The Mad Hedge Guide to Trading Bitcoin

A Guide to All Aspects of the Cryptocurrency Markets

By John Thomas

CEO & Publisher

The Diary of a Mad Hedge Fund Trader

A 50 year trading veteran and active Bitcoin miner

Biography of John Thomas - The Mad Hedge Fund Trader

www.madhedgefundtrader.com

John Thomas graduated from the University of California at Los Angeles (UCLA) with a degree in Biochemistry and a minor in Mathematics in 1974.

Upon graduation, he used his math skills to get a job with the Atomic Energy Commission at the Nuclear Test Site in Nevada to do research on the long term effects of low level radiation.

As part of this research John interviewed many survivors of the atomic bomb at the Atomic Bomb Victims Hospital in Hiroshima.

Liking Japan, he decided to stay, moving to Tokyo, Japan to join a Japanese securities house as a research analyst, becoming fluent in Japanese in the process.

In 1976 he was appointed the Tokyo correspondent for ***The Economist*** magazine and the ***Financial Times***.

For the next seven years he published thousands of articles about the economies, companies, and leaders of every country in Asia. He was one of the first American correspondents to cover China during the Cultural Revolution.

He reported on the American climb of Mount Everest and guerilla wars throughout Southeast Asia, including in Cambodia, Laos, Burma, and Thailand.

The major figures he interviewed included China's Premier Deng Xiaoping, Ferdinand Marcos of the Philippines, the UK's Margaret Thatcher, the PLO's Yassir Arafat, CIA head William Colby, and of course, President Ronald Reagan.

In 1982 John Thomas moved to New York as the US editor of ***The Economis***t. As a member of the White House Press Corps he covered the early years of the Reagan administration.

In 1983 he was hired by Morgan Stanley to build a new division in international equities. Later, he was promoted and transferred to London to head up the sales and trading of Japanese equity derivatives in Europe and the Middle East.

In 1989 John Thomas was appointed a director of the Swiss Bank Corp responsible for its then vast portfolio of Japanese equity derivatives.

That effort was cut short when John was drafted by the US Marine Corp to fly the C-130 Hercules as part of Operation Desert Shield/Desert Storm. John was wounded in action and received a purple heart.

Leaving the military after the war, he set up the first ever dedicated international hedge fund. It became a top performer in the industry, eventually bringing in a tenfold return in a decade.

In 2000, John Thomas sold his hedge fund to concentrate on managing his personal investments. He focused on natural gas exploration and development in Texas and Colorado, as well as other commodities.

This made him one of the early pioneers in the “fracking” technology which is now dramatically reshaping America’s energy landscape. After catching a double in the price of natural gas, John sold this business in 2005.

Seeing the incredible inefficiencies and severe mispricing offered by the popping of multiple bubbles during the Great Crash of 2008, and missing the adrenaline of the marketplace, he returned to active hedge fund management.

With ***the Diary of a Mad Hedge Fund Trader***, his goal is to broaden public understanding of the techniques and strategies employed by the most successful hedge funds so that they may more profitably manage their own money.

In 2020, John launched a major research effort into Bitcoin and the crypto currencies and began active trading.

Today, John works out of his three homes in Silicon Valley, Incline Village, Nevada, and Zermatt, Switzerland.

In his free time, John Thomas climbs mountains, does long distance backpacks, practices karate, performs aerobatics in antique aircraft, collects vintage wines, reads the Japanese classics, and engages in a wide variety of public service and philanthropic activities.

His career has taken him up to 20,000 feet on Mount Everest, to the edge of space at 90,000 feet in the Cockpit of a MIG-25, and to the depths of a sunken Japanese fleet in the Truk Lagoon.

Why they call him ***"Mad"*** he will never understand.

Chapter 1: Introduction

I first got involved with bitcoin in 2011, when a subscriber wanting to thank me for a spectacular investment performance ***GAVE*** me ten Bitcoin. They were then worth $1 each.

Then, I forgot about them. When they appreciated to $100 in 2013, I decided to sell them and take the family out to dinner at **The French Laundry**, the best restaurant in California's Napa Valley. I thought I was a genius.

Back then, early in the life of Bitcoin, theft was rampant, and exchange regularly went bankrupt. So cashing in on my windfall wasn't such an unreasonable thing to do.

That turned out to be the most expensive dinner of my life. If I had kept the ten Bitcoins, they would be worth over $600,000 today. Maybe I'm not such a genius after all.

Unless you have been living in a cave for the past five years, you have probably heard of Bitcoin.

By now, you have decided that it is the greatest money-making opportunity of all time, or the greatest scam since Carlo Ponzi amassed a fortune selling international postal coupons in 1922.

Some things are certain. Bitcoin will change the financial system beyond all recognition. It will revolutionize banking and investment. And it will vastly accelerate the digitization of the global economy, to everyone's benefit.

After reading this book, you may or may not want to invest in Bitcoin. However, a working knowledge of what it is and how it works will become essential for everyone as the 21st century unfolds.

For a start, Bitcoin, other cryptos, and future cryptos, yet to be invented, will save $1 trillion a year in transaction costs in the global economy. Who will be the beneficiary of this bounty? You, me, and all the companies we invest in.

It is certain that some form of current or future crypto will be a stepping stone to a global digital currency, not just for emerging nations like El Salvador, but all nations.

And here is the most interesting thing. The eventual impact of crypto on our lives hasn't even been imagined yet.

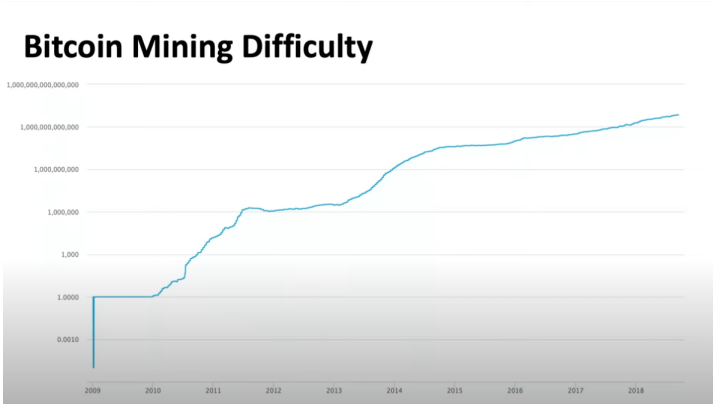
Going back to my Defense Department days, I was one of a handful who was present at the birth of the Internet and the similarities are legion. A few clever people were aware of bits and corners of the Internet back in 1989, but nobody had a big picture.

Long term predictions might as well have been science fiction. Insiders were buying up domain names for a dollar each, such as for mcdonalds.com, whitehouse.com, and sex.com. The MacDonald's site was later sold to the fast-food company for $10 million.

When the Internet began mass adoption in 1995, no one imagined that every taxi company in the world would be out of business in 15 years. New York City taxi medallions once worth $1 million became worthless, prompting many suicides.

Nor did prime downtown apartment owners all over the world expect they could rent their homes for astronomical daily rates through Airbnb (ABNB). They didn't even expect that a small startup named Netflix (NFLX) would stream videos online, wiping out Blockbuster Video.

Bitcoin was created by **Satoshi Nakamoto**, a pseudonymous person or team who outlined the technology in a **2008 white paper**. Nobody knows for sure. It might even be a US government agency that invented Bitcoin. It's an appealingly simple concept: bitcoin is digital money that allows for secure, trustless, peer-to-peer transactions on the internet.



Unlike other payment services, like PayPal's Venmo (PYPL), which rely on the traditional financial system for permission to transfer money and on existing debit/credit accounts, bitcoin is decentralized: any two people, anywhere in the world, can send bitcoin to each other without the involvement of a bank, government, or other institution.

Every transaction involving Bitcoin is tracked on the blockchain, which is like a bank's ledger, or log of customers' funds going in and out of the bank. In simple terms, it's a record of every transaction ever made using bitcoin. Think of blockchain as a chain of blocks of code, each one of which contains millions of lines of code.

Genesis Block (1/3/09) – 10 leading zeros, though only required 8
000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Block 541974 (9/18/18)- 18 leading zeros
0000000000000000001104a863046dfbad1a2941128815669623ff93c2a3945f

Unlike a bank's ledger, the Bitcoin blockchain is distributed across the entire network. No company, country, or third party is in control of it; and anyone can become part of that network. The Mad Hedge Fund Trader is part of that network, otherwise known as a "node."

There will only ever be 21 million Bitcoin. This is digital money that cannot be inflated or manipulated in any way.

It isn't necessary to buy an entire bitcoin: you can buy just a fraction of one if that's all you want or need. To open my own crypto wallet, I started with an initial buy of one ten thousand of a Bitcoin, or $10. Now, I'm trading in the millions.

Whatever the outcome of Bitcoin is, one thing is certain. None of our lives will be the same.

Bitcoin Mining Evolution

Application Specific Integrated Circuit
(ASICs) 2013 – 2018
4 – 16 TH/S

Graphics Processing Units
(GPUs) 2010 – 2013
20 - 300 MH/S

Central Processing Units
(CPUs) 2009 – 2010
2 - 20 MH/S

Bitcoin vs Ethereum Design

• Founder: Satoshi Nakamoto	⟷	Vatalik Buterin
• Genesis: January 2009	⟷	July 2015
• Code: Non Turing (Script)	⟷	Turing Complete (Solidity, Serpent, LLL or Mutan)
• Ledger: UTXO – Transaction	⟷	State - Account Based
• Merkle Trees: Transactions	⟷	Transactions, State, Storage, Receipts (w/nonces)
• Block Time: 10 minutes	⟷	14 seconds
• Consensus: Proof of Work	⟷	Proof of Work
• Hash Function: SHA 25[illegible]	⟷	Ethash

Vatalik decided to use a different hash function.

Smart Contract Potential Use Cases

Digital Chamber of Commerce (12/16)

• Digital Identity	Records
• Securities	Trade Finance
• Derivatives	Financial Data
• Mortgages	Land Title
• Supply Chain	Auto Insurance
• Clinical Trials	Cancer Research

And we're going to study most of these, not all

Chapter 2: What is Blockchain

Cryptocurrencies, like Bitcoin and Ethereum, are powered by a technology called blockchain.

At its most basic, a blockchain is a list of transactions that anyone can view and verify. The Bitcoin blockchain, for example, contains a record of every time someone sent or received Bitcoin.

Cryptocurrencies and the blockchain technology that powers them make it possible to transfer value online without the need for a middleman like a bank or credit card company.

Imagine a global, open alternative to every financial service you use today, accessible with little more than a smartphone and internet connection.

Almost all cryptocurrencies, including Bitcoin, Ethereum, Cardano, and Litecoin, are secured via blockchain networks. That means their accuracy is constantly being verified by a huge amount of computing power.

The list of transactions contained in the blockchain is fundamental for most cryptocurrencies because it enables secure payments to be made between people who don't know each other without having to go through a third-party verifier like a bank.

Due to the cryptographic nature of these networks, payments via blockchain can be more secure than standard debit/credit card transactions. When making a Bitcoin payment, for instance, you don't need to provide any sensitive personal information, like your name and address.

That means there is almost zero risk of your financial information being compromised, or your identity being stolen.

Blockchain technology is also exciting because it has many uses beyond cryptocurrency. Blockchains are being used to explore medical research, improve the accuracy of healthcare records, streamline supply chains, settle stock transactions and so much more.

Due to the cryptographic nature of these networks, payments via blockchain can be more secure than standard debit/credit card transactions.

What are some advantages of blockchains?

They're global, which means that cryptocurrencies can be sent across the planet quickly and cheaply.

They increase privacy. Cryptocurrency payments don't require you to include your personal information, which protects you from being hacked or having your identity stolen.

They're open. Because every single transaction on cryptocurrency networks is published publicly in the form of the blockchain, anyone can scrutinize them. That leaves no room for manipulation of transactions, changing the money supply, or adjusting the rules mid-game. The software that constitutes the core of these currencies is free and open source so anyone can review the code.
There are a few key questions.

What's the main advantage blockchains have over the old financial system?

Think about how much of your financial life takes place online, from shopping to investing – and how every single one of those transactions requires a bank or a credit card company or payment processor like PayPal in the middle of it. Blockchains allow for those transactions to happen without a middleman, and without the added costs and complexity that come with them.

That function alone would remove $1 trillion in costs from the global economy, or about 1% of global GDP.

Is Bitcoin a blockchain? Bitcoin is a form of digital money. And the underlying technology that makes it possible is a blockchain.

How many kinds of blockchains are there? Thousands, from the ones that power Bitcoin, Litecoin, Tezos, and countless other digital currencies to an increasing number that have nothing to do with digital money.

How does a blockchain work? Picture a chain you might use for a ship's anchor. But in this case, every link on the chain is a chunk of information that contains transaction data. At the top of the chain, you see what happened today, and as you move down the chain you see older and older transactions. And if you follow it all the way down to the anchor sitting at the bottom of the harbor, you'll have seen every single transaction in the history of that cryptocurrency.

Imagine a dollar bill that has on it a record of the name and address of everyone who has ever held it. The number would be in the thousands for each bill. That is what we are talking about here. The data demands are exponential.

This gives the blockchain powerful security advantages: it's an open, transparent record of a cryptocurrency's entire history. If anyone tries to manipulate a transaction it will cause the link to break, and the entire network will see what happened. That, in a nutshell, is blockchain explained.

Another way people often describe the blockchain is that it's a ledger (sometimes you'll hear the terms 'distributed ledger' or 'immutable ledger'), that is comparable to the balance sheet of a bank. Like a bank's ledger, the blockchain tracks all the money flowing into, out of, and through the network.

But, unlike a bank's books, a crypto blockchain isn't maintained by any individual or organization, including banks and governments. In fact, it isn't centralized at all. Instead, it is secured by a large peer-to-peer network of computers running open-source software. The network is constantly checking and securing the accuracy of the blockchain.

Where does new cryptocurrency come from? Every so often – around every ten minutes in the case of Bitcoin – a new chunk of transaction information (or a new block) is added to the chain of existing information. In exchange for contributing their computing power to maintaining the blockchain, the network rewards participants with a small amount of digital currency.

