadvertently or by choice. In cryptoasset investing, an investor will sometimes see that a particular project is suddenly appreciating in value for some reason. Due to a "fear of missing out" on a chance to make some money, they impulsively invest in the project (often with less research than they should have performed). FOMO often causes an impulsive investor to invest at a "less-than-optimal" point on a pricing curve. If you are going to invest in cryptocurrencies, your best chance for success is to remain disciplined and rational, and make sure that you do a large amount of research before ever investing in any project.

Fear, Uncertainty, & Doubt (FUD) - This acronym/phrase refers to a disinformation strategy used in sales, marketing, public relations, talk radio, politics, religious organizations, and propaganda. FUD is generally a strategy to influence perception by disseminating negative and dubious or false information, in an attempt to discredit something or to foster uncertainty and disbelief. In the traditional stock market world, "bashers" are people who attempt to discredit companies or stocks through a campaign of negative statements and opinion. Fudders or Fudsters take the same approach, especially within the world of crypto. This is not new slang that is particular to crypto. The term originated more than a century ago.

Fiat - Traditional money, ie. nationalized currencies such as the US Dollar, the Canadian dollar, the Euro, the British pound sterling, the Japanese Yen, the Chinese Renminbi (Yuan), and so on.

Fill – To have an exchange order met and completed by an opposing buyer/seller. Market orders almost always get a fill immediately, but for limit orders, the person who placed the order generally has to wait until an opposing trader meets his/her financial terms.

Flappening - A theoretical future point in time at which Litecoin switches places with Bitcoin, taking over the largest position in the cryptocurrency world in terms of market cap. Bitcoin currently has a very large dominance within the cryptocurrency markets, so it is possible that it will always retain its dominance, and the flappening may never happen. This is a play on words for "flippening" which relates to the "Arise Chikun" meme for Litecoin.

Flippening - The theoretical future point in time at which some type of cryptocurrency (perhaps Ethereum) switches places with Bitcoin, taking on the largest position in the cryptocurrency world in terms of market cap. Bitcoin currently has a very large dominance within the cryptocurrency markets, so it is possible that it will always retain its dominance, and that the flippening may never happen.

Forging - Forging is a process that is fairly similar to mining. However, forging is what happens in a Proof of Stake system, and Mining is what happens in a Proof of Work system. In Proof of Stake, the creator of the next block is chosen via various combinations of random selection and wealth or age (i.e. the stake). Once the creator of that next block is chosen, the creator is the one who "forges" or creates the block. Mining is a "random probability" process, with people competing to find the next block, but the process of forging means that once the creator is chosen, there is no competition anymore because the creator is the only entity allowed to make the block.

Fork - A software fork occurs when there is a change in the underlying programming protocol, resulting in the "forking" or split of the original blockchain. This usually results in the creation of a new coin. There are different types of forks such as hard forks, soft forks and accidental forks.

Fundamentals Analysis (FA) - A method of evaluating a security in an attempt to measure its basic intrinsic value, by examining related economic, financial and other qualitative and quantitative factors. This analysis relates to the strength of the security and company or project that it represents. In traditional markets, close examinations of income statements and balance sheets would come into play, along with other factors such as cash flow analysis, predicted payback periods on projects and ROI, etc.

Funding - To process of adding funds to an exchange, ie. to deposit traditional fiat currencies (such as $USD or Euros) into an exchange, so you can subsequently use that money to buy cryptocurrencies. Technically speaking, you can also fund an account with crypto, although most people think of funding in terms of fiat.

Fungibility - The property of a good or a commodity whose individual units are essentially interchangeable. For example, gold is fungible since one kilogram of pure gold is equivalent to any other kilogram of pure gold, regardless of whether it is in the form of coins, ingots, or in other states. Gold can be melted down, and if that happens, nobody can tell one specific ounce from any other ounce. Other fungible commodities include sweet crude oil, company shares, bonds, other precious metals, and traditional fiat currencies. Fungibility refers only to the equivalence of each unit of a commodity with other units of the same commodity. One important characteristic of money is that it be fungible. This is one weakness shared by almost all cryptocurrencies. Because the blockchains for various cryptocurrencies contain an immutable (unchangeable) public ledger of all transactions in the currency's history, then cryptocurrencies are not perfectly fungible. For example, if the government discovered that certain Bitcoins were used in connection with a crime, then those particular Bitcoins could become "tainted." The government could take efforts to find the holder of those particular coins, and there could be negative ramifications for someone who was discovered as being the person who holds them. It is not possible to just swap your tainted Bitcoins for other Bitcoins, because there is still a permanent public record. Therefore, blockchain currencies with public ledgers are NOT completely fungible.

Game Theory Optimized (GTO) - Game theory is the study of mathematical models of conflict and cooperation between intelligent rational decision-makers. Originally, it addressed zero-sum games, in which one person's gains result in losses for the other participants. Today, game theory applies to a wide range of behavioral relations, and is now an umbrella term for the science of logical decision making in humans, animals, and computers. Optimization is the action of making the best or most effective use of a situation or resource.

Gas - Any usage token associated with a blockchain-based smart contract development platform. Two good examples of platforms that use gas are Ethereum and Neo. For Ethereum, the network uses very small amounts of the Ether token itself (symbol ETH) as a gas token. For the Neo project, there is a separate gas token which is appropriately called Gas (symbol GAS). In terms of the gas token on the Neo platform, GAS is the token used to pay for all the service fees on the blockchain (service fees are different than transaction fees, and transaction fees on Neo are free). Any company that desires to register or change assets on the blockchain will have to acquire GAS to pay for the service fees. The service fee for registering or changing assets will be distributed proportionally to all NEO holders, so GAS is never destroyed.

Gateway – A specific category of exchange that allows a person to deposit traditional fiat money into the exchange in order to purchase crypto assets. Some exchanges do not allow the deposit of fiat, and on those exchanges, you have to deposit Bitcoin or other cryptocurrencies into the exchange to be able to start trading. Within the US market, Coinbase and Gemini have traditionally been known as the main gateway exchanges, and Bittrex was an example of a non-gateway exchange that did not accept traditional fiat US dollars for the first several years that it was in operation. You would think that every exchange would want to be able to accept fiat for trading, but accepting fiat usually involves dealing with a huge number of government and banking regulations, which is why some exchanges like to keep things more simple and avoid trades with fiat currencies.

Genesis Block – The first block in a blockchain.

GitHub - A web-based collaboration platform that lets developers all around the world work on projects simultaneously.

Golden Nonce – Any nonce in a proof-of-work system which results in a hash that "solves" the current block.

Gox'd - To become the victim of a hack, particularly one in which your cryptocurrency gets stolen. This is in reference to the large hack that shut down the Mt. Gox Bitcoin exchange in 2014. Another similar sounding but completely unrelated hack is when a person get dox'd, which refers to their identity and personal private information (addresses, phone numbers, social security numbers, banking info, etc.) getting shared on the internet or with other hackers.

Graphical Processing Unit (GPU) - A computer chip or processor that is designed to specialize in display functions. Graphical Processing Units render images, animations and video for the computer's screen. GPUs are often located on separate cards which can be plugged into the motherboard on a computer. Some GPU's are chips that are embedded right into the motherboard at the factory, or coupled with the CPU of the computer. Because GPU's are very good at performing incredible amounts of fast transactions (measured in terms of their hash rate), they are often tasked to perform complex mathematical tasks that a computer is asked to do. The mining of cryptoassets in any Proof of Work system is usually a complex mathematical task that is ideal for GPU's. GPU's can often "mine" cryptocurrencies much faster than a CPU can. The most popular GPU's on the market today are Nvidia's line of "GeForce" GPU's. A less common brand, but one which still has a significant market share, is AMD's "Ratheon" line.

Graphical User Interface (GUI) - A type of user interface that allows users to interact with electronic devices or apps or software through graphical icons and visual indicators, instead of having to use text-based user interfaces or typed commands in a command-line interface (CLI). A GUI is usually significantly more user-friendly than command-line interfaces, especially for people who are less familiar with computer technology.

Green Coins - Coins which do not use energy-consumptive Proof-of-Work algorithms as a means of mining or maintaining the security of their network.