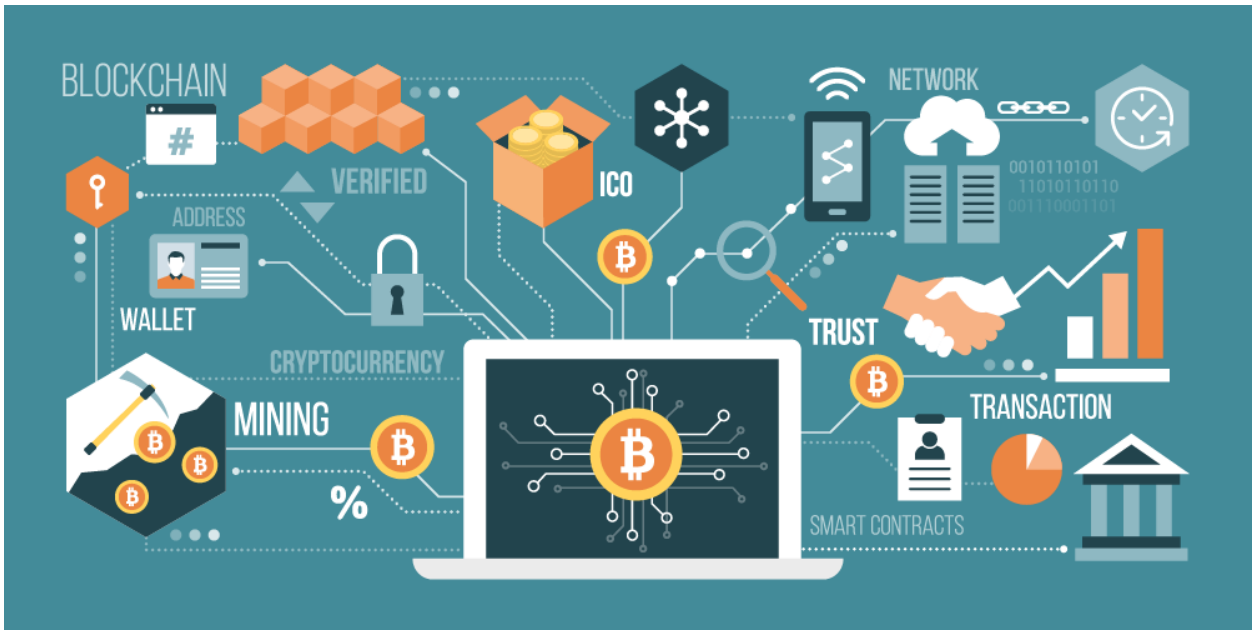
A crypto blockchain is distributed across the digital currency's entire network. No company, country, or third party is in control of it; and anyone can participate.

The network is constantly checking and securing the accuracy of the blockchain.

How do you send and receive money over a blockchain? The cryptocurrency network assigns each user a unique 'address,' which is made up of a private key and a public key. Anyone can send you money via your public key, which is akin to an email address. When you want to spend your money, you use your private key, which is basically your password, to digitally 'sign' transactions. The easiest way to manage your cryptocurrency is via software called a wallet, which you can get via an exchange like Coinbase.

Who invented the blockchain? A person or group using the name Satoshi Nakamoto published a whitepaper online explaining the principles behind a new kind of digital money called Bitcoin in late 2008. Every cryptocurrency since is an evolution of the ideas laid out in that paper.

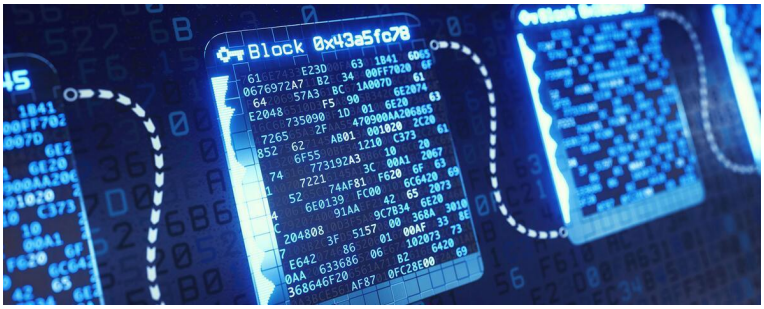
Nakamoto's goal was to create digital money that would make online transactions between two strangers anywhere in the world possible without requiring a third party like a credit card company or a payment processor like PayPal in the middle.



This required a system that would eliminate a thorny issue called the 'double spending' problem, where a person might use the same money more than once. The solution is a network that is constantly verifying the movement of Bitcoin. That network is the blockchain.

Every Bitcoin transaction is stored and verified by a global network of computers beyond the control of any person, company, or country.

The database that holds all that information is called the blockchain. Bitcoins are 'mined' via that huge, decentralized (also known as peer-to-peer) network of computers, which are also constantly verifying and securing the accuracy of the blockchain.



Every single Bitcoin transaction is reflected on the ledger, with new information periodically gathered in a "block," which is added to all the blocks that came before.

The miners' collective computing power is used to ensure the accuracy of the ever-growing ledger. Bitcoin can't exist separately from the blockchain; each new Bitcoin is recorded on it, as is each subsequent transaction with all existing coins.

In exchange for contributing their computing power to the blockchain, miners are rewarded with small amounts of cryptocurrency.

What's the future of blockchains? The blockchain idea has turned out to be a platform that can support a huge range of applications. It's still a new and rapidly developing technology, but many experts have described blockchain's potential to change the way we live and work as being akin to the potential public internet protocols like HTML had in the early days of the World Wide Web.

The Bitcoin Cash and Litecoin blockchains work in a very similar way to the original Bitcoin blockchain. The Ethereum blockchain is a further evolution of the distributed ledger idea, because unlike the Bitcoin blockchain it's not solely designed to manage digital money.

That said, Ethereum is a cryptocurrency and certainly can be used to send value to another person. Yet, the Ethereum blockchain is more like a powerful and highly flexible computing platform that allows coders to easily build all kinds of applications leveraging the blockchain.

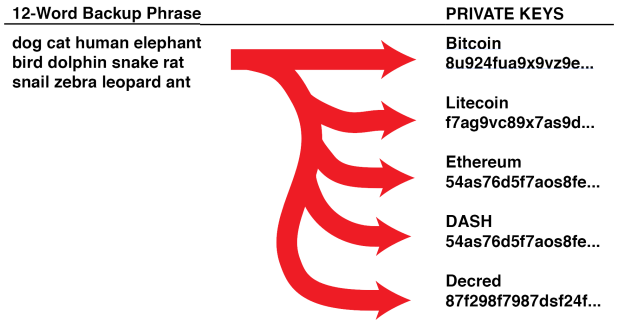
Let's consider examples here. Imagine a charity that wants to send money to a thousand people every day for a year. Using Ethereum, that would only take a few lines of code. Or maybe you're a video game developer that wants to create items like swords and armor that can be traded outside of the game itself? Ethereum is designed to do that, too. Thus, Ethereum is a more advanced technology.


EMERGENCY
PHONE
AND
CRISIS
COUNSELING
TEXT GGB TO 741741
FREE SUPPORT 24/7
53
53

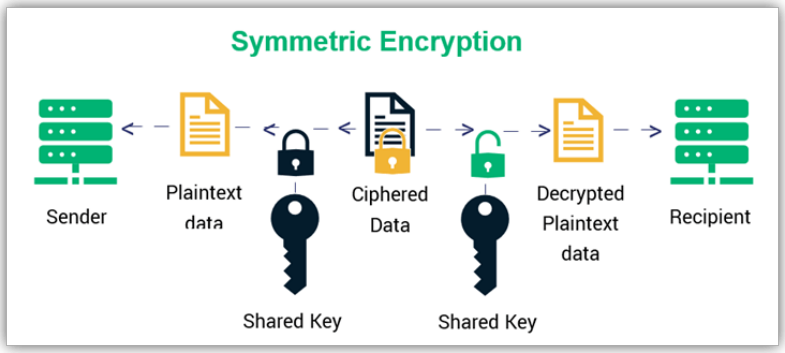
Chapter 3: Private & Public Keys

A key is like a password — a string of letters and numbers — that allows you to access and manage your crypto funds.

When you first buy cryptocurrency, you are issued two keys: a public and private key. A **public key** works like an email address, meaning you can safely share it with others, allowing you to send or receive funds. A **private key** is typically a string of letters and numbers, which is not to be shared with anyone.



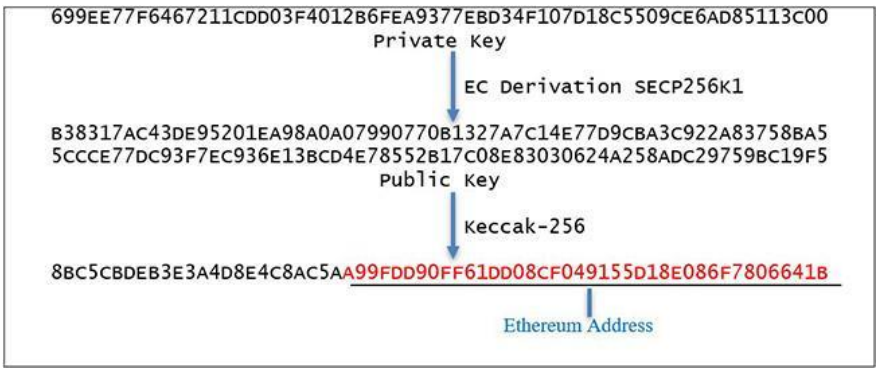
You can think of the private key as a password that unlocks the virtual vault that holds your money. If you — and only you — have access to your private key, your funds are safe and can be managed anywhere in the world with an internet connection.



Why are private keys important? The system of public and private keys is one of the cryptographic innovations that make digital money possible and secure.

This is how they work. Cryptocurrencies like Bitcoin and Ethereum are decentralized — meaning there is no bank or any other institution in the middle holding your digital money. Instead, your crypto is distributed across a network of computers via a technology called a blockchain. One feature of crypto blockchains is that they are open: all public key and transaction information is available for anyone to see.

Via some complicated math, your public key is generated by your private key, which makes them a matched pair. When you make a transaction using your public key, you verify that it's really you by using your private key.

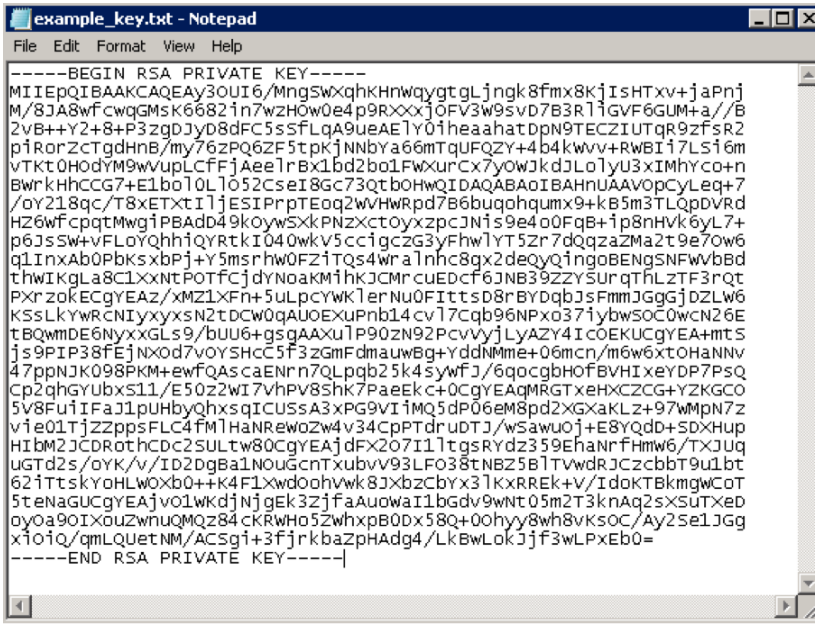


Even though everything is out in the open, it's also anonymous — you don't need to provide a name or address or any other information to use cryptocurrency.

Take Bitcoin, for example. Even though any curious observer can see when Bitcoin is bought or sold or used, only the holder of a private key can make those transactions.

Where should you store your private keys? Like any password, it's crucial to keep your private keys safe. The two major ways to keep track of them are:

Store them online in a crypto wallet: The best and simplest option for most people is to use a virtual wallet, like the one offered by Coinbase, to manage your private keys. These are known as **"hot wallets**" because your private keys are stored on the internet.



This makes buying, selling, or using your digital money as convenient and accessible as using a credit card online. Choose a wallet provided by a company with a long track record for security and features like two-factor authentication.

Alternatively, you can store them offline somewhere safe: Some investors choose to keep their private keys on a computer that isn't connected to the internet, written on pieces of paper, or even just memorized. This is referred to as **"cold storage,"** and while it does protect your private key against digital theft, it makes using your cryptocurrency much less convenient while creating other risks.

Chapter 4: How to Open a Bitcoin Wallet

A crypto wallet is a place where you can securely keep your crypto. There are many different types of crypto wallets, but the most popular ones are hosted wallets, non-custodial wallets, and hardware wallets.

Which one is right for you depends on your experience level, risk tolerance, what you want to do with your crypto, and what kind of safety net you want to have.

Hosted wallets

The most popular and easy-to-set-up crypto wallet is a hosted wallet. When you buy crypto using an app like Coinbase, your crypto is automatically held in a hosted wallet.

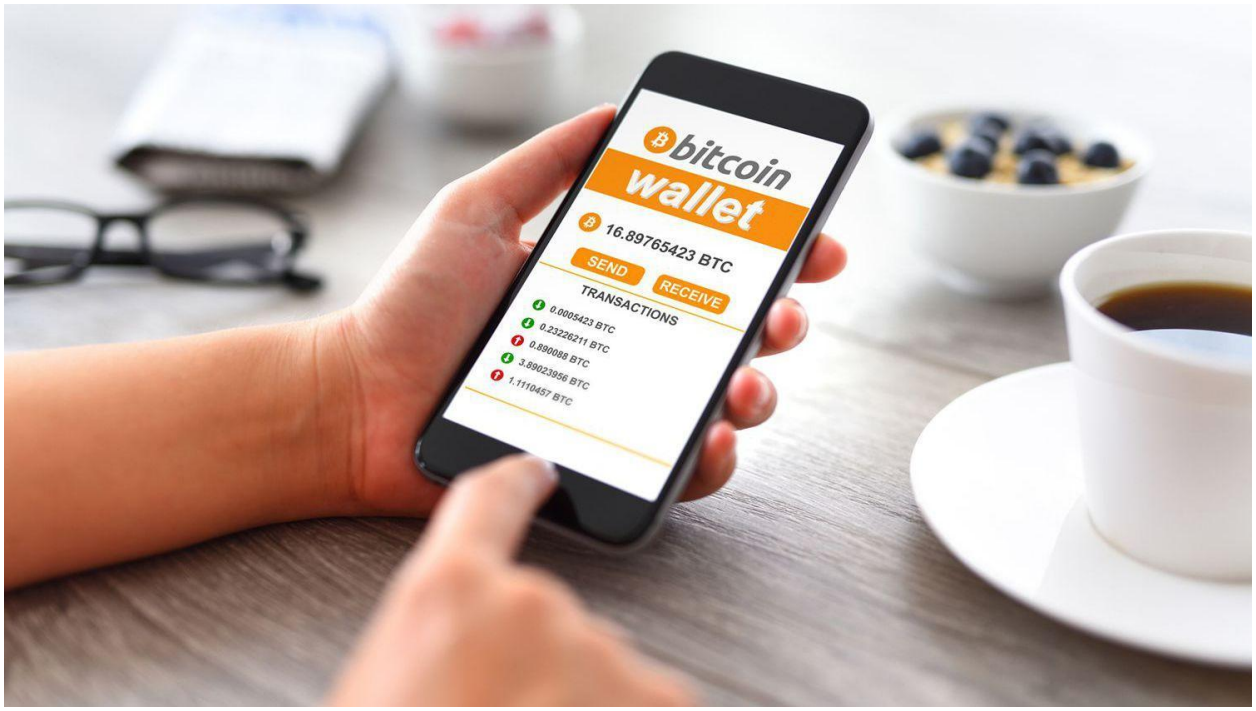
It's called hosted because a third party keeps your crypto for you, comparative to how a bank keeps your money in a checking or savings account. You may have heard of people "losing their keys" or "losing their USB wallet" but with a hosted wallet you don't have to worry about any of that.

The main benefit of keeping your crypto in a hosted wallet is if you forget your password, you won't lose your crypto. A drawback to a hosted wallet is you can't access everything crypto has to offer. However, that may change as hosted wallets start to support more features.

How to set up a hosted wallet:

Choose a platform you trust. Your main considerations should be security, ease of use, and compliance with government and financial regulations. The top crypto exchange apps are (click here for the list at https://coinmarketcap.com/rankings/exchanges/) :

Binance.US - https://www.binance.com/en
Coinbase - https://www.coinbase.com
KuCoin - https://www.kucoin.com
FTX - https://ftx.com/en
Kraken - https://www.kraken.com
Gate.io - https://www.gate.io
Crypto.com - https://crypto.com
Gemini - https://www.gemini.com



Create your account. Enter your personal info and choose a secure password. It's also recommended to use 2-step verification (also called 2FA) for an extra layer of security.

Buy or Transfer Crypto

Most crypto platforms and exchanges allow you to buy crypto using a bank account or credit card. If you already own crypto, you can also transfer it to your new hosted wallet for safe keeping.

Non-Custodial Wallets

A non-custodial wallet, like Coinbase Wallet or MetaMask, puts you in complete control of your crypto. Non-custodial wallets don't rely on a third party — or a "custodian" — to keep your crypto safe.

While they provide the software necessary to store your crypto, the responsibility of remembering and safeguarding your password falls entirely on you. If you lose or forget your password — often referred to as a **"private key"** or "seed phrase" — there's no way to access your crypto. And if someone else discovers your private key, like when you forget your cell phone in the back of an Uber cab, they'll get full access to your assets.

Why have a non-custodial wallet? In addition to being in full control of the security of your crypto, you can also access more advanced crypto activities like yield farming, staking, lending, borrowing, and more. But if all you want to do is buy, sell, send, and receive crypto, **a hosted wallet is the easiest solution**.

How to set up a non-custodial wallet:

Download a wallet app. Popular options include Coinbase Wallet and MetaMask.

Create your account. Unlike a hosted wallet, you don't need to share any personal info to create a non-custodial wallet. Not even an email address.

Be sure to write down your private key. It's presented as a random 12-word phrase. Keep it in a secure location. If you lose or forget this 12-word phrase you won't be able to access your crypto.

Transfer crypto to your wallet.

It's not always possible to buy crypto using traditional currencies (like US dollars or Euros) with a non-custodial wallet, so you'll need to transfer crypto into your non-custodial wallet from elsewhere.

Hardware wallets

A hardware wallet is a physical device, about the size of a thumb drive, that stores the private keys to your crypto offline. Most people don't use hardware wallets because of their increased complexity and cost, but they do have some benefits — for example, they can keep your crypto secure even if your computer is hacked.

However, this advanced security makes them inconvenient to use compared to a software wallet and they can cost upwards of $100 to buy.

How to set up a hardware wallet:

Buy the hardware. The two most well-known brands are **Ledger** and **Trezor**.

Install the software. Each brand has their own software that's needed to set up your wallet. Download the software from the official company website and follow the instructions to create your wallet.

Transfer crypto to your wallet. Like a non-custodial wallet, a hardware wallet typically doesn't allow you to buy crypto using traditional currencies (like US dollars or Euros), so you'll need to transfer crypto to your wallet.

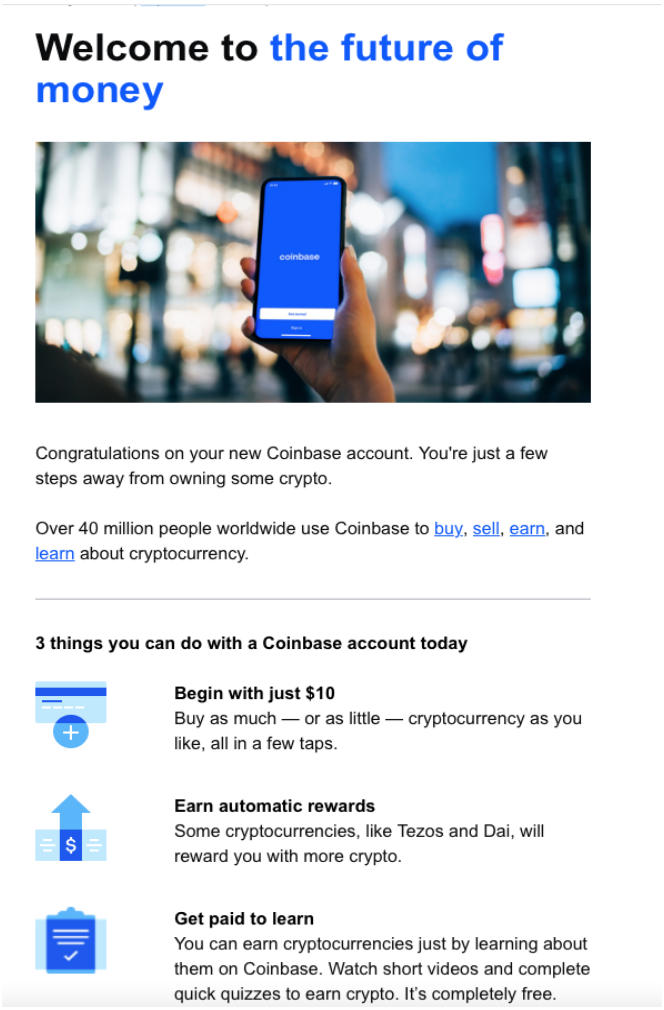
Just as there are many ways to store cash (in a bank account, in a safe, under the bed), there are many ways to store crypto. You can keep things simple with a hosted wallet, have full control of your crypto with a non-custodial wallet, take extra precautions with a hardware wallet, or even have multiple types of wallets — with crypto the choice is yours.

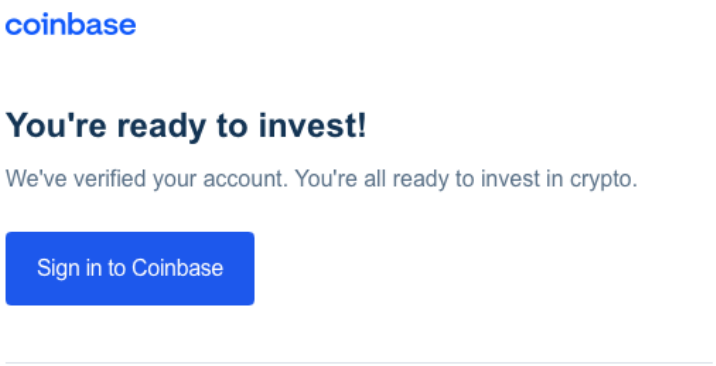
I'll go through the drill for you on setting up a wallet at the popular exchange Coinbase. Do so, and they will give you $5 worth of free Bitcoin at https://www.coinbase.com/

1) Click on the blue **"Sign up"** button on the right.
1) You instantly receive an email to verify your **email address**
2) Enter your **cell phone number**

3) They then email you a seven digit **verification code** which you enter into your account
4) It then asks for more personal information like address and the last 4 digits of your **social security number**
5) Enter your personal bank account info to fund account via the **Plaid** app with the login ID and password of your bank account
6) Do a **second text verification** to your phone
7) You are ready to buy bitcoin and have dollars directly debited from your bank account with a five cent fee. Trading is 24/7, seven days a week. The crypto market never takes a holiday.

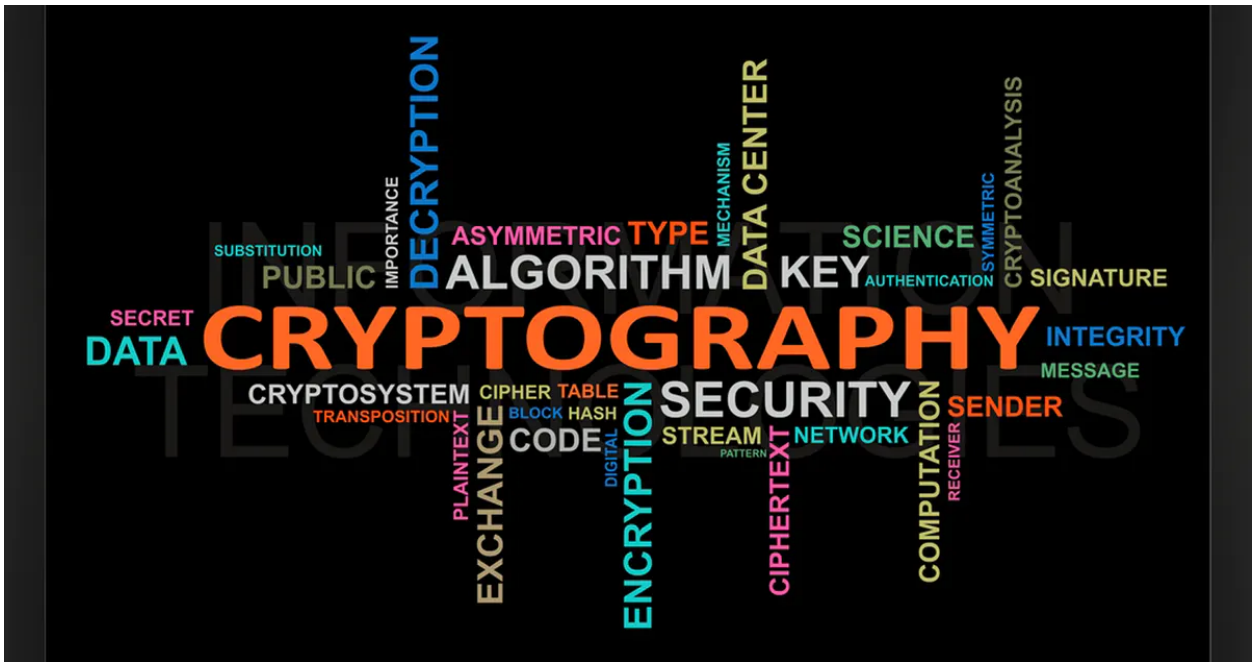
Once your account is open you get the confirmation above, followed by an invitation to do your first trade.





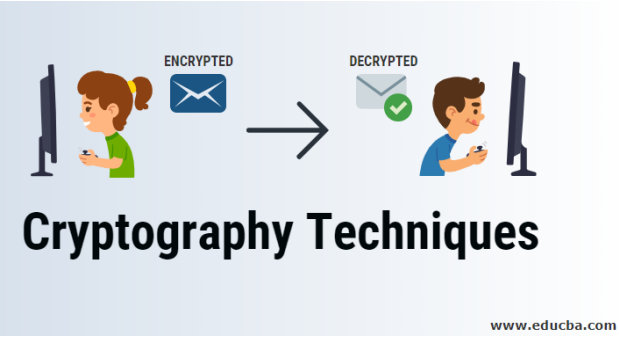

USMC

Chapter 5: Cryptography



The “crypto” in the word “cryptocurrency” means “secret” in Greek – which gives you a clue as to what the field of cryptography is all about. How appropriate.

Cryptography is the study and practice of sending secure, encrypted messages or data between two or more parties. The sender “encrypts” the message, which obscures its content to a third party, and the receiver “decrypts” the message, making it legible again.