Halvening (or Halving) - This event only occurs with certain cryptocurrencies. Some examples include the Bitcoin family, Litecoin, and Vertcoin. The halvening for those projects occurs approximately every four years and signifies a reduction in the rate in which new coins are released. When a halvening happens, there is a decrease in the number of coins given to a miner as a reward for mining a block. Bitcoin underwent a halvening in 2016, and at that time, the block reward dropped from 50 coins per block to 25 coins per block. When a halvening happens, there is no effect upon the current supply of the currency, however, going forward, the inflation rate (generation of new coins) is cut in half, which in theory makes the currency slightly more valuable (or to be more precise, inflation does not reduce the value as quickly). When a halvening happens, miners suddenly realize that their long-term mining revenues are cut in half, which means that their profits (revenues less expenses) are cut even more (on a percentage basis). This has the effect of driving hash power out of the network to other, more profitable coins to mine. Block difficulty algorithms will also start adjusting for the lower hash rate, making it easier for the remaining miners to mine blocks. The mining power on the network will eventually come to a new equilibrium.

Hard Fork - A radical change to a blockchain protocol that makes previously invalid blocks/transactions valid, or vice-versa. It requires all nodes or users to upgrade to the latest version of the protocol software. A hard fork is a permanent divergence from the previous version of the blockchain, and nodes running previous versions will no longer be accepted by the newest version. This essentially creates a fork in the blockchain, with one path which follows the new, upgraded blockchain, and another path which continues along the old path. Generally, after a short period of time, those on the old chain will realize that their version of the blockchain is outdated or irrelevant and quickly upgrade to the latest version. A hard fork can be implemented to correct important security risks found in older versions of the software, to add new functionality, or occasionally to reverse a large group of transactions (this happened once after an Ethereum hack with the DAO project).

Hash - A term used commonly in computing. A hash (noun) is the output of a computation or calculations on a computer. Hash can also be used as a verb, where "to hash" means the same as "hashing" or "performing the hash function.” When you consider a hash to be an object, it is usually a specific type of data on a computer, such as an alphanumeric string or an integer or a real number. A hash can have a defined size, length, or range. For example, a hash in one particular computing environment may be mandated to be a 27 character long alphanumic string where all letters must be lowercase. Another option could be that a particular hash could be required to be a 16-bit integer, which means an integer between the values of 0 and 65535.

Hash Function - A computing process which analyzes input(s), and then outputs a string or number which is based specifically upon rules or mathematical formulas that were applied to the input(s). The input objects are usually members of basic data types like strings, integers, or bigger ones composed of other objects like user defined structures. The output (regardless of the exact type) is called the "hash." Some examples of hash functions used in various cryptoasset mining protocols include CryptoNight, Equihash, Lyra2REv2, SHA256, and NeoScrypt.

Hash Rate - The number of times a specific hash function can be computed per second. The hash rate is typically expressed in hashes per second, or h/s. Remember that various prefixes can qualify the hash rate: "k" stands for kilo (thousand), "M" stands for mega (million), "G" stands for giga (billion), and the prefix "T" stands for tera (trillion). So a computer performing 2.73 Mh/s is performing 2,730,000 hashes per second, or taking 2.73 million different inputs and calculating the appropriate corresponding outputs, every second. Be aware that different hash functions can result in different hash rates, depending upon the complexity of the calculations in the hash function. For example, a given computer and GPU might be able to return 14.7Mh/s of the Lyra2REv2 function, but only 2.19Mh/s of the CryptoNight function, because the functions are of different complexity.

Hodl - A meme that means "hold" or "to hold" cryptocurrency for the long term. "I'm hodling" means that you're not selling your crypto, often proclaimed when the market price is dipping or in a correction. Visit the memes page on our website for a link to see where this particular spelling originated. Interestingly, it is also a good acronym for "Hang On for Dear Life."

Honey Pot - In traditional InfoSec terminology, a honey pot is a decoy computer system that is set up in order to trap hackers, or to track unconventional/new hacking methods. Honey pots are designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet. Multiple honey pots can be set on a network to form a honey net. With respect to cryptocurrencies, the term has often become perverted to also refer to any sites used by scammers to lure investors in an attempt to defraud them. In such a case, a better term would [sometimes] be "watering hole."

Hot Wallet - A wallet of any type (be it physical or software) that is connected to the internet.

Immutability - This happens when an object is characterized as being impossible to change. It is desirable for a blockchain to have immutable records/blocks, so that everybody knows that nobody has ever had the ability to go into blockchain records to edit, change, or falsify the information contained therein.

Independent Management Architecture (IMA) - Provides a framework for server communications. By this, we mean how servers talk to other electronic technology. This is heady computer stuff, move right along.

InfoSec - The field of study/practice relating to information security, or the protection of digital assets.

Initial Coin Offering (ICO) - An unregulated and controversial means of crowd-funding via use of cryptocurrency, which can be a source of capital for start-up companies. In an ICO, a percentage of the newly issued cryptocurrency is sold to investors in exchange for legal tender fiat or other cryptocurrencies (Bitcoin, Ethereum, etc.). The term may be analogous with 'token sale' or crowd-sale, which refers to a method of selling opportunities for participation in an economy, giving investors access to the features of a particular project starting at a later date. ICO's may sell a right of ownership or royalties to a project, in contrast to an initial public offering (IPO) in traditional markets, which sells a share in the ownership of the company itself. The coin in an ICO can be considered to be a symbol of ownership interest in an enterprise. ICO's can be used for a wide range of activities, ranging from corporate finance to charitable fundraising to outright fraud. The US Securities and Exchange Commission (SEC) has warned investors to beware of scammers using ICOs to execute "pump and dump" schemes, in which the scammer talks up the value of an ICO in order to generate interest and drive up the value of the coins, and then quickly "dumps" the coins for a profit. However, the SEC has also acknowledged that ICO's, "may provide fair and lawful investment opportunities." The UK Financial Conduct Authority has also warned that ICO's are very high risk and speculative investments, are scams in some cases, and often offer no protections for investors. Even in the case of legitimate ICO's, funded projects are typically in an early and therefore high-risk stage of development.

Internet of Things (IoT) - The network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity, which enables these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system, but is able to inter-operate within the existing Internet infrastructure. Experts estimate that the Internet of Things will consist of about 30 billion devices by 2020.

Invisible Internet Project (I2P) - A network layer that allows for censorship-resistant, peer to peer communication. It is a decentralized anonymizing network built on similar principles to Tor, but which was designed from the ground up as a self-contained darknet. I2P was built with open source tools and is designed to run traditional internet services including email, IRC and web hosting.

Jinn Processor - A type of general purpose ternary processor, which uses a three-state architecture rather than the traditional two-state binary that most processors have always used.

Key Logger - A type of malware that is secretly installed on your computer, then discretely records all your key strokes and sends them all to a bad actor. The hacker can therefore see everything you type, which includes all the website URLs you enter, the emails you write, and most importantly, private keys to crypto wallets that you might be typing (or cutting/pasting) into your computer.

Know Your Customer (KYC) - The process whereby a business identifies and verifies the identity of its clients. The term is also used to refer to banking and anti-money laundering regulations which govern these activities. This phrase/acronym is often used simultaneously with anti-money laundering, for example, "The Bittrex Exchange just shut down several thousand accounts worldwide because the exchange was trying to ensure compliance with KYC and AML regulations."

Lambo - Short for Lamborghini. It is the dream of some crypto investors to be able to make enough money to be able to ostentatiously flaunt their new wealth by spending it on one of the world's most expensive supercars.

Ledger - In general terms, a ledger is a collection of financial accounts of a particular type. Within the cryptosphere, the public ledger is also known as the block chain. It is a public record of transactions in chronological order. Its structure is time-stamped such that transactions can be proven to have been carried out by the owner of the coins/tokens at that time, and ownership of any particular coins/tokens (or fractions thereof) can always be tracked back through a series of transactions to the original creation of the asset being utilized on the ledger. Many blockchain ledgers are publicly viewable, although there are some (such as for a privacy coin like Monero, or for private blockchains created by a corporation for confidential internal use) which cannot be seen/explored by the general public (or in the case of Monero, by anyone). Note that there is also a professional scientific journal called The Ledger, which is a peer-reviewed scholarly journal that publishes full-length original research articles on the subjects of cryptocurrency and blockchain technology.