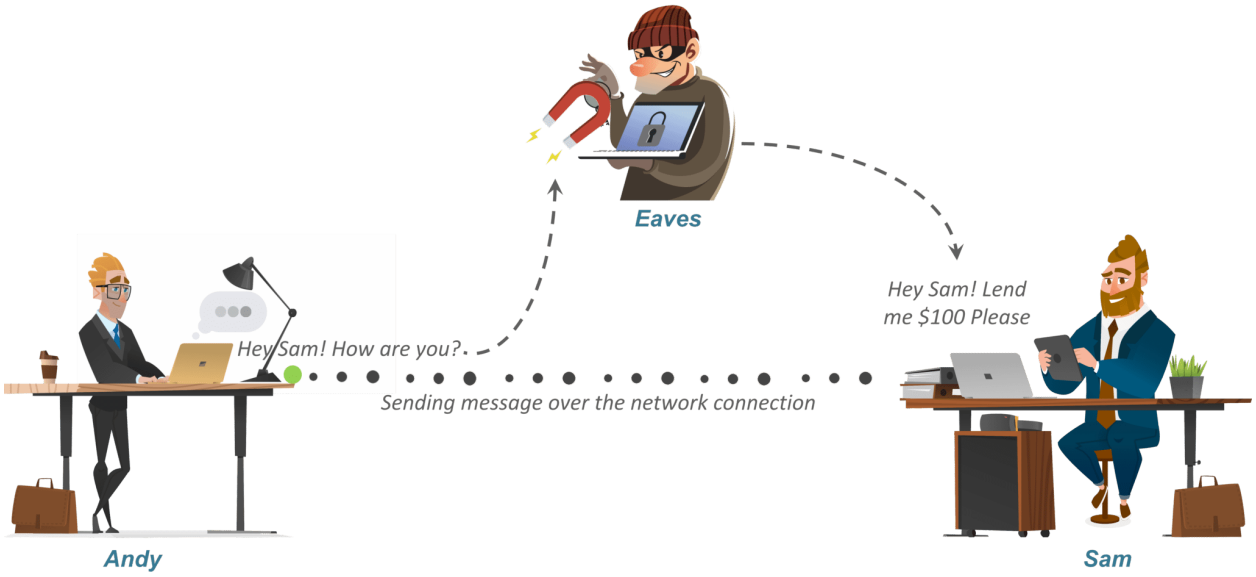
Cryptocurrencies use cryptography to allow transactions to be anonymous, secure, and “trustless,” which means you don’t need to know anything about a person to safely make transactions with them – and you don’t need a bank, credit-card company, government, or any other third party in the middle.

And cryptography isn’t just important for digital money — our computer and the networks it’s attached to are encrypting and decrypting data constantly, from every Google search you make to every email you send.

Why is cryptography important? Cryptocurrencies are entirely based on cryptographic ideas. Bitcoin was invented by a pseudonymous person (or group of people) going by the name of Satoshi Nakamoto, who proposed the idea in the form of a whitepaper posted to a cryptography message board back in 2009.

The thorniest issue that Nakamoto solved was something called the **double-spend problem**. Because Bitcoin is just code, what's to stop a person from making and spending multiple copies of their money?

Nakamoto's solution was based on a well-known encryption arrangement known as **public-private key encryption**. Bitcoin, as well as Ethereum and many other cryptocurrencies, use a technology called public-private key encryption. This allows them to be **"trustless"** – and makes secure transactions between strangers possible without a "trusted intermediary" like a bank or PayPal in the middle.



How does public-private key encryption work? The Bitcoin network issues all users a private key (essentially a strong password) from which it cryptographically generates a linked public key. You can freely give people your public key – in fact, that's the only piece of information anyone needs to send you Bitcoin. But to access those funds, the private key is required.

Part of what makes Bitcoin revolutionary is its solution for the double-spend problem: A peer-to-peer network that uses cryptographic methods to verify the authenticity of transactions.

Your public key is generated from your private key via a method called **"hashing"** – which is taking a string of data and processing it through an algorithm. It's virtually impossible to reverse this process, so nobody can guess your private key from your public key.

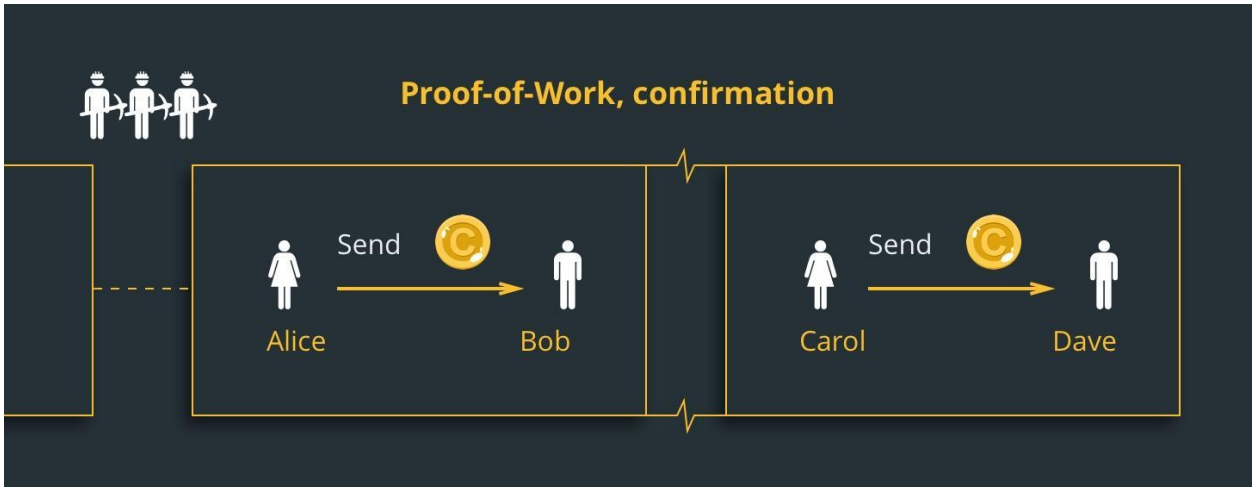
Because your public and private keys are linked, the network knows that your Bitcoin belongs to you – and will remain yours as long as you have your private key.

Another impact of not having an intermediary is that Bitcoin transactions are irreversible (after all, there is no credit-card company to call if you make a mistake). But this is a feature, not a bug: permanent transactions are a key part of the solution to the double spend problem. Any merchant who has suffered chargebacks, or refunds based on false premises, can tell you all about the wonders of irreversible transactions. Political campaign fundraisers are in the same boat.

The other half of the solution is the Bitcoin blockchain, which is a giant, decentralized ledger, like a bank's balance books, that documents every transaction and is constantly verified and updated by all the computers in the network.

Chapter 6: Proof of Work vs. Proof of Stake

"**Proof of work"** and **"proof of stake"** are the two major consensus mechanisms cryptocurrencies use to verify new transactions, add them to the blockchain, and create new tokens.



Proof of work, first pioneered by Bitcoin, uses mining to achieve those goals. Proof of stake — which is employed by Cardano, the ETH2 blockchain, and others — uses staking to achieve the same things.

Decentralized cryptocurrency networks need to make sure that nobody spends the same money twice without a central authority like Visa or PayPal in the middle. To accomplish this, networks use something called a **"consensus mechanism,"** which is a system that allows all the computers in a crypto network to agree about which transactions are legitimate.

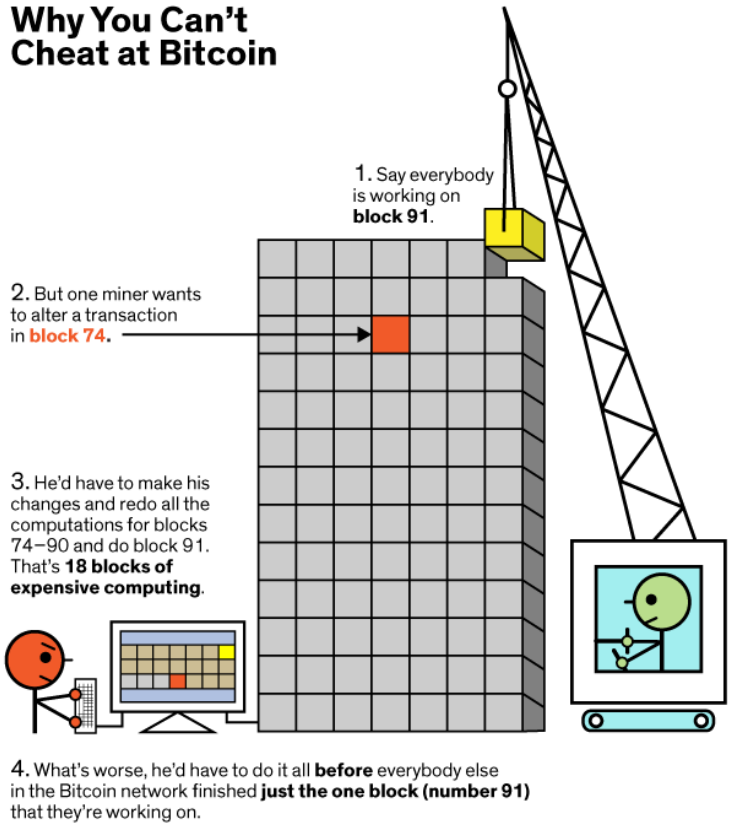
There are two major consensus mechanisms used by most cryptocurrencies today. Proof of work is the older of the two, used by Bitcoin, Ethereum 1.0, and many others.

The newer consensus mechanism is called proof of stake, and it powers Ethereum 2.0, Cardano, Tezos and other (generally newer) cryptocurrencies. To understand proof of stake, it's helpful to first understand proof of work, so we've paired them in this explainer.

What is proof of work? Proof of work is the original crypto consensus mechanism, first used by Bitcoin. Proof of work and mining are closely related ideas. The reason it's called "proof of work" is because the network requires a huge amount of processing power. Proof-of-work blockchains are secured and verified by virtual miners around the world racing to be the first to solve a math puzzle. The winner

gets to update the blockchain with the latest verified transactions and is rewarded by the network with a predetermined amount of crypto.

Proof of work has some powerful advantages, especially for a relatively simple but hugely valuable cryptocurrency like Bitcoin. It's a proven, robust way of maintaining a secure decentralized blockchain. As the value of a cryptocurrency grows, more miners are incentivized to join the network because of the higher price, increasing its power and security. Because of the astronomical amount of processing power involved, it becomes impractical for any individual or group to meddle with a valuable cryptocurrency's blockchain.



On the flip side, it's a massively energy-intensive process that can have trouble scaling to accommodate the vast number of transactions that smart contract compatible blockchains like Ethereum can generate. So, alternatives have been developed, the most popular of which is called proof of stake.

What is proof of stake? Ethereum's developers understood from the beginning that proof of work would present limitations in scalability that would eventually need to be overcome — and, indeed, as Ethereum-powered decentralized finance (DeFi) protocols have surged in popularity, the blockchain has struggled to keep up, causing fees to spike.

While the Bitcoin blockchain mostly just processes incoming and outgoing Bitcoin transactions, much like a vast checkbook, Ethereum's blockchain also has to process a vast array of DeFi transactions, like Stablecoin smart contracts, Non-Fungible Token minting and sales, and whatever imaginative innovations developers come up with in the future.

Their solution has been to build an entirely new ETH2 blockchain — which began rolling out in December 2020 and should be finished in 2022. The upgraded version of Ethereum will employ a faster and less resource intensive consensus

mechanism called proof of stake. Cryptocurrencies including Cardano, Tezos, and Atmos all use proof-of-stake consensus mechanisms — with the goal being to maximize speed and efficiency while lowering fees.

In a proof of stake system, staking serves a similar function to proof of work's mining, in that it's the process by which a network participant gets selected to add the latest batch of transactions to the blockchain and earn some crypto in exchange.

The exact details vary by project, but in general proof of stake blockchains employ a network of "validators" who contribute — or "stake" — their own crypto in exchange for a chance of getting to validate new transaction, update the blockchain, and earn a reward.

The network selects a winner based on the amount of crypto each validator has in the pool and the length of time they've had it there — literally rewarding the most invested participants.

Once the winner has validated the latest block of transactions, other validators can attest that the block is accurate. When a threshold number of attestations have been made, the network updates the blockchain.

All participating validators receive a reward in the native cryptocurrency, which is generally distributed by the network in proportion to each validator's stake.

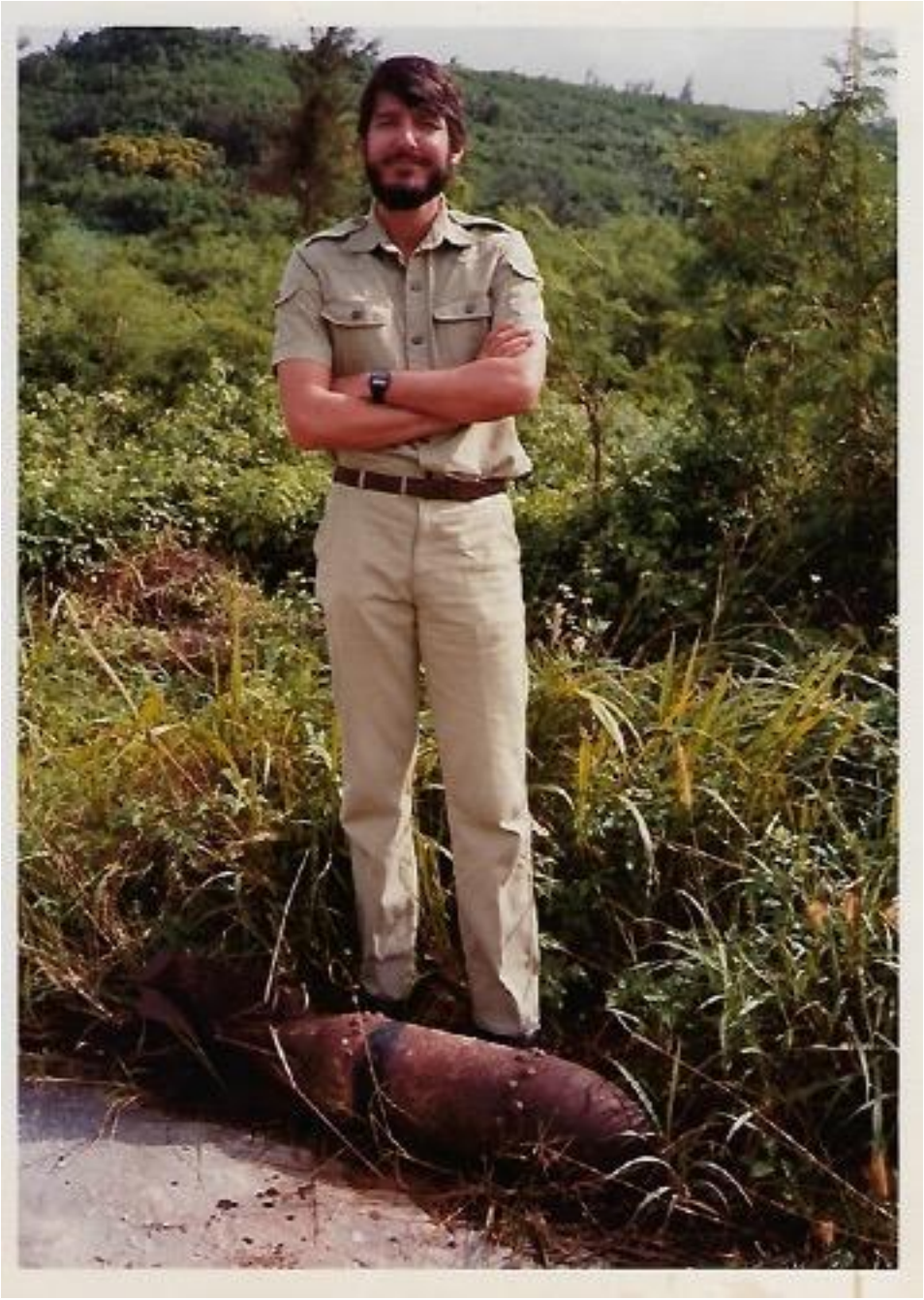
Becoming a validator is a major responsibility and requires a rather high level of technical knowledge. The minimum amount of crypto that validators are required to stake is often relatively high (for ETH2, for example, it's 32 ETH) and validators can lose some of their stake via a process called slashing if their node goes offline or if they validate a "bad" block of transactions.

But even if that sounds like too much responsibility, you can still participate in staking by joining a staking pool run by someone else — and earn rewards for crypto that would otherwise be sitting around. This process is often referred to as delegating, and tools offered by exchanges such as Coinbase can make it simple and seamless.

What are some differences between proof of work and proof of stake? Energy consumption is one major difference between the two consensus mechanisms. Because proof-of-stake blockchains don't require miners to spend electricity on duplicative processes (competing to solve the same puzzle), proof of stake allows networks to operate with substantially lower resource consumption.

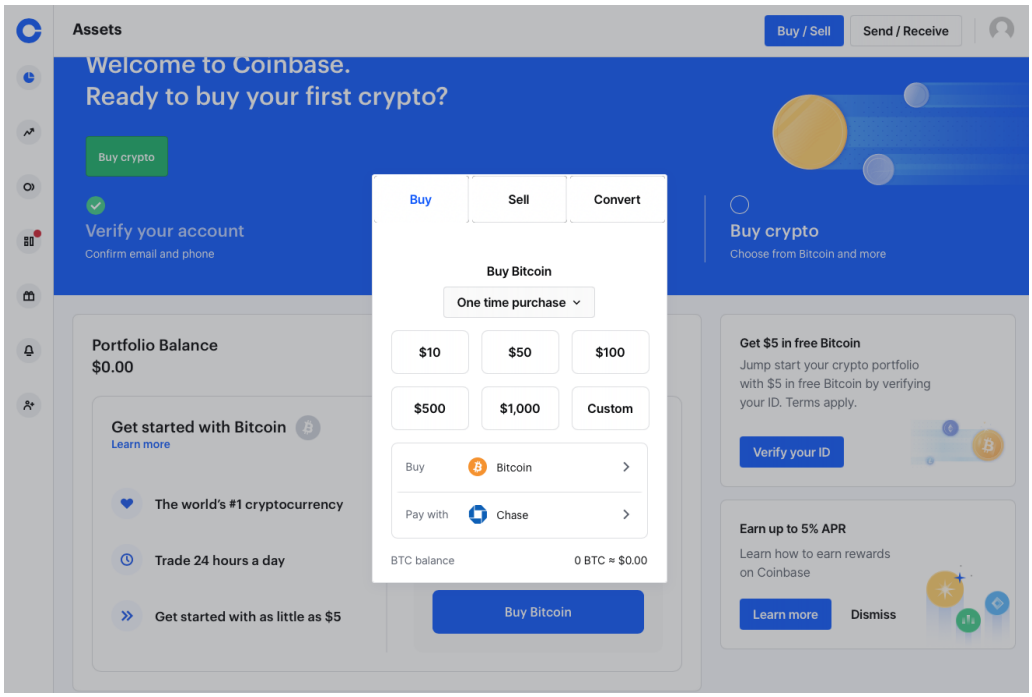
Both consensus mechanisms have economic consequences that penalize network disruptions and thwart malicious actors. In proof of work, the penalty for miners submitting invalid information, or blocks, is the sunk cost of computing power, energy, and time.

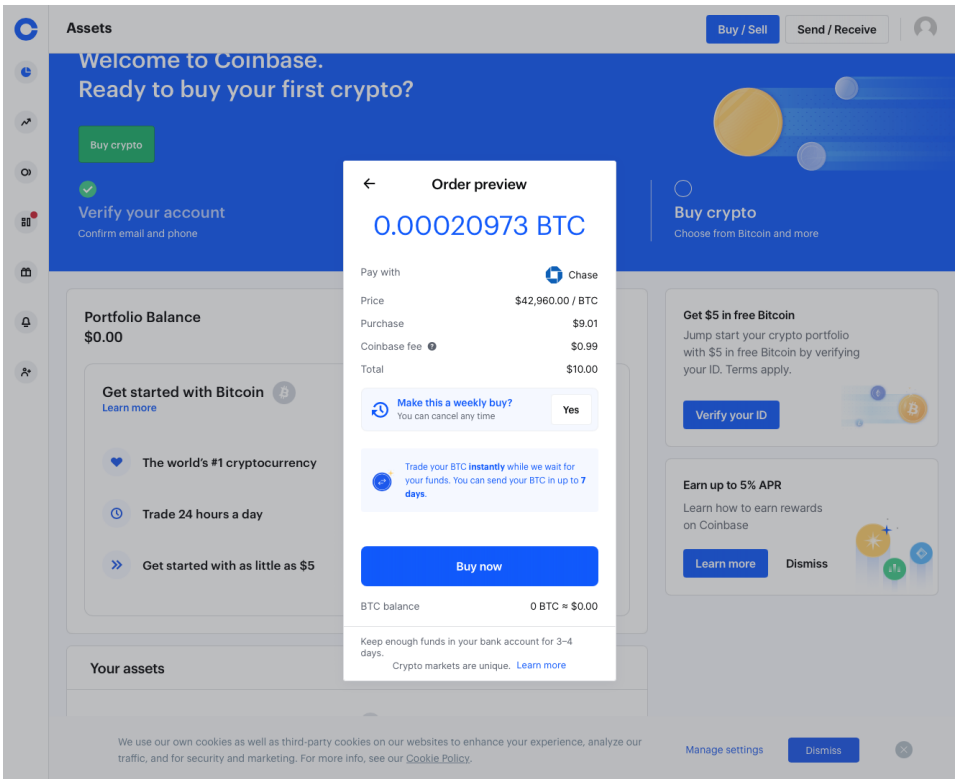
In proof of stake, the validators' staked crypto funds serve as an economic incentive to act in the network's best interests. In the case that a validator accepts a bad block, a portion of their staked funds will be "slashed" as a penalty. The amount that a validator can be slashed depends on the network.



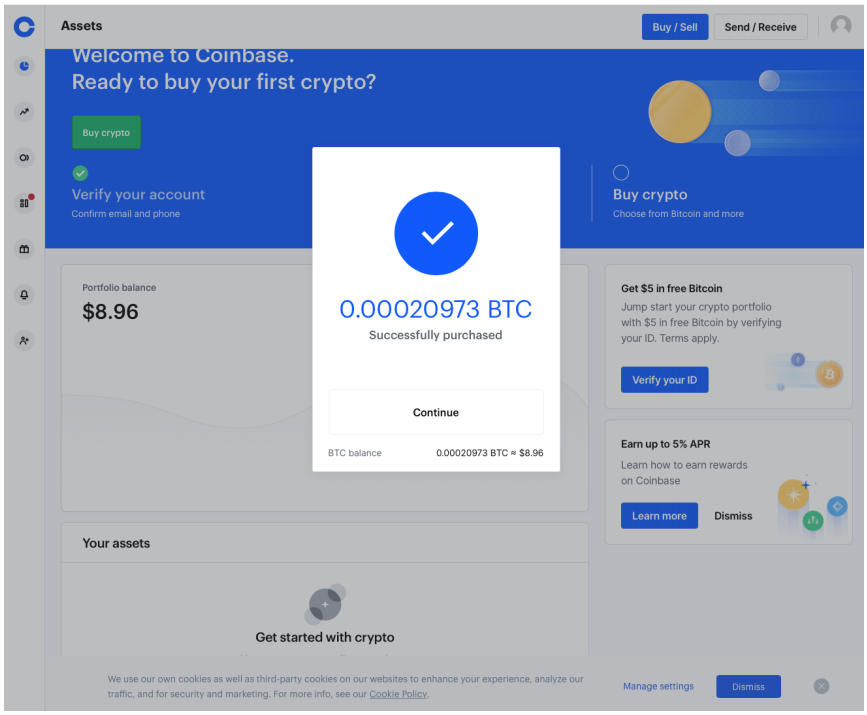
Chapter 7: How to Execute a Bitcoin Trade

Now that you have opened an account with a crypto exchange and linked it to you bank account, let's execute a trade. I'll start with my Coinbase account. I think I'll buy some Bitcoin. Click on the "BUY" tab and click on a "Buy Bitcoin" button. Being a cautious sort, I'll start with an initial purchase of $10.

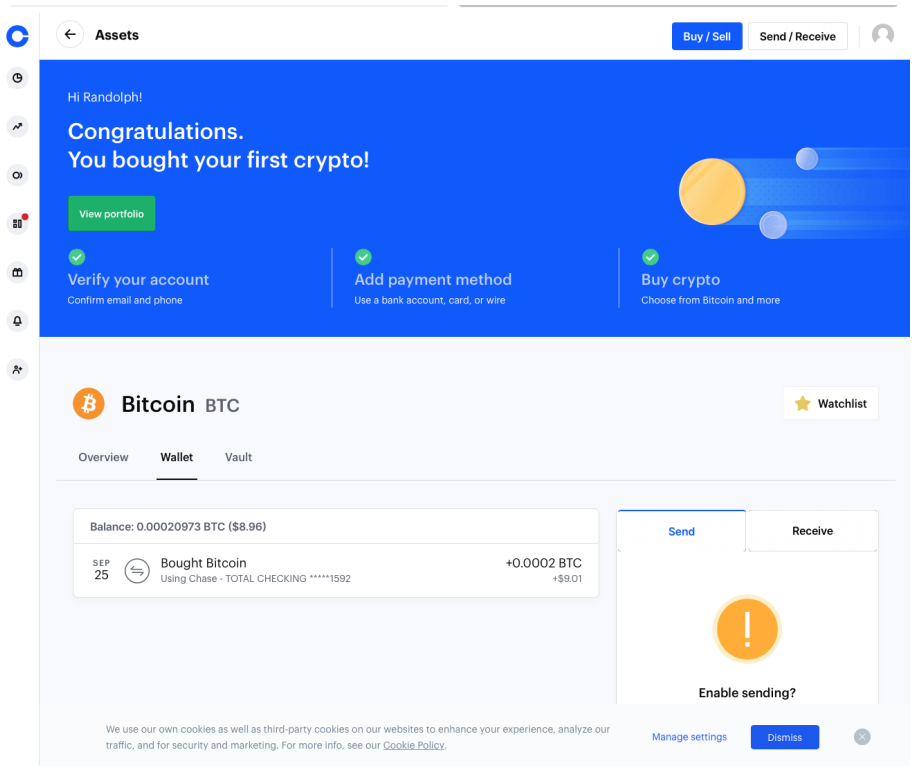




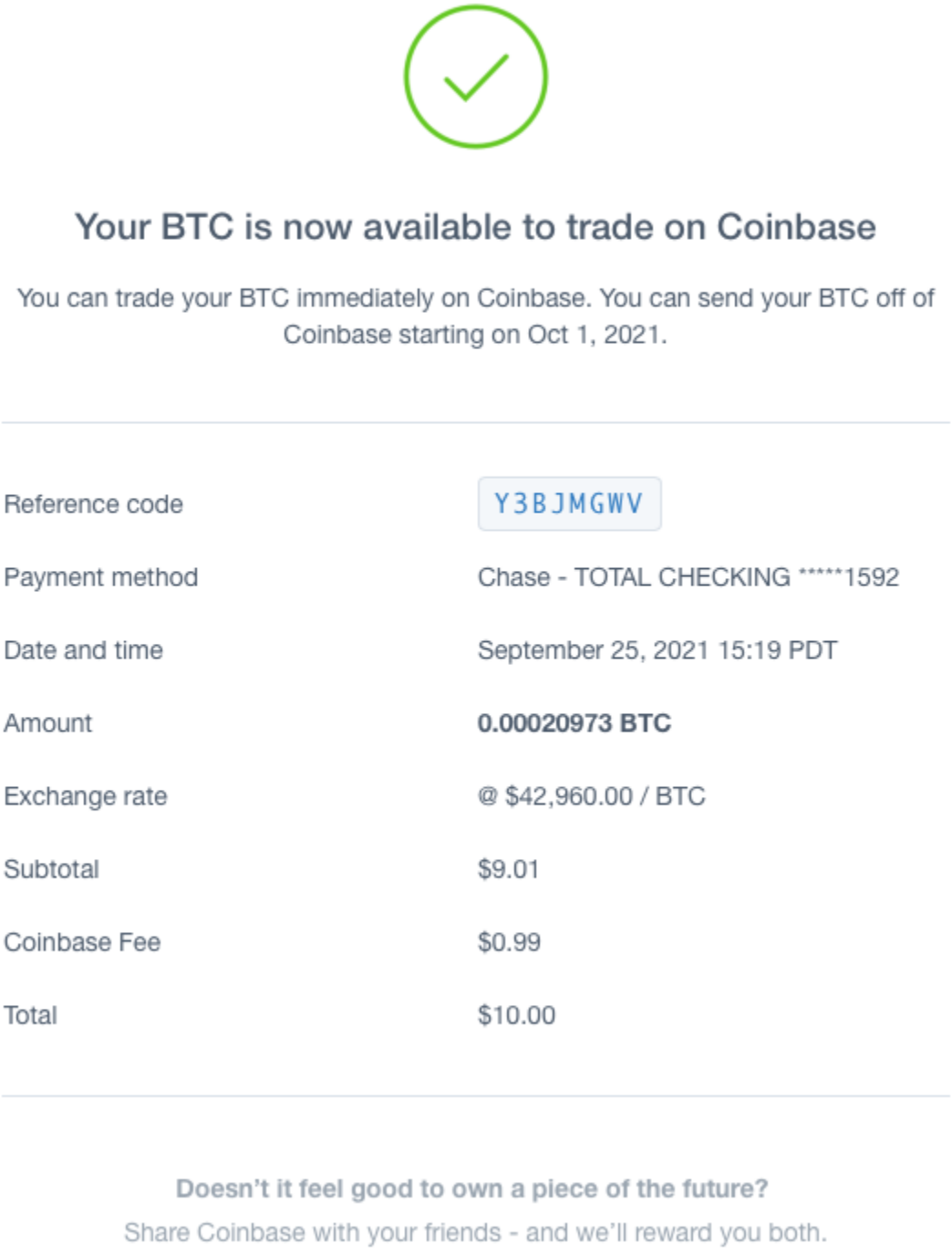
An order ticket will pop up. Review this carefully to make sure you're entering a "BUY" and not a "SELL" and that you entered the correct crypto currency. If everything looks good then click the blue "Buy Now" button.