Lightning Network (LN) - A proposed implementation of Hashed Timelock Contracts (HTLC’s) with bi-directional payment channels, which allows payments to be securely routed across multiple peer-to-peer payment channels. This allows the formation of a network where any peer on the network can pay any other peer even if they don’t directly have a channel open between each other. The Lightning Network is a proposed long-term solution to Bitcoin’s current transaction-processing bottleneck, although there is widespread disagreement over whether or not the Lightning Network can ultimately be implemented successfully as anything other than a niche or specialty feature.

Liquidity - Describes the degree to which an asset or security can be quickly bought or sold in the market without affecting the asset’s price. Market liquidity refers to the extent to which a market, such as a cryptocurrency exchange, allows coins/securities to be bought and sold at stable prices.

Limit Order - An order on an exchange in which you need to specify an exact "worst case scenario" price at which you are willing to trade. Note that if there is a better price available to you, the exchange is supposed to try to ensure that you get the better price. For example, let’s say that there are 50 ExampleCoins offered for sale for $7.00 each, and 200 ExampleCoins offered for sale for $7.20 each, but that’s it. You put in a Limit buy order for up to 150 ExampleCoins with a Limit price of $7.10. The exchange will immediately match the offer of 50 ExampleCoins at $7.00 each, because that volume doesn’t exceed your limit (and the coins are cheaper than the maximum price that you are willing to pay per unit). But that’s all that you’ll end up buying, since the rest of the ExampleCoins are being offered at a price higher than you said you’d be willing to pay. The remainder (100 more ExampleCoins) of your order will sit unfilled until someone else is willing to place a Limit sell of $7.10 (or less) for their ExampleCoins, OR places a Market sell (which sells their securities immediately at the best price people are willing to buy). An unfilled Limit order may sit on the exchange for minutes or hours or days, or may never be filled. Exchanges sometimes impose arbitrary maximum time limits for Limit orders, perhaps only allowing a month or sixty days into the future from the time the order was placed.

Mainnet - The official working public platform or blockchain for a project. After a project has been vetted using a testnet, and the developers feel that it is ready for public launch, they release the mainnet.

Man In The Middle (MITM) - In hacking, this is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. Also known as a Janus attack.

Margin Call - Occurs when the value of margined securities in your account drops below a certain point. Depending on the brokerage/exchange, your securities may be sold instantly, regardless of market price, in order to preserve capital (to be able to repay the margin). In other cases, with traditional stock exchanges and traditional non-discount brokers, your broker may actually phone you and let you know that you have 24 hours to fund your account with a certain amount of money (either by depositing cash, or by selling shares of other securities) and if you fail to comply by the deadline, then the broker will arbitrarily unload your position. See also the Margin Trading definition.

Margin Trading - Buying on margin means that you are borrowing money from a broker or exchange to purchase securities. You can think of it as a loan from your brokerage/exchange. Margin trading allows you to buy more securities than you'd normally be able to. To trade on margin, you specifically need a "margin account." Of course, brokerages/exchanges don't just loan out money freely. You'll need to secure your margin against some kind of collateral, which is usually other securities/value in your account. In the traditional stock markets, only certain securities (medium-risk and low-risk) are marginable. The entity loaning the money to you will put certain rules in place to ensure that they get it back. For example, if the value of your securities drops below a certain predetermined point, your securities may automatically be sold (at a loss) by the brokerage/exchange so they can ensure that they get their original loan back. A sudden margin call can really wipe out an investor.

Market Capitalization - The temporary market value of a company's outstanding shares/securities. This amount is determined by taking the stock price and multiplying it by the total number of shares outstanding. This is a very arbitrary and sometimes misleading figure, as the "market value" of the shares is usually determined by the trade price on the last share traded. So for example, let's say that we're talking about a huge company that has a billion shares outstanding, and the price per share usually trades in the range of several hundred dollars. If the last trade of the day was a computer-generated downtick of $2 placed intentionally in the last millisecond of trading, then that single trade would instantly knock two billion dollars off the market cap of the company. Did the value of the company actually change by two billion dollars in that fraction of a second? It's hard to say. There are a lot of diverse ways to value a company. In terms of crypto, it could be possible for someone with deep pockets to do a lot of wash trading (from themselves right back to themselves) in order to artificially set a high trade range for their cryptoasset, and fool the market into thinking that the project is much more valuable than it would be without this devious manipulation. In most cases, the market capitalization of a project is a fairly accurate way to gauge the relative performance of the project within the marketplace. Sometimes, when someone is talking about market capitalization, they are referring to the total cumulative value of the entire cryptoasset ecosphere, rather than of one specific project. Be aware that (at the moment) the overall crypto market capitalization moves very much in lockstep with the price of Bitcoin, since Bitcoin makes up such a large proportion (greater than half) of the perceived financial value of the cryptosphere as a whole.

Market Order - An order (buy or sell) placed with no price restrictions in place. If there are enough shares offered by other market participants on the opposing side of the bid/ask, then the market order will get filled at the best available price(s). For example, if the order book on an exchange currently lists ExampleCoin for sale with 10 coins on the ask at $10.50 and 70 coins on the ask at $10.60 and 720 coins on the ask at $10.70, and buyer John Smith places a market buy order for 100 coins, then he will pay $10.50 each for his first 10 coins, $10.60 each for his next 70 coins, and $10.70 each for his last 20 coins. The disadvantage of market orders is the lack of price control (you have to accept what is on the current order books), so the price is not usually as competitive as placing a Limit order. The advantage of a market order is speed, which can be important if you're in a rush and if a possible minor disadvantage in pricing doesn't matter to you. A market order will almost always get filled immediately, within a second or so of being placed, whereas with a limit order you have to wait for someone to meet your price, which could be minutes or hours or days or never.

Market Sentiment - The feeling or tone of a market, or its crowd psychology, as revealed through the activity and price movement of the securities traded in that market. Basic categories for market sentiment can include bearish (negative), neutral, or bullish (positive). Uncertainty is also another factor to consider.

Market Maker (MM) - A dealer in traditional securities or other assets who undertakes to buy or sell at specified prices at all times, by simultaneously having large open bid and ask orders on the security. In some cases, the market maker (also known as liquidity provider) is a company or an individual hoping to make a profit on the bid-offer spread, or turn/churn. There are almost always people buying and selling any given security, so if the market marker is always prepared to buy securities that are offered at a specific price, and simultaneously sell the same securities at a slightly higher price, they are constantly accumulating money. Some market makers are not actually doing it for the profits on the spread; in some cases, a promotions firm or issuer of the security could hire a market maker to create an artificial trading range for the security. Be aware that in traditional finance, this practice is not legal in many jurisdictions.

Mechanical Turk - A person who is hired to perform repetitive, intelligence-based tasks. Amazon Mechanical Turk is a crowdsourcing internet marketplace which enables individuals and businesses (known as Requesters) to coordinate the use of human intelligence to perform tasks that computers are currently unable to do. Some examples of such human intelligence tasks (HIT's) might include classifying the color of birds in a series of photos, or listening for specific audio cues in a series of audio files.

Mempool - Any cryptoasset project's network holding area for transactions that have been initiated but not yet confirmed. A transaction is not confirmed until it is included in a block.

Merkle Tree – A data structure used in cryptography and computing sciences. The structure is set up so that each "leaf node" on the tree (termini) is a hash of a data block, and each node that is not a leaf node has the cryptographic hash of the labels of its child nodes. Merkle trees are often binary at each node, but this is not necessarily a requirement for all Merkle trees.

Meta Coins - Meta coins are extensions of the Bitcoin protocol that use either a new blockchain or tie into Bitcoin's blockchain (while adding more features). Meta coins that are built using Bitcoin's blockchain are said to be on-chain, and those with their own blockchain are said to be off-chain. The basic idea of meta coins is to offer additional functionality to Bitcoin, such as distributed exchanges, CFD's, digital assets and various forms of contracts.

Miner - Can refer to different things. A miner can be a single person engaged in mining on a small scale, or it can be a large entity (corporation, foundation, server farm) that engages in mining on a large scale. It can also refer to a software package or app used for mining, or to a physical machine/device used for mining.