Next, you immediately get a trade confirmation. My $10 purchase got me 0.00020973 Bitcoin, which after fees is worth $8.96.



Click on the “Assets” tab and there is my bitcoin holding, except that it has since risen by .00002 bitcoin and is now worth $9.01. I’m already a winner!



Your BTC is now available to trade on Coinbase

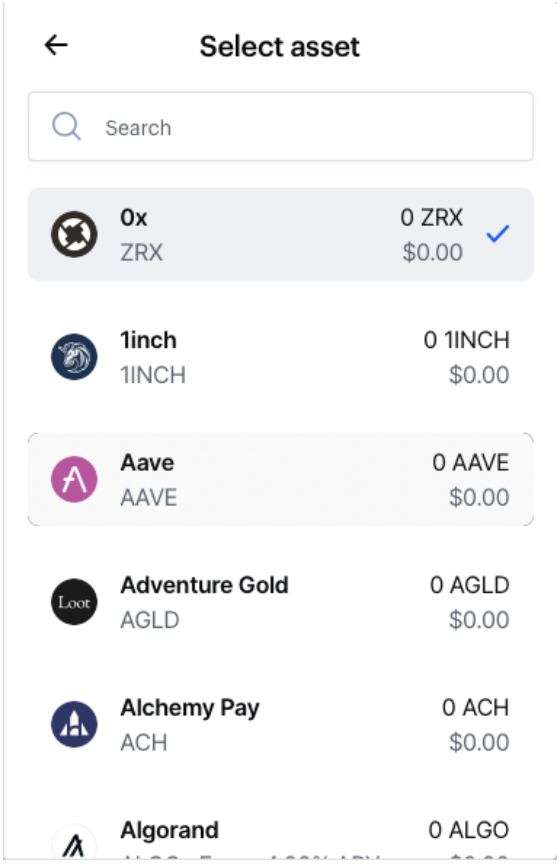
You can trade your BTC immediately on Coinbase. You can send your BTC off of Coinbase starting on Oct 1, 2021.

Reference code	Y3BJMGWV
Payment method	Chase - TOTAL CHECKING *****1592
Date and time	September 25, 2021 15:19 PDT
Amount	**0.00020973 BTC**
Exchange rate	@ $42,960.00 / BTC
Subtotal	$9.01
Coinbase Fee	$0.99
Total	$10.00

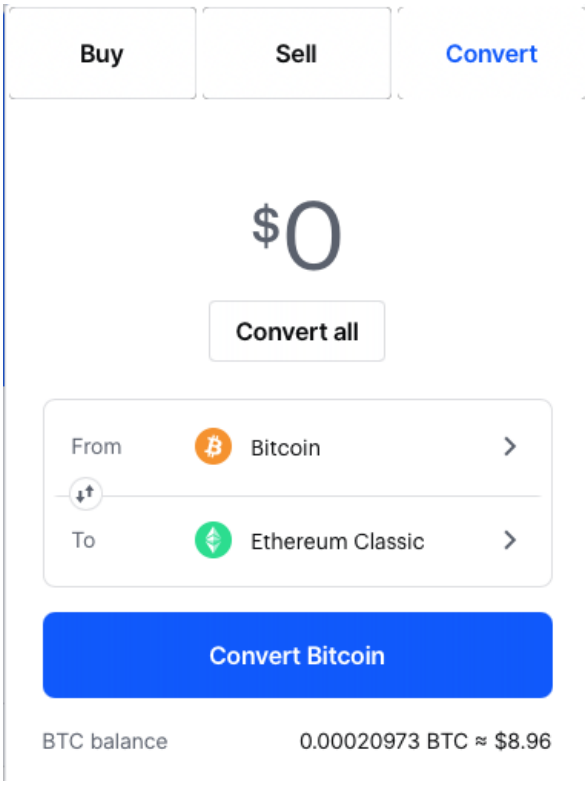
Doesn’t it feel good to own a piece of the future?

Share Coinbase with your friends - and we’ll reward you both.

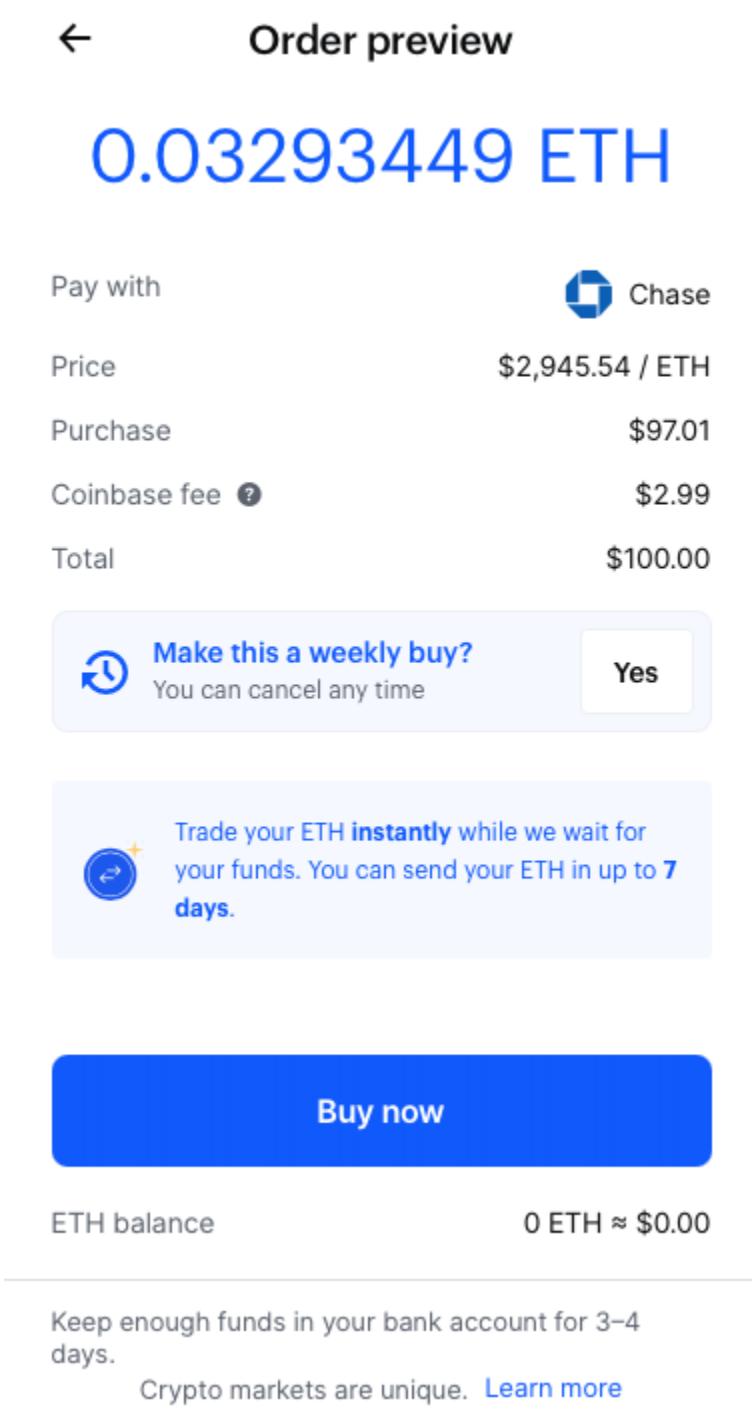
You also get a secondary confirmation listing all the details of the trade.



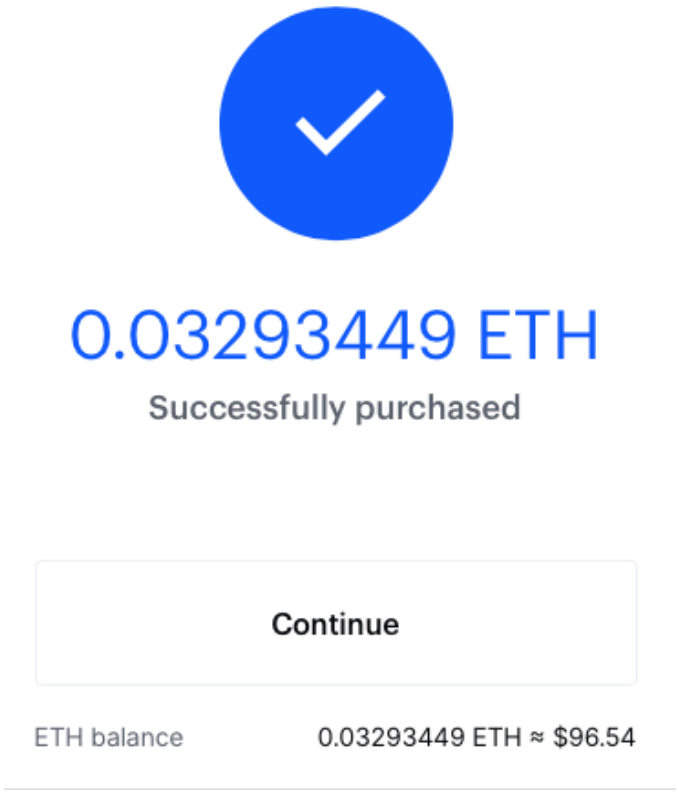
In addition to the dominant Bitcoin and Ethereum cryptos, most of the largest exchange platforms now allow you to buy a multitude of Altcoins. These are the Coinbase offerings above.



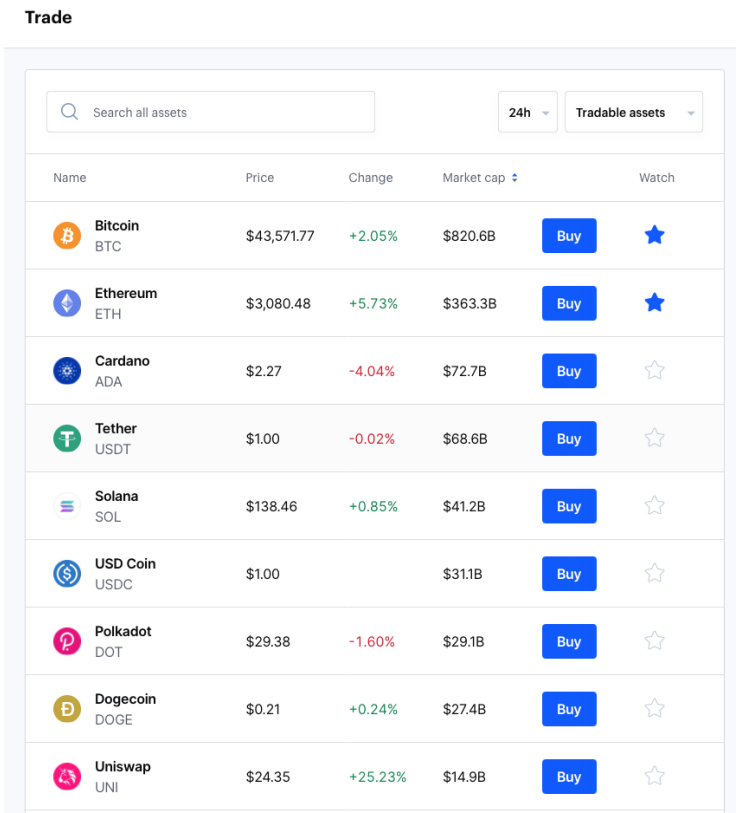
My new Bitcoin holding can be converted into other crypto currencies at any time.



That worked out so well that I think I'll diversify my crypto holdings and buy some Ethereum. Since Ethereum is much newer and cheaper than Bitcoin there is a chance that it might appreciate faster. So, I am going to be a little bit more aggressive and buy $100 worth. I hit the **"Buy Now"** button and this is what I got.