Minimum Balance - Some types of cryptoasset wallets (especially those designed by the developers of the crypto projects themselves) require a certain minimum amount of the asset to open a new wallet, and require the user to always maintain that same amount as a minimum balance. For example, Ripple at one point had a minimum balance of 125 XRP. If you had 200 XRP in your wallet and tried to withdraw all of it, you'd only be able to withdraw 75 XRP, because the other 125 XRP would remain locked in the wallet (the minimum balance number has since changed a few times). This is a smart idea on the part of the developers, because it ensures that a small portion of the trading assets are locked up, and it encourages users to hold some assets. It also discourages people from setting up a ton of empty wallets, although there is no real cost to that practice for most cryptoassets.

Mining - The process by which some cryptocurrency transactions are verified and added to the public ledger (the blockchain), and also the means through which new coins may be released. The mining process involves compiling recent transactions into blocks and trying to solve a computationally difficult puzzle. The participant who first solves the puzzle gets to place the next block on the block chain and claim the rewards. The rewards, which incentivize mining, are both the transaction fees associated with any transactions compiled in the block as well as newly released Bitcoins. Not every cryptoasset project uses mining to process transactions and to create new coins, but it is a common approach. A project that is referred to as a "Proof of Work" system relies on mining. In theory, anyone with access to the internet and suitable hardware can participate in mining. In practice, however, mining for some cryptocurrencies has become so challenging that only large-scale mining farms using specialized equipment (referred to as ASIC's) are now able to mine profitably.

Mining Rig – A computer designed and built specifically with cryptocurrency mining in mind. Chances are high that it was a fairly powerful computer when it was first built, and probably includes one or more high-end video cards

(GPU’s) to help process mining algorithms efficiently. It may also be used for additional purposes (internet, work, gaming) but in many cases, a crypto enthusiast may design a rig specifically to be used for mining and will use a different computer for all other applications.

Mixing - See "Tumbling."

Moon - Slang for that fantasy world where crypto investors will live once the value of their portfolio has grown to unbelievable wealth. To say that a cryptoasset is going to "moon" means that one believes the trading value of the coin is going to skyrocket and increase in value by many times the current trading price. There is no specific multiplier that qualifies as mooning; that’s up to the personal preference of the investor. Some investors may see a 10x return on investment (a ten-bagger in the traditional stock investment community) as qualifying as mooning. Others expect gains of 100x or more. In the traditional stock markets, gains of this nature are almost unheard of. Thanks to huge gains in Bitcoin and many other cryptoassets between 2012 and 2017, a lot of participants seem to think that gains of 100x and more are "normal." They aren’t. As the cryptoasset industry continues to mature, there will be a flight to quality, and many projects will decrease in value or collapse. To be sure, some excellent individual projects will probably see gains similar to what Bitcoin experienced, but in most cases, more rational trading and valuations will eventually become the norm. Enjoy the volatility while it lasts.

Mt. Gox - A Bitcoin exchange that was based in Shibuya, Japan. In 2013, it was handling over two-thirds of global Bitcoin transactions. However, in February of 2014, it suspended trading and shut down its website and exchange service, and filed for bankruptcy protection from creditors. At that time, Gox announced that approximately 850,000 Bitcoins belonging to customers and the company were missing and likely stolen. The reason(s) for the disappearance (possibly theft, fraud, mismanagement, or a combination of these) were initially unclear. More recent evidence suggests that most or all of the missing Bitcoins were stolen straight out of the Mt. Gox hot wallet over an extended period of time, beginning in late 2011. Claims are still being processed by the courts, although it is doubtful that most investors will get more than a fraction of their holdings back, at best. Even if they recover their initial investments (in terms of fiat value), they probably will not recover capital gains to that point, nor would they likely be able to realize any opportunity costs that might have accrued to them had they held Bitcoin assets past the time of the suspension of trading.

Multisig - Short for multi-signature. A digital signature scheme which allows a group of users to sign a single document, or to authorize a specific transaction. Usually, a multi-signature algorithm produces a joint signature that is more compact than a collection of distinct signatures from all users. Multisig allows for a form of escrow (see also the Escrow definition). For example, a contract can be set up on a blockchain or for a cryptocurrency transaction whereby any two of three possible users must authorize the transaction (by signing, ie. providing a private key) before the transaction is allowed to be processed on the blockchain. Other multisig sizes are also possible, ie. a contract can specify that any three of seven users must sign. A good example of a situation (besides escrow) where multisig is possible or useful would be a situation whereby a board of directors all has access to a pool of funds for a project, and three of seven members of the group must all sign for a transaction to be processed. This way, a single member of the board can’t send funds to someone without other members of the board being complicit in facilitating the transaction.

Nash Equilibrium - Occurs when every player in a non-competitive game has nothing to gain by deviating from his own current strategy.

Near-Field Communication (NFC) - A set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within approximately 4 cm (1.6 in) of each other. NFC devices are used in contactless payment systems, similar to those used in credit cards and electronic ticket smartcards and allow mobile payment to replace/supplement these systems. NFC is used for social networking, and for sharing contacts, photos, videos or files. NFC enabled devices can act as electronic identity documents and keycards.

Nonce - A random or semi-random number generated in a cryptographic hashing function. It is believed to stand for the phrase “number used once.” In proof-of-work (mining) systems, a nonce is used to create a cryptographic hash, with the hope of “solving” the mining equation for the current block.

Normie - A "normal" person who has not yet gotten involved in the world of using and investing in cryptoassets.

Nvidia - An American technology company based in Santa Clara, California. It designs graphics processing units (GPUs) for the gaming, cryptocurrency, and professional markets, as well as system on a chip units (SoCs) for the mobile computing and automotive market. These graphic cards are usually the most sought-after in terms of conventional GPU-based mining rigs which are affordable to many people within traditional consumer markets. Nvidia's main graphic card line at the moment is the GeForce line. Nvidia's main competitor is AMD with their "Radeon" GPU line. Nvidia is typically ranked as the leader in the market, in terms of price/performance analysis, and best capabilities.

Obfuscation - The action of making something obscure, unclear, or unintelligible. Sometimes, when a crypto project is being criticized on social media, defenders of that project resort to obfuscation to try to deflect criticism, by pointing out alleged solutions in a manner that lay users may not understand.

Open Source - Computer software that has its source code made available with a license whereby the copyright holder(s) provide the rights to study, change, and distribute the software to anyone and for any purpose. Open-source software may be developed in a collaborative public manner, and in fact, quite a few cryptoasset projects have been developed in such a collaborative manner. Diverse groups of developers from around the world often donate their time on a volunteer basis to their project(s), simply because they know they are making contributions which will benefit people from around the world.

Oracle - A computing mechanism for determining whether a test has passed or failed. The use of oracles involves comparing the output(s) of the system under test, for a given test-case input, to the output(s) that the oracle determines that product should have. Oracles often operate separately from the system being tested.

Order Book - The list of orders that an exchange uses to record the interest of buyers and sellers in a particular security. A "matching engine" uses the order book to determine which new orders can be fulfilled.

Order Completion – See “Fill.”

Overclocking – Setting up a CPU or GPU to run at a rate faster than the manufacturer’s specifications. Overclocking allows a user to increase performance, but comes at a risk of possibly damaging the component (usually through overheating).

Patch - A "fix" or revision to computer code, to make it more secure and/or efficient. Most patches are issued to resolve security vulnerabilities.

Permissioned Blockchain - A private blockchain, which the general public can’t examine or use. This type of blockchain requires a user to possess certain credentials to gain access, and to interact with it.

Plaintext - Text or written information that has not been encrypted. Sometimes referred to as cleartext.

Plasma - A protocol that allows for a tree of blockchains on Ethereum in order to hyper-scale transaction capacity. Designed as a mid-term solution for scalability in Ethereum.