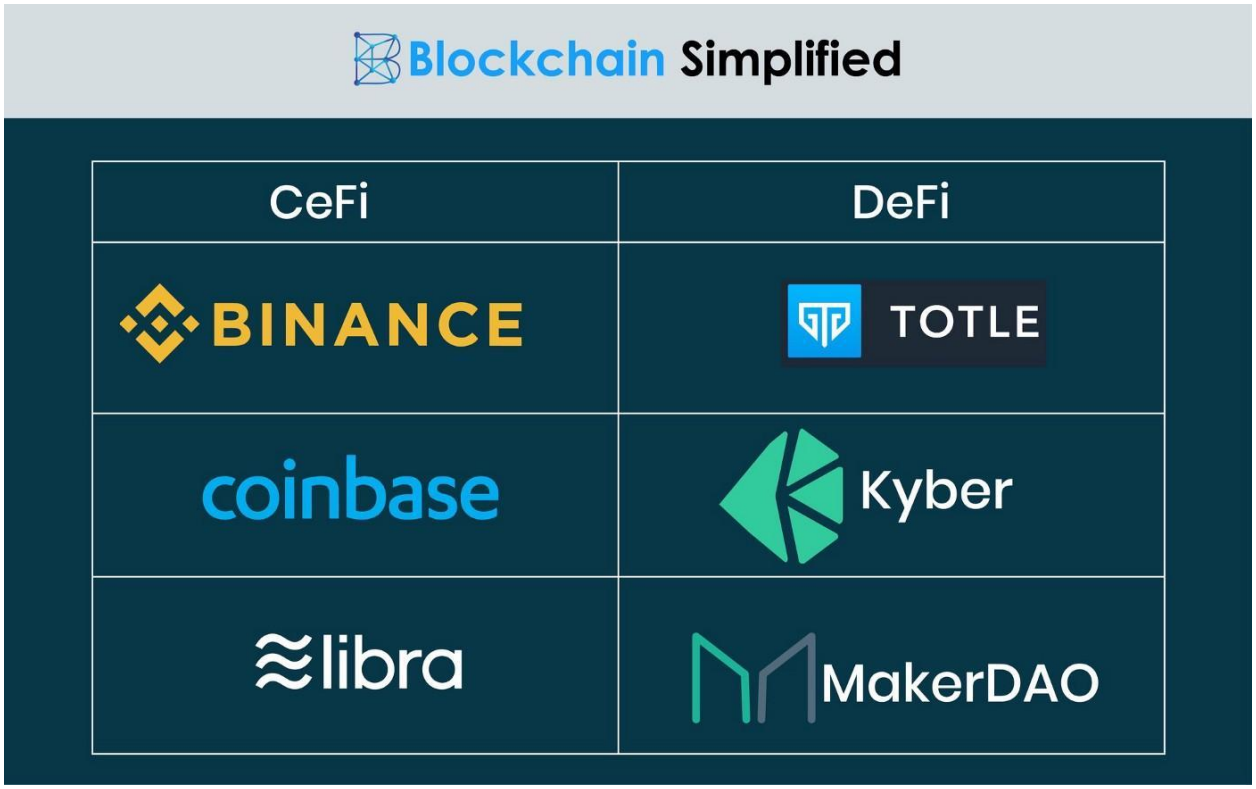
I am now the proud owner of 0.03293449 Ethereum, which after fees is worth $96.54.



Surprise, surprise, Coinbase now wants me to check out a host of other altcoins to buy. I think I'll pass for now. There is safety in size, and Bitcoin and Ethereum are far and away the largest crypto currencies.

Good luck and good Trading!

Chapter 8: Centralized Finance (CeFi) & Decentralized Finance (DeFi)



DeFi (or **"decentralized finance")** is an umbrella term for financial services on public blockchains, primarily Ethereum. With DeFi, you can do most of the things that banks support — earn interest, borrow, lend, buy insurance, trade derivatives, trade assets, and more — but it's faster and doesn't require paperwork or a third party. As with crypto generally, DeFi is global, peer-to-peer (meaning directly between two people, not routed through a centralized system), pseudonymous, and open to all.

One of crypto's core concepts is "decentralization" — which allows transactions between strangers anywhere in the world to be conducted without any kind of institution in the middle.

(DeFi) takes that idea the farthest. It's an entire ecosystem of smart-contract powered apps that make it possible to lend, save, trade, and more — all without any kind of bank or payment processor in the middle.

But because DeFi is an emerging technology, it comes with a set of unique risks. Navigating DeFi protocols requires a relatively strong level of technical knowledge and comfort with the potential for losing some or all of your investment in the case of buggy code, malicious actors, or even simple user error.

CeFi, as you've probably guessed, stands for "centralized finance." The core idea behind CeFi is to create crypto investment opportunities that offer some of the yield benefits of DeFi with some of the ease of use and security of traditional financial-services products (sometimes referred to as TradFi). With CeFi, you can borrow money, buy and sell crypto, spend and earn rewards with a crypto debit card, and more.

How do you earn yield with CeFi? CeFi creates the potential for earning yield via crypto-based accounts that are functionally similar to a traditional bank's savings account— but may offer substantially higher returns. Unlike conventional savings accounts, crypto deposits aren't currently eligible for government-backed FDIC or SIPC insurance so you should make sure to understand the risks involved.

Coinbase, however, does offer a principal guarantee on the USDC you deposit for CeFi lending. The general concept involves holding some of your crypto on one of the many platforms that offer this kind of product. Via Coinbase, US-based customers in many states can now sign up for a waiting list to start earning an annual yield of 4% for holding USD Coin (USDC).

Where does the yield come from? Some or all of your crypto holdings are put to work and lent out to others. These borrowers pay the centralized provider an interest rate for borrowing, and that provider passes on some of the interest to you.

How does CeFi borrowing connect to CeFi lending/saving? CeFi makes it possible to borrow money against your crypto holdings, the same way you'd use traditional assets as collateral to apply for a bank loan. It's the flip side of lending — the interest users pay for borrowing money is where the yield you can earn for holding crypto via CeFi is generated.

Unlike bank loans, CeFi loans typically require little or no paperwork. Via Coinbase, US-based customers in many states can borrow up to $100,000 without a credit check.

What are some CeFi risks? Each CeFi product and provider is unique and may put your deposited crypto to work in ways that have higher or lower levels of risk. It's important to do your homework and understand how your crypto is being used, how the yield you're earning is generated, and what risks are entailed.

Remember, crypto deposits aren't currently eligible for the government-backed insurance that protects savings held by a traditional bank. That said, Coinbase's CeFi lending product offers a principal guarantee as long as Coinbase remains in business.

Some CeFi providers might lock up your principal for a period of time, like a year. Coinbase, however, allows you to access your USDC at any time.

All stablecoins aren't created equal. For example, USDC is based on open-source code that anyone can scrutinize. USDC is backed by dollar-denominated assets of at least equal fair value to the USDC in circulation, in segregated accounts with US regulated financial institutions. You can buy USDC via exchanges like Coinbase and hold it in any Ethereum compatible wallet.

There are no fees for transferring a US dollar to USDC. The launch of USDC was powered by a collaboration between Coinbase and Circle through the co-founding of the CENTRE Consortium.

Chapter 9: Bitcoin Details

Bitcoin (₿) is a decentralized digital currency without a central bank or single administrator, that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.

Transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a blockchain.

The cryptocurrency was invented in 2008 by an unknown person or group of people using the name Satoshi Nakamoto. The currency began use in 2009 when its implementation was released as open-source software. There are 100 million **satoshis** to a bitcoin, the unit with which we will all someday be buying our cups of coffee.

Bitcoins are created as a reward for a process known as mining. They can be exchanged for other currencies, products, and services, but the real-world value of the coins is extremely volatile. Research produced by the University of Cambridge estimated that in 2017, there were 2.9 to 5.8 million unique users using a cryptocurrency wallet, most of them using Bitcoin.

Bitcoin has been criticized for its use in illegal transactions, the large amount of electricity (and thus carbon footprint) used by mining, price volatility and thefts from exchanges. Bitcoin has suffered five 80% corrections since inception.

Some economists and commentators have characterized it as a speculative bubble

at various times. Bitcoin has also been used as an investment, although several regulatory agencies have issued investor alerts about Bitcoin such as America's Securities Exchange Commission.

The word Bitcoin was defined in a white paper published on October 31, 2008. It is a combination of the words "bit" and "coin." No uniform convention for Bitcoin capitalization exists; some sources use Bitcoin, capitalized, to refer to the technology and network and Bitcoin, lowercase, for the unit of account.

Chapter 10: Bitcoin - A Long History

Creation

Bitcoin logos made by Satoshi Nakamoto in 2009 depict Bitcoins as imaginary gold tokens.

The domain name bitcoin.org was registered on 18 August 2008. On 31 October 2008, a link to a paper authored by Satoshi Nakamoto titled "***Bitcoin: A Peer-to-Peer Electronic Cash System***" was posted to a cryptography mailing list.

Nakamoto implemented the Bitcoin software as open-source code and released it in January 2009. Nakamoto's identity remains unknown. I personally believe it is likely to be a major US government agency such as the CIA or the National Security Agency.


THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69523 £1.50

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salmon Rushdie I Won't Marry Again

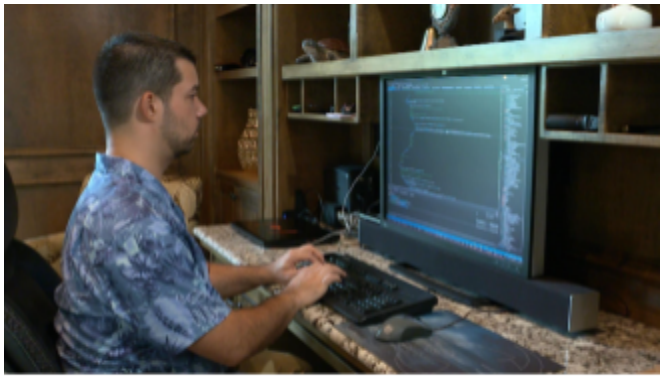
Giant Killing? Guide to the FA Cup Third Round

On 3 January 2009, the Bitcoin network was created when Nakamoto mined the starting block of the chain, known as the genesis block. To prove that the creators had a sense of humor, embedded in the coinbase of this block was this text, a headline from the ***London Times***, "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." This note references a headline published and has been interpreted as both a timestamp and a comment on the instability caused by traditional reserve banking.

The receiver of the first Bitcoin transaction was Mr. Hal Finney, who had created the first reusable proof-of-work system (RPoW) in 2004. Finney downloaded the Bitcoin software on its release date, and on 12 January 2009 received ten Bitcoins from Nakamoto. Other early cypherpunk supporters were creators of Bitcoin predecessors: Wei Dai, creator of b-money, and Nick Szabo, creator of bitgold.

Mr. Hal Finney

Wei Dai



Laszlo Hanyecz

Nick Szabo

Gavin Andresen

In 2010, the first known commercial transaction using bitcoin occurred when programmer Mr. Laszlo Hanyecz bought two Papa John's pizzas for ฿10,000. Today, ฿10,000 is worth about $500 million.

Blockchain analysts estimate that Nakamoto had mined about one million Bitcoins before disappearing in 2010 when he handed the network alert key and control of the code repository over to Mr. Gavin Andresen. Andresen later became lead developer at the Bitcoin Foundation. Andresen then sought to decentralize control.

2011–2012

After early “proof of concept” transactions, the first major users of Bitcoin were black markets, such as Silk Road. During its 30 months of existence, beginning in February 2011, Silk Road exclusively accepted Bitcoins as payment, transacting 9.9 million in Bitcoins, worth about $214 million.

In 2011, the price started at $0.30 per Bitcoin, growing to $5.27 for the year. The price rose to $31.50 on 8 June. Within a month, the price fell to $11.00. The next month it fell to $7.80, and in another month to $4.77.

In 2012, Bitcoin prices started at $5.27, growing to $13.30 for the year. By 9 January the price had risen to $7.38, but then crashed by 49% to $3.80 over the next 16 days. The price then rose to $16.41 on 17 August but fell by 57% to $7.10 over the next three days.

2013–2016

In 2013, prices started at $13.30 rising to $770 by 1 January 2014. In March 2013 the blockchain temporarily split into two independent chains with different rules due to a bug in version 0.8 of the Bitcoin software. The two blockchains operated simultaneously for six hours, each with its own version of the transaction history from the moment of the split.

Normal operation was restored when most of the network downgraded to version 0.7 of the Bitcoin software, selecting the backwards-compatible version of the blockchain. As a result, this blockchain became the longest chain and could be accepted by all participants, regardless of their Bitcoin software version.

During the split, the Mt. Gox Exchange briefly halted Bitcoin deposits and the price dropped by 23% to $37 before recovering to the previous level of approximately $48 in the following hours.

The US Financial Crimes Enforcement Network (FinCEN) established regulatory guidelines for "decentralized virtual currencies" such as Bitcoin, classifying American Bitcoin miners, who sell their generated Bitcoins as Money Service Businesses (MSBs), that are subject to registration or other legal obligations.

In April, Mt. Gox exchange experienced processing delays due to insufficient capacity resulting in the Bitcoin price dropping from $266 to $76 before returning to $160 within six hours. The Bitcoin price rose to $259 on 10 April, but then crashed by 83% to $45 over the next three days.

On 15 May 2013, US authorities seized accounts associated with Mt. Gox after discovering it had not registered as a money transmitter with FinCEN in the US. On 23 June 2013, the US Drug Enforcement Administration listed ₿11.02 as a seized asset in a United States Department of Justice seizure notice pursuant to 21 U.S.C. § 881.

This marked the first time a government agency had seized Bitcoin. The FBI seized about ₿30,000 in October 2013 from the dark web website, Silk Road. These Bitcoins were sold at blind auction by the United States Marshals Service to my friend, well known venture capital investor.

Bitcoin's price rose to $755 on 19 November and crashed by 50% to $378 the same day. On 30 November 2013, the price reached $1,163 before starting a long-term crash, declining by 87% to $152 in January 2015.

On 5 December 2013, the People's Bank of China prohibited Chinese financial institutions from using Bitcoins. After the announcement, the value of Bitcoins dropped, and Chinese Internet platform, Baidu no longer accepted Bitcoins.

In 2014, prices started at $770 and fell to $314 for the year.

In 2015, prices started at $314 and rose to $434 for the year. In 2016, prices rose and climbed up to $998 by 1 January 2017.

Release 0.10 of the software was made public on 16 February 2015. It introduced a consensus library which gave programmers easy access to the rules governing on the network. In version 0.11.2 developers added a new feature, which allowed transactions to be made unspendable until a specific time in the future.