Platform - The environment in which a piece of software or code is executed. Some cryptoassets can be best defined as platforms. Common examples include Neo, Ark, and Ethereum. All crypto platforms share the ability for users to develop smart contracts on the platform, and also to develop entire new crypto projects that are based upon the framework of the platform. By using a platform such as Neo, Ark, or Ethereum as the basic framework for a project, developers of that new project are able to build upon the coding achievements of previous developers, so they aren't building their new project completely from the ground up. An analogy could be this: Rather than building a house on an undeveloped property, where trees have to be cut and the ground has to be leveled and heavy equipment needs to excavate and prepare a foundation, the developer is able to start working on a site where the foundation is already set in place and the house just needs to be built on top.

Polo - Slang for the Poloniex exchange.

Post Only Order - A limit order where the bid or ask is for a price that is currently not on the order book, thus adding liquidity and being considered a "maker" order. On traditional stock exchanges such as NASDAQ, Post Only orders usually also have to be displayed orders (not hidden or non-displayed).

Proof of Authority (PoA) - A system that can act as a replacement for POW, and which can be used effectively for some private chain setups. Proof of Authority is suitable for centralized blockchain projects. POA does not depend on nodes solving arbitrarily difficult mathematical problems, but instead uses a set of "authorities," which are nodes that are explicitly allowed to create new blocks and secure the blockchain. The chain has to be signed off by the majority of authorities, at which point it becomes a part of the permanent record. This makes it easier to maintain a private chain and keep the block issuers accountable. In an enterprise/consortium setting, there are no disadvantages to a POA network as compared to POW. It is more secure, less computationally intensive, and since blocks are released at specific time intervals, it is more predictable.

Proof of Brain (PoB) - This consensus reward algorithm encourages people to create and curate content. It is used on platforms such as Steem. It enables tokens to be distributed by "upvote" and "like"-based algorithms, and can be integrated with websites to align incentives between application owners and community members to spur growth.

Proof of Burn (PoB) - A method for distributed consensus which is not as common as protocols including Proof of Stake, Proof of Work, etc. In Proof of Burn, miners show proof that they burned some coins or tokens by sending them to a verifiably unspendable address. This is expensive from their individual point of view (just like proof of work) but it consumes no resources other than the burned underlying asset. To date, all PoB cryptocurrencies work by burning separate PoW cryptocurrencies, so the ultimate source of scarcity remains the proof-of-work efforts in those other cryptocurrencies. For example, SlimCoin uses a PoB system, and Bitcoin is the currency burned in that system.

Proof of Concept (PoC) - This is not a type of consensus system, despite the similarity in name. Proof of concept refers to evidence, typically derived from an experiment or pilot project, which demonstrates that a design concept, business proposal, or network build-out is feasible.

Proof of Devotion (PoD) - This consensus mechanism gives an "influential" user on the blockchain network an opportunity to become a bookkeeper and receive block rewards and transaction fee as revenue, which will encourage them to contribute to the stability and security of the blockchain on a continuous basis. Users with high ratings take part in the bookkeeper selection procedure by paying a security deposit. Through virtual mining, each bookkeeper candidate competes to earn bookkeeping rights. Users with bookkeeping right are responsible for block generation, and in return receive block reward and transaction fee as revenue. If any user behaves in an inappropriate fashion, the user's security deposit will be confiscated and reassigned to other bookkeeper candidates.

Proof of Research (PoR) - In this system, each participant contributes to research by performing computations in the network, somewhat similar to a PoW system. Gridcoin, which is associated with the BOINC network, is a good example of this type of system. The network average in a PoR system is similar to the "difficulty" in PoW mining. As the network average hashrate rises, it becomes harder to get the same "magnitude" (share of the overall hashrate), so to keep getting the same reward you would need to increase your computing contribution. If the price rose significantly and more computing power came on board (raising the overall network hashrate), it would become harder for a single entity with a constant rate of research contributions to get the same reward.

Proof of Stake (PoS) - Proof of Stake is a form of distributed consensus system which validates transactions in order to achieve the distributed consensus. It is still an algorithm, and the purpose is the same as PoW, but the process to reach the goal is quite different. In a Proof of Stake system, the creator of a new block is chosen in a deterministic way, depending on the creator's wealth (also defined as stake). PoS systems have no block reward, and instead the creators of blocks only receive the transaction fees in those blocks. This is why the creators of blocks in a PoS system are called Forgers instead of Miners.

Proof of Work (PoW) - A system that requires some work from the service requester (or miner), usually meaning processing time or CPU cycles on a computer. The specific work that must be performed has to be hard enough to make it challenging to complete, yet also easy enough to be feasible. Complex mathematical calculations of slowly increasing difficulty are the norm. More importantly, it must be easy for the service provider to validate the veracity of the provided answer. This idea is also known as a CPU cost function. There is a specific cost for computers to perform large numbers of calculations, which can be calculated in terms of electricity consumed, cost of hardware and components, and other incidentals. Although some miners in certain jurisdictions may have some advantages due to things like lower costs of power, or specialized computers (ASIC's) that are extremely efficient at performing calculations, the basic tenet is that the consumption of computing resources acts as a barrier to ensure that other miners have to pledge similar resources to the system in order to gain mining power. Therefore, if a PoW network grows to a point where very large numbers of computers are devoting their resources to mining, those computers can also be thought of as providing security to the network, because the costs for someone to expend a greater number of resources to overcome or "attack" the existing network would be prohibitive. Therefore, although PoW systems on major cryptocurrencies are criticized for consuming enormous amounts of electricity, it can also be pointed out that this consumption of resources is exactly what provides security to the system and maintains the integrity of the underlying asset. If Bitcoin were to suddenly become the central global currency of choice, it would be a fatal problem if someone were to be able to spend a few million dollars to game the system, therefore, there must be a significant economic outlay required to obtain power (mining hashrate) in the system.

Public Key Infrastructure (PKI) - Digital identities are based on a system called the PKI X.509 standard. This is an internationally agreed-upon standard for what constitutes a digital identity.

Public Ledger - See "Ledger."

Pull Request - A method of submitting contributions to an open development project. It is often the preferred way of submitting contributions to a project using a distributed version control system. A pull request occurs when a developer asks for changes committed to an external repository to be considered for inclusion in a project's main repository. It is important to note that "pull requests" are a workflow method, and are not a feature of the version control system itself.

Pwn - The act of dominating an opponent, originating from a typo on a World of Warcraft map from many years ago. In context, if a hacker manages to compromise your system and steal your assets, then you have been pwned.

Quantum Computing (QC) - Quantum computers are incredibly powerful machines that take a new approach to processing information. Built on the principles of quantum mechanics, they make direct use of quantum-mechanical phenomena, such as superposition and entanglement, to perform operations on data. Quantum computers are different from binary digital electronic computers (which are based on transistors). Whereas common digital computing requires that the data be encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1), quantum computation uses quantum bits, which can be in superpositions of states. Although Quantum Computing is still in its infancy today, the possibility exists in a few years that quantum computers will be unbelievably more complex than even the best computers that exist today, and will be able to solve problems that scientists simply didn't think were solvable. There is also some concern in the cryptocurrency community that quantum computers will eventually be able to break the encryption standards used in various projects, which basically means that someone with a quantum computer could empty everybody's wallets. While that is a definite concern, that sort of a situation is probably at least a decade away, and there should be adequate time in the interim for any developers to create new quantum-resistant or quantum-proof cryptography.

Quantum Supremacy (QS) - The ability to tackle a problem too complex to solve on any standard supercomputer.

Quick Response (QR) Code - A type of barcode that contains a matrix of dots. It can be scanned using a QR scanner, or a smartphone with built-in camera. Once scanned, software on the device converts the dots within the code into numbers or a string of characters. For example, scanning a QR code with your phone might open a URL in your phone's web browser. All QR codes have a square shape and include three square outlines in the bottom-left, top-left, and top-right corners. These square outlines define the orientation of the code. The dots within the QR code contain format and version information as well as the content itself. QR codes also include a certain level of error correction. QR codes have two significant benefits over traditional UPCs (the barcodes commonly used in retail packaging). First, since QR codes are two-dimensional, they can contain significantly more data than a one-dimensional UPC. Another advantage of QR codes is that they can be scanned from a screen (like a smartphone) regardless of orientation. Public and private keys can both be encoded as QR codes, which makes it very easy for someone to quickly share a public key with others via screen scan, and not have to worry about cutting and pasting or retyping a long and complex set of alphanumeric characters.

Raiden - The Raiden Network is an off-chain Ethereum scaling solution, enabling near-instant, low-fee and scalable payments. It is complementary to the Ethereum blockchain and works with any ERC20 compatible token. The Raiden project is a work in progress. Its goal is to research state channel technology, define protocols, and develop reference implementations. It is designed as a near-term solution for scalability in Ethereum. Raidan scales linearly with the number of participants. Transfers can be confirmed in less than a second. It is somewhat more private, in that individual transfers don't show up in the global shared ledger. It works with any token that follows Ethereum's ERC20 protocol. Transfer fees can be orders of magnitude lower than on the blockchain, which allows for micropayments (the transfer of very tiny values).

Rekt - Slang for "wrecked." Someone can get rekt financially (suffer large losses) or get rekt in an argument or game/contest (destroyed by an opponent).

Repo - Short for Repository. This is a location where coders and developers store code/apps/software on a server for public or private access. GitHub is probably the most well-known. Some cryptoasset projects which are open source and publicly shared will store all code on a repository, for anyone to download and examine. If you see that there is a lot of activity in the repository, you can see what kind of code changes are happening and determine if the project has a lot of active developer support. Be aware though that for some projects, most of the development activity takes place on private repos, so you may not be able to see much happening even though there may still be a lot of active development happening in the background.

Rich List - A list of the most valuable wallets or public addresses (usually the top 100) for a particular cryptocurrency. The blockchain explorers for most cryptocurrencies have an option to display the rich list, or perhaps even all addresses ranked by the size of holdings. Some explorers also give a great deal of additional statistical information, such as the percentage of the total float being held in the top 10 wallets, top 100 wallets, top 500 wallets, etc.

Rig – See "mining rig."

Ring Signature - A type of digital signature that can be performed by any member of a group of users that each have keys. Therefore, a message signed with a ring signature is endorsed by someone in a particular group of people. However, it is important that the identity of the specific individual member who signed the transaction must remain hidden.

Ring Confidential Transactions (RingCT) - Coded transactions which have been designed to hide the amount of Monero sent in any specific transaction. Ring Confidential Transactions are one of the three key ways that Monero ensures privacy of transactions (hiding the sender, hiding the receiver, and hiding the amount transferred).

Scalable Transparent Argument of Knowledge (STARK) - A theorum proofing system that features perfect witness indistinguishability, is publicly verifiable, has no trusted setup, is universal, and has succinct verification. It is scalable and post-quantum secure. It's a feature used in privacy situations for certain cryptographic projects.

Scaleability - The capability of a system, network, process, or blockchain to handle a growing amount of work, throughput, or transactions, or its potential to be enlarged to accommodate that growth.

Second Layer Solution - The use of alternative and interconnected blockchain networks to complement an existing blockchain project. Large cryptocurrencies and platforms such as Bitcoin and Ethereum began to experiment with research and development of second layer solutions in 2017 in order to start trying to solve scalability issues. For many projects, once the scale of the projects reaches a point where transactional bottlenecks begin to occur, it becomes evident that true scalability can only be reached if users do not have to verify every transaction sent to the main blockchain. In fact, it is highly impractical and inefficient to handle every single piece of information that is sent to the main blockchain. Some potential second layer solutions that are being considered include Plasma or Raidan (for Ethereum), and the Lightning Network (for the Bitcoin family).

Segregated Witness (SegWit) - The process by which the block size limit on a blockchain is increased by removing signature data from blockchain transactions. When certain parts of a transaction are removed, this frees up space or capacity to add more transactions to the chain. Segregated Witness has been activated on several blockchains including Bitcoin, Litecoin, and

Vertcoin. Segregate means to separate, and Witnesses are the transaction signatures. Hence, Segregated Witness means to separate transaction signatures.

Seed - A seed phrase is a specific collection of common words, in a particular order, which acts like a complex password. Seed phrases can have a varying number of words, but 12 word seeds and 24 word seeds are both common, and different numbers of words are also possible. Unlike a pass phrase that might be used to get into a wallet or website, a seed phrase actually generates a specific public and private key.

Sell Wall - A sell wall on an exchange is a large order(s) at a certain price that acts as an obstacle to restrict the trading price from rising. If the sell wall is large enough, there may not be enough buyers to overcome it and push the market price higher. For instance, if certain whales don't want the price of Ethereum to go above $1000, because they think that would be a psychological barrier and prices could skyrocket if that price is breached, then they may want to put up a large sell wall of tens of thousands of Ethereum at $985 or some value in that area. It would then take a lot of buyers to eat through all of the coins offered at that level and bring the market trading price up into four digits.

Sentiment Analysis (SA) - The process of identifying and categorizing opinions expressed in the news, articles, or on social media, especially in order to determine whether the market's attitude towards a particular project or security is positive, negative, or neutral.

Shapeshift - An instant digital asset exchange, supporting dozens of blockchain tokens including Bitcoin, Ethereum, Monero, Zcash, Dash, and dozens of other cryptoassets. It performs the same function as traditional exchanges (Bithumb, Bitfinex, Binance, etc.) but you don't need to sign up for accounts, or deal with placing orders on both the buy and sell sides. It's a very convenient and simple way to convert one type of cryptoasset into another, with a very simple interface.

Sharding - Designed as one possible long-term solution for scalability in Ethereum. Sharding is a type of database partitioning that separates very large databases into smaller, faster, more easily managed parts called data shards. The governing concept behind sharding is based on the idea that as the size of a database and the number of transactions made on the database per unit of time increase linearly, the response time for querying the database increases exponentially. Vitalek Buterin hopes to potentially apply sharding to the Ethereum blockchain as a means of increasing speed, scalability, and storage.

Shill - A person engaged in covert advertising. The shill attempts to spread buzz by personally endorsing the product or cryptoasset in public forums with the pretense of sincerity, when in fact he/she is being paid directly for their services (a paid shill), or has a vested financial interest in promoting the product or cryptoasset (ie. holding a significant amount of that specific asset in their portfolio). Some aggressive shills cross the line from covert to overt, open promotion. Some people who are well-intentioned but overly-enthusiastic can end up acting like shills, even if they didn't originally intend to. In Scotland, they're usually called schills.

Shitcoin - A project which is underperforming the general crypto market, either due to lack of market interest, or due to lack of fundamentals relating to valuation.

Short Selling (Shorting) - A type of trade whereby a purchaser bets that a financial instrument (stock, crypto, bond, forex) will go down in price. The "shorter" (short seller) borrows a security from someone and then sells it at the current market price, while entering into a promissary contract to buy that security in the future to return it from the entity that you borrowed it from. The hope of the shorter is that the security will eventually go down in price, so it will cost less money to buy and return to the lender than received from selling when the short trade was set up. For example, if you could short Bitconnect at $300, you would be selling shares of Bitconnect that you don't own (but have just borrowed from someone willing to lend them). If the price of Bitconnect then went down to $10 at some point a few months later, you could buy shares on the open market for $10 each to return to the entity you borrowed them from. In the process, you would have made $290 per share. It's a "buy low then sell high" profit that works in reverse chronological order because someone is willing to loan you the security temporarily (you often have to pledge collateral). Some exchanges will allow you to short certain stocks or cryptos as long as you hold a certain amount of funds or crypto on the exchange to act as collateral. The risk to shorting is that if the securities go up in price instead of down, and you have to buy them back at a higher price, then you've lost money on the trade. Shorting is not a good trading strategy for inexperienced traders/investors, or for those without deep pockets.

Should Have Used Monero (SHUM) - This slogan is commonly used when referring to articles that talk about people getting into trouble for doing immoral or criminal acts, and then getting caught because their activities were caught on public blockchain ledgers. At the moment, it appears that Monero may be the only truly private and untraceable cryptocurrency in usage today (although Z-Cash may be another). Many people assume that Bitcoin and other cryptocurrencies are anonymous, but that is not correct. Remember the phrase, "Public Ledger." In some cases, privacy may be desirable.

Sidechain - A separate, subordinate blockchain on a network, which is attached to the parent chain through the use of a two-way peg which allows for assets to be interchangeable and moved across the chain at a fixed deterministic exchange rate. Sidechains are complex and require a lot of coding to integrate properly with their parent chains, but they have a lot of potential as second-layer solutions that may be able to significantly increase the transaction capability of popular parent blockchains (such as Bitcoin).