Bitcoin Core 0.12.1 was released on 15 April 2016 and enabled multiple soft forks to occur concurrently. Around 100 contributors worked on Bitcoin Core 0.13.0 which was released on 23 August 2016. In July 2016, the CheckSequenceVerify soft fork activated.

2017–2019

On 21 July 2017, Bitcoin was trading at $2,748, up 52% from 14 July 2017's $1,835. Supporters of large blocks who were dissatisfied with the activation of SegWit forked the software on 1 August 2017 to create Bitcoin Cash, becoming one of many forks of Bitcoin. Prices started at $998 in 2017 and rose to $13,412.44 on 1 January 2018, after reaching its all-time high of $19,783.06 on 17 December 2017.

China banned trading in Bitcoin, with first steps taken in September 2017, and a complete ban that started on 1 February 2018. Bitcoin prices then fell from $9,052 to $6,914 on 5 February 2018. The percentage of Bitcoin trading in the Chinese renminbi fell from over 90% in September 2017 to less than 1% in June 2018.

Throughout the rest of the first half of 2018, Bitcoin's price fluctuated between $11,480 and $5,848. On 1 July 2018, Bitcoin's price was $6,343. The price on 1 January 2019 was $3,747, down 72% for 2018 and down 81% since the all-time high.

In September 2018, an anonymous party discovered and reported an invalid-block denial-of-server vulnerability to developers of Bitcoin Core, Bitcoin ABC and Bitcoin Unlimited. Further analysis by Bitcoin developers showed the issue could also allow the creation of blocks violating the 21-million-coin limit and it was assigned and the issue resolved.

Bitcoin prices were negatively affected by several hacks or thefts from cryptocurrency exchanges, including thefts from Coincheck in January 2018 Bithumb, in June, and Bancor in July. For the first six months of 2018, $761 million worth of cryptocurrencies was reported stolen from exchanges.

Bitcoin's price was affected even though other cryptocurrencies were stolen at Coinrail and Bancor as investors worried about the security of cryptocurrency exchanges. In September 2019 the Intercontinental Exchange (the owner of the New York Stock Exchange) began trading Bitcoin futures on its exchange called Bakkt. Bakkt also announced that it would launch options on Bitcoin in December 2019.

In December 2019, YouTube removed Bitcoin and cryptocurrency videos, but later restored the content after judging they had "made the wrong call." In February 2019, Canadian cryptocurrency exchange Quadriga Fintech Solutions failed with approximately $200 million missing. By June 2019 the price had recovered to $13,000.

2020–present

On 13 March 2020, Bitcoin fell below $4,000 during a broad market selloff, after trading above $10,000 in February 2020. On 11 March 2020, 281,000 Bitcoins were sold, held by owners for only thirty days. This compared to ₿4,131 that had laid dormant for a year or more, indicating that most of the Bitcoin volatility on that day was from recent buyers.

During the week of 11 March 2020, cryptocurrency exchange Kraken experienced an 83% increase in the number of account signups over the week of Bitcoin's price

collapse, a result of buyers looking to capitalize on the low price. These events were attributed to the onset of the Covid-19 pandemic.

In August 2020, MicroStrategy (MSTR) invested $250 million in Bitcoin as a treasury reserve asset. In October 2020, Square (SQ) placed approximately 1% of total assets ($50 million) in Bitcoin. In November 2020, PayPal (PYPL) announced that US users could buy, hold, or sell Bitcoin. On 30 November 2020, the Bitcoin value reached a new all-time high of $19,860, topping the previous high of December 2017.

Alexander Vinnik

Alexander Vinnik, founder of BTC-e, was convicted and sentenced to five years in prison for money laundering in France while refusing to testify during his trial. In December 2020, Massachusetts Mutual Life Insurance Company announced a Bitcoin purchase of USD $100 million, or roughly 0.04% of its general investment account.

On 19 January 2021, Elon Musk placed the handle #Bitcoin in his Twitter profile, tweeting "In retrospect, it was inevitable", which caused the price to briefly rise about $5,000 in an hour to $37,299. On 25 January 2021, MicroStrategy announced that it continued to buy Bitcoin and as of the same date it had holdings of ₿70,784 worth $2.38 billion. On 8 February 2021
Tesla's announcement of a Bitcoin purchase of USD $1.5 billion and the plan to start accepting Bitcoin as payment for vehicles, pushed the Bitcoin price to $44,141.

On 18 February 2021, Elon Musk stated that "owning Bitcoin was only a little better than holding conventional cash, but that the slight difference made it a better asset to hold". After 49 days of accepting the digital currency, Tesla reversed course on May 12, 2021, saying they would no longer take Bitcoin due to concerns that "mining" the cryptocurrency was contributing to the consumption of fossil fuels and climate change. The decision resulted in the price of Bitcoin dropping around 12% on May 13.

During a July Bitcoin conference, Musk suggested Tesla could possibly help Bitcoin miners switch to renewable energy in the future and stated at the same conference that if Bitcoin mining reaches, and trends above 50 percent renewable energy usage, that "Tesla would resume accepting Bitcoin." The price for Bitcoin rose after this announcement.

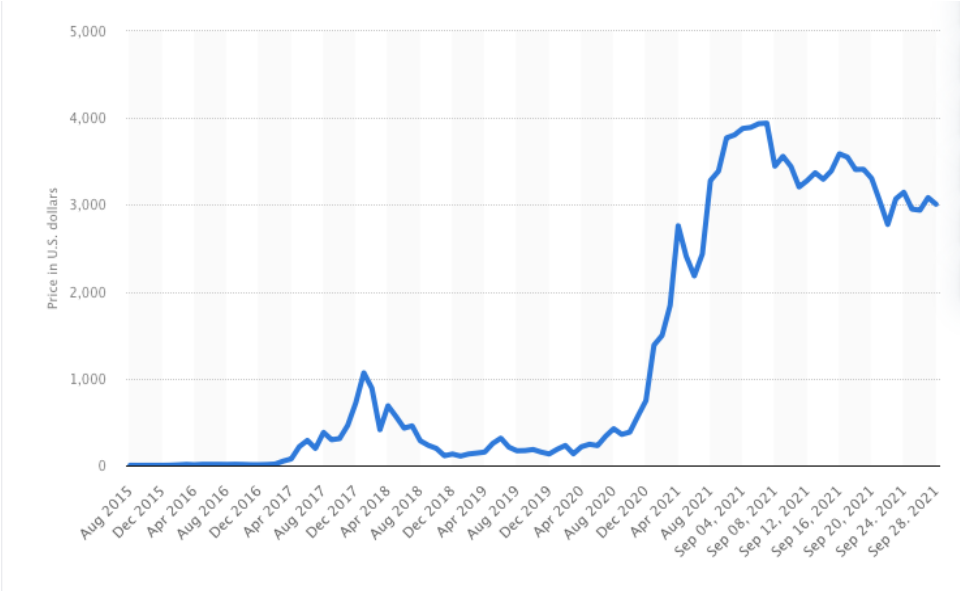
In September 2020, the Canton of Zug, Switzerland announced that it would start accepting tax payments in Bitcoin by February 2021. In June 2021, El Salvador voted to make Bitcoin legal tender in El Salvador. The law took effect on September 7.

Chapter 11: Ethereum

Ethereum is a decentralized, open-source blockchain with smart contract functionality. Ether (ETH or Ξ) is the native cryptocurrency of the platform. Amongst cryptocurrencies, Ether is second only to Bitcoin in market capitalization.

Ethereum was conceived in 2013 by programmer Vitalik Buterin. In 2014, development work commenced which was crowdfunded, and the network went live on 30 July 2015. The platform allows anyone to deploy permanent and immutable decentralized applications onto it, with which users can interact.

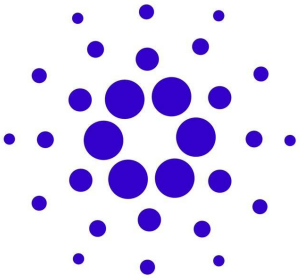
Decentralized Finance (DeFi) applications provide a broad array of financial services without the need for typical financial intermediates like brokerages, exchanges, or banks such as allowing cryptocurrency users to borrow against their holdings or lend them out for interest.



Ethereum also allows for the creation and exchange of Non Fungible Tokens, which are non-interchangeable tokens connected to digital works of art or other real-world items and sold as unique digital property. Additionally, many other cryptocurrencies operate as ERC-20 tokens on top of the Ethereum blockchain and have utilized the platform for initial coin offerings.

Ethereum has started implementing a series of upgrades called Ethereum 2.0, which includes a transition to proof of stake and aims to increase transaction throughput using sharding, or database partitioning.

Chapter 12: Cardano



Cardano is one of the biggest cryptocurrencies by market capitalization. It's designed to be a next-gen evolution of the Ethereum idea — with a blockchain that's a flexible, sustainable, and scalable platform for running smart contracts, which will allow the development of a wide range of decentralized finance apps, new crypto tokens, games, and more.

Smart-contract functionality has yet to be rolled out by developers. An upgrade in the second quarter of 2020 unlocked smart-contract features, bringing Cardano one step closer to its goal of providing developers with a blockchain platform that is robust, secure, scalable, and highly energy-efficient.

Much like the Ethereum blockchain's native cryptocurrency is ETH, the Cardano blockchain's native cryptocurrency is ADA — which can be bought or sold via exchanges like Coinbase. Today, ADA can be used to store value (perhaps as part of your investment portfolio), to send and receive payments, and for staking and paying transaction fees on the Cardano network.

How does Cardano work? Cardano's goal is to be the most environmentally sustainable blockchain platform. It uses a unique proof-of-stake consensus mechanism called Ouroboros, as opposed to the energy-intensive proof-of-work system currently used by Bitcoin and Ethereum. (Ethereum is also moving to a proof-of-stake system via the ETH2 upgrade).

What is proof of work? Decentralized cryptocurrency networks need to make sure that nobody spends the same money twice without a central authority like Visa or PayPal in the middle. To accomplish this, they use a "consensus mechanism." The original crypto consensus mechanism is called proof of work, first popularized by Bitcoin mining.

Proof of work requires a huge amount of processing power, which is contributed by virtual "miners" around the world competing to be the first to solve a time-consuming math puzzle. The winner gets to update the blockchain with the latest verified transactions and is rewarded with a predetermined amount of crypto.

What is proof of stake? Rather than using a network of miners racing to solve a puzzle, proof of stake uses a network of invested participants called validators.

Instead of contributing processing power to secure the network and verify transactions as miners do, validators stake their own ADA. The network selects a winner based on the amount of ADA each validator has in the pool and the length of time they've had it there — literally rewarding the most invested participants.

Once the winner has validated the latest block of transactions, other validators can attest that the block is accurate. When a threshold number of attestations have been made, the network updates the blockchain. All participating validators receive a reward in ADA, which is distributed by the network in proportion to each validator's stake.

Becoming a validator is a major responsibility but interested parties can also earn ADA rewards by "delegating" some of their crypto to a staking pool run by someone else.

The Cardano blockchain is also divided into two separate layers: the Cardano Settlement Layer (CSL) and the Cardano Computing Layer (CCL). The CSL contains the ledger of accounts and balances (and is where the transactions are validated by the Ouroboros consensus mechanism).

The CCL layer is where all the computations for apps running on the blockchain are executed — via the operations of smart contracts. The idea of splitting the blockchain into two layers is to help the Cardano network to process as many as a million transactions a second.

What are Cardano native tokens? On March 1, 2021, the Cardano blockchain introduced the ability to create native tokens. Like Ethereum tokens — which can include things like NFTs or stablecoins like USD Coin — Cardano native assets can be created and distributed on the blockchain and are able to interact with smart contracts.

But unlike Ethereum-based tokens, Cardano native tokens aren't created via smart contract. Instead, they run on the same architecture as the ADA cryptocurrency itself. According to the nonprofit Cardano Foundation, this makes Cardano native assets "first-class citizens" on the blockchain. Their native architecture can theoretically make these tokens more secure and reduce the fees associated with transactions.

Cardano was launched in September 2017 by Ethereum co-founder Charles Hoskinson and aims to be a third generation blockchain (or blockchain 3.0) project — building on top of the technology pioneered by Bitcoin (first gen) and Ethereum (second gen). Cardano's goal is to be a highly scalable and energy-efficient smart contract platform.

The Ouroboros consensus mechanism is based on peer-reviewed research by a team of computer scientists and cryptographers from the University of Edinburgh, Tokyo University, and other institutions. Their goal was to build a decentralized network that could validate transactions in a scalable, secure way — while ensuring that the Cardano platform would be as energy-efficient as possible.

What is ADA? ADA is the native cryptocurrency of the Cardano platform (named after Ada Lovelace, the 19th-century mathematician often referred to as the "world's first computer programmer"). ADA tokens fuel the Cardano platform much like ETH tokens fuel the Ethereum platform. They're used to pay transaction fees and are staked by validators (and delegators) who want to help maintain security and stability of the network in exchange for earning rewards.

In the future, ADA will also be used as a governance token, which will allow holders to vote on changes and upgrades to the Cardano platform.

What's next for Cardano? In the second quarter of 2021, smart contract functionality is scheduled to arrive on the Cardano platform. Developers have also announced that the blockchain will become compatible with Ethereum-based smart contracts later in the year — potentially allowing it to run a wide range of existing apps and allowing developers to work on Cardano projects using the familiar Solidity programming language.

Cardano also plans to become completely decentralized through the implementation of community-driven governance and an automated treasury system to fund the future of the network.

Chapter 13: Altcoins

Altcoins are cryptocurrencies other than Bitcoin. They share characteristics with Bitcoin but are also different from them in other important ways. For example, some altcoins use a different consensus mechanism to produce blocks or validate transactions. Or they distinguish themselves from Bitcoin by providing new or additional capabilities, such as smart contracts or low-price volatility.

As of March 2021, there were almost 9,000 cryptocurrencies. According to CoinMarketCap, altcoins accounted for over 40% of the total cryptocurrency market in March 2021.[1]Because they are derived from Bitcoin, altcoin price movements tend to mimic Bitcoin