Silk Road - A "dark net market" website, administered by Ross Ulbricht, which allowed users to transact discretely in various types of contraband and illegal services. The Silk Road was one of the first and most notorious of online black markets, until the FBI shut it down in 2013. Many buyers and sellers used Bitcoin as a way of facilitating transactions, in an attempt to avoid having their transactions tracked through traditional financial systems.

Sleeping Giant - A project that an investor feels is going to become very popular and valuable in the future, but which is currently flying under the radar of the investment community.

Smart Contract - A self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code on a blockchain. Smart contracts permit trusted transactions and agreements to be carried out among disparate, anonymous parties without the need for a central authority, legal system, or external enforcement mechanism. They render transactions traceable, transparent, and irreversible. The aim of smart contracts is to provide security that is superior to traditional contract law and to reduce other transaction costs associated with contracting. Smart contracts are especially well-suited for use in certain blockchain networks such as Ethereum or Neo, but it should be noted that not every cryptoasset has smart contract capabilities.

SmartBridge - SmartBridge is a functionality built upon the Ark platform, providing the ability to connect and communicate between blockchains. If you want to trigger an event on a blockchain via a different blockchain, and that chain is SmartBridge compatible, then you can issue a SmartBridge transaction to any compatible blockchain via the Ark wallet. For example, you could write a smart contract on Neo, or enter data into a record on Factom, without actually holding any NEO or FCT crypto.

Sock Puppet - An online identity used for purposes of deception.

Soft Fork - A soft fork is a change to a blockchain protocol wherein only previously valid blocks/transactions are made invalid. Since old nodes will recognise the new blocks as valid, a soft fork is backward-compatible. This kind of fork requires only a majority of the miners to upgrade to enforce the new rules. Let's try to make this easier to understand. A soft fork is any change that's backward compatible. As an example, instead of blocks with a maximum size of 2MB being valid, a new rule might only allow 1MB blocks. Nodes that have not been upgraded to the new protocol will still see the new transactions as valid (because 1MB is less than 2MB, so the new blocks will still pass the “old” test). However, if non-upgraded nodes continue to mine blocks, the blocks they mine will be rejected by the upgraded nodes. This is why soft forks need a majority of hash power in the network. Soft forks have been the most commonly used option to upgrade the Bitcoin blockchain so far, because it is argued that they present a lower risk of splitting the network.

Staking - Staking is what occurs in a Proof of Stake system to earn additional coins. If you already hold some coins in that system, staking is equivalent to earning interest on your holdings. In a staking system, you may receive new coins that are being created slowly, and/or you may receive transaction fees from growth of the blockchain. The growth of new coins is a form of inflation, and if the staking payouts (interest) are not equivalent to the inflation of the supply of coins, you may actually slowly fall behind in net value of your assets. This is similar to a traditional monetary system, because if the interest you earn in a bank account is not equal to the devaluation of the currency due to inflation, then your net worth is slowly eroded. To stake a cryptoasset in a POS system, you may be required to hold your coins or tokens in a certain specific wallet. Critics of PoW (mining) systems point out that staking a coin (merely holding onto the coin) is much more environmentally friendly than mining (which consumes a lot of electricity).

Stealth Addresses - Allows you to generate a public key that you can provide to multiple parties, and the parties can pay you but cannot see funds you receive from the other parties. Essentially, although the public key is visible, each individual transaction made to that key ends up getting its own specific public and private key, which provides a greater (but not absolute) amount of privacy for parties to the transaction. For example, if a company is soliciting payments on a website, they might not want every client's payment to go to the same address, because then clients can be tied to the same supplier/company. By using a stealth address system, each payment actually goes to a different wallet with its own public and private keys, and the receiver accesses that wallet individually, rather than owning a single wallet with all transactions combined.

Stop Loss - A type of order that is set and left as a long-term precautionary measure to conserve capital in the market in the event of a downturn in a specific security. The stop-loss sets a specific low price at which an order is triggered. If the trading price of a stock goes low enough to hit that price or drop below that price, the order is then executed at the best possible price. Note that the executed price is not necessarily going to be the same as the stop-loss price, especially in a market with low liquidity or in a situation where the market price drops precipitously. For example, let's assume that ExampleCoin is trading for several days in a range around $8 to $9, and you hold 1000 coins of ExampleCoin, and you're worried that the bottom is going to drop out of the market if a certain hypothetical upcoming news announcement doesn't materialize. You don't want to get caught blind-sided when you're asleep at night, or away from your trading desk, so you set a stop-loss order for $7.50. If at any point ExampleCoin's trading price hits or drops below $7.50, your exchange will automatically do a market sell of your holdings at the best possible price for you. If there were a lot of buyers sitting at $7.50, you might get lucky and your 1000 coins might get sold at that price. If there weren't a lot of buy orders sitting on the exchange, maybe some of your coins were sold for $7.50 and some for $7.40 and some for $7.27, or whatever price points existed for the available buy orders on the exchange at the time that your stop-loss was triggered.

StringCT - An upgrade to the original RingCT (Ring Confidential Transactions) used in Monero to help ensure that transactions are untraceable. Ring signatures that allow for higher ring sizes provide greater untraceability, privacy and fungibility. Ring signatures that are more compact provide greater scalability. StringCT delivers these improvements. StringCT ring signature sizes are independent of the number of real inputs, which leads to dramatic storage savings (but not computational savings). StringCT allows for a much smaller blockchain than RingCT.

Sub - Slang used commonly on Reddit, but which can mean two different things. The first is short for "SubReddit," which is any online community within Reddit that is dedicated to a specific topic or group. Reddit subs are usually listed in the format **/r/SubredditName**. The second slang usage is a shortened form of "subscriber." This can lead to confusion, although the context may indicate the meaning. For example, a comment such as "this sub has 10k subs" would mean that the particular SubReddit in question has over ten thousand subscribers.

Sybil Attack - A computer security term referring to an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks.

Tainted Coins - Taint is the probability of tracing coins back to any given address after mixing and tumbling, or the level of connectivity between two wallet addresses which have both held certain coins. This sounds confusing. It is, because in the popular lexicon, most people say that tainted coins are coins which have at some point been used for some sort of transaction which does not meet certain standards for ethical transactions. For example, if someone uses some Bitcoin to buy drugs on a darknet market, then it is said that those particular coins have become tainted, as if it was some form of dirty money. Because the public blockchains of all cryptocurrencies can be examined by anyone, it is easy to trace the path of any particular Bitcoin through all the wallets that they have been stored in since they were mined. The same applies to all other cryptocurrencies, not just Bitcoin (actually, Monero is an exception since its ledger cannot be examined). Interestingly, probably the vast majority of all Bitcoins were used in some sort of shady transaction at some point in their history, so according to this definition, almost all Bitcoins are tainted in some manner. Ironically, most fiat paper money is probably similarly tainted, although of course it is very difficult to trace a single paper bill of any currency back through all the different entities that have held it since it was issued by a mint. That's because even though each bill has a unique identifier (the serial number on the bill), there is no public ledger to trace the transactions of a bill. Some people worry that some governments may be able to trace certain coins of various cryptocurrencies back to specific criminal transactions, and to say that since they were part of a crime, those coins should be seized by the government. This may be a valid concern, even if a remote one. After all, the US government enacted an Executive Order in 1933 to confiscate most gold from US citizens, except for allowing some minor exceptions for jewelry and collector coins. Stranger things have happened.

Take A Position - To either buy securities outright, or to set up a short sale.

Tangle - A third-generation distributed Ledger used by the Iota project, based on a directed acyclic graph (DAG). Rather than a structured orderly chain of blocks, the Tangle is a network that grows in a method that mimics nature in some ways. The Tangle is scalable, lightweight, and makes it possible to transfer value without any fees. It has no blocks and therefore no miners. Each transaction on the Tangle is required to "verify" two previous transactions, therefore the proof-of-work being done by the network is spread out among all participants of the network, rather than concentrated into the hands of miners. If you were to try to envision the Tangle (there are 3D graphic live representations online) you might be able to say that it is slightly analogous to a swarm of ants moving through the jungle. However, with the ants, there is a fixed number of ants and they are moving, whereas on the Tangle, each transaction stays put and new transactions are attached to historical transactions, so the size of the Tangle is constantly growing. Another analogy, again not a perfect one, is to envision a giant three-dimensional petri dish where the bacteria grows outward from existing growth, akin to new transactions being attached to and expanding the Tangle.

Technical Analysis (TA) – Evaluating the trading patterns of securities, in an attempt to forecast their future movement. Technical analysis is based upon statistics gathered from trading activity, such as price movement and volume. Technical analysis has a heavy reliance upon trading charts, candlesticks, trends, and moving averages.

Testnet - The pre-public-release test platform or blockchain for a project. After a project has been vetted using a testnet, and the developers feel that it is ready for public launch, they release the mainnet.

Ternary Computer - A computing device that uses three separate states of logic in its calculations, instead of the much more common binary that permeates the landscape today.

Three Letter Agency – Government agencies with three-letter acronyms, which are also associated with oversight or law enforcement. Examples include the NSA, FBI, CIA, ATF, ICE, SEC, and so on.

Ticker - The ticker is the symbol for a stock or for a cryptoasset. It can also refer to a data stream showing prices for a number of assets. Examples include stock tickers (AAPL for Apple or MSFT for Microsoft on the NYSE), crypto tickers (ETH for Ethereum or LTC for Litecoin), and foreign exchange tickers (CAD for Canadian dollars or GBP for Britain's pound sterling). In the case of a data stream, if you're watching a show on a financial television network, you may see a stream of stock symbols running dynamically along the bottom of the screen, with current prices for various stocks. This is also referred to as a ticker, shortened from the original Ticker Tape.

Token - A token is a symbolic representation of a portion of the value of a project. Tokens represent assets that can range from accounting info to commodities to intellectual property to loyalty points to computing resource rights. Tokens are usually built on top of another blockchain platform (such as Ethereum or Neo) so they don't really need all of the technology created from scratch. Examples of projects that currently use Ethereum-based tokens include Golem, OmiseGo, District0x, and Civic. We often categorize tokens based upon their purpose, ie. a platform token is used with a platform such as Ethereum or Neo, and a Utility Token is used within a specific project that has been built upon one of the platforms. Utility tokens can be further broken down into Usage Tokens and Work Tokens (see those definitions).

Token Burn - See "Burn."

Token Sale - See "Initial Coin Offering."

Trex - Slang for the Bittrex Exchange.

Trusted Platform Module (TPM) - An international standard (written by a computer industry consortium called Trusted Computing Group) for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware by integrating cryptographic keys into devices. TPM offers facilities for the secure generation of cryptographic keys and limitation of their use, as well as other capabilities such as remote attestation, sealing, and binding.

Trustless - In traditional finance, parties to a contract need a trusted third party to ensure that a transaction can be processed, such as a bank or credit union or credit card issuer. When a transaction occurs, that third party acts as the middleman to facilitate the transfer of value (when you buy a computer from NewEgg using a Visa, Visa pays NewEgg and then you subsequently pay Visa). The trusted party acting as an intermediary takes on the risk of the transaction, hence the reason why there are banking and credit fees to compensate the trusted third party for their efforts and assumption of risk. With a trustless transaction, no third party is necessary. You interact directly with another party during your trade. Of course, when the two parties are in different parts of the world, how does that happen? If you're sending them 1 Bitcoin and you expect 20 Ethereum in return, how do you know that you'll get your 20 Ethereum after you've sent your Bitcoin? Well, certain transactions can be set up through mechanisms such as atomic swaps, such that both parties have to "irrevocably" commit their sides of the transaction before either side can move ahead to complete their own side of the transaction. Once both sides have committed, one party can then opt to "instantiate" the transaction by telling the blockchain code to move forward. From that point forward, the transaction cannot be stopped, although failure to instantiate by a certain time will cancel the transaction for both sides. Because neither of the parties to the transaction had to trust the other in order for the transaction to occur, it's called a trustless transaction. Of course, this is really just a transfer of trust. You're trusting technology and the cyptoasset mechanisms rather than trusting another human.

Tumbling - A service offered to mix potentially identifiable or colored cryptocurrency funds with other coins, with the intention of confusing the trail that leads back to the fund's original source.

Turing Machine - A computer science term which refers to a system of rules, states and transitions, rather than to a real physical machine.

Two Factor Authentication (2FA) - A security protocol whereby in order to access a system, a user must have more than just a username and password; they must also possess a second form of identification or verification to make it more difficult for anyone else to bypass the password security for the account. 2FA is usually tied to actions relating to physical devices that a person carries with them, such as inserting a special type of USB key, receiving a SMS text message on a specific cell phone, or getting an authorization code from an authenticator app on a mobile device.

Unbanked – People who aren't able to open traditional bank accounts, either due to financial constraints or due to rules and regulations such as identification criteria.

Unload a Position - To sell your securities.

Usage Token - These are tokens that act like native currency in their respective DAPPS. Golem is a good example of this. If you want to use the services in Golem then you will need to pay with Golem Network Token (GNT). While these tokens have monetary value they won't give you any particular rights or privilege within the network itself.

Utility Token - A token used in a specific project. Some utility tokens are integral to coding used in a project, and derive their value from utility in the operations of the project. For other projects, the project's token may not be used directly in coding or transactions, and instead acts only as a representation of the value of a project. Tokens are usually treated similar to a security, namely functioning like a share in a company's stock.

Wash Trading – Using a group of accounts to trade a security back and forth solely for the purpose of trying to inflate the trading volume and make the security look more popular than it really is.

Watering Hole - A watering hole is a computer attack strategy, in which the victim is targeted as any individual within a particular group of members who share a common characteristic(s), such as an organization, an industry, or a geographic region. In this attack, the attacker guesses or observes which website(s) the group often uses, and infects one or more of those sites with malware. Eventually, some member(s) of the targeted group become infected. The malware used in these attacks typically collects information about the user, and with respect to cryptocurrencies, may seek seeds or private keys as the primary target.

Weak Hands - Someone who is very nervous and considers selling a coin during a bearish period, because they think it's going to go down a lot more. Someone with weak hands can't hold their coins when there is downward pressure.

Whale - A market participant with a large amount of power (money) in the market. Because they have so much money invested, they can make trades that affect pricing and sentiment in the markets, or they act as a market maker by putting up very large buy and sell walls that keep a coin trading in a certain price range (a collar). A whale may have hundreds of thousands or even millions of dollars to play with in the markets.

White Paper - A report about a subject that may contain overview, technical, marketing, and other information about a potential project. This written document is intended to inform readers in detail about the characteristics, attributes, and features of a project or proposed project. It can include information about everything from the creation of the project to ongoing technical features and considerations, to proposals for future governance. The white paper can be treated as something that acts partly as a vision and mission statement, and partly as a master plan for a project.

Winternitz Hash - Formerly known as the Winternitz One-Time Signature Scheme, this is a hash (encryption algorithm) which is known as a post-quantum signature because quantum attacks don't significantly lower the security given by this hash. While this is rather irrelevant at the present time, since we don't have practical working quantum computers, it may become important in the foreseeable future.

Work Token - These are tokens that identify you as being effectively similar to being a shareholder in a DAPP. Because of that, you have a say in the direction that the DAPP takes. A perfect example of this is the DAO tokens. If you were a DAO token holder then you had the right to vote on whether a particular DAPP could get funding from the DAO or not. This type of token is very much akin to a share of stock in a traditional corporation.

Wraith Protocol - A privacy protocol that was intended for use by the Verge project. Basically, Verge uses a dual private/public blockchain approach, so theoretically, when Wraith is turned on, the blockchain info is hidden from the public. When wraith is off, the blockchain info is visible to the public. The last time we looked, this protocol was not yet perfected/implemented properly, although it had been promised many times.

Fomo, Moon, Lambo: The Complete Beginner's Guide to Cryptocurrencies

www.beginnersguidetocryptocurrencies.com

Fomo, Moon, Lambo: The Complete Beginner's Guide to Cryptocurrencies

www.beginnersguidetocryptocurrencies.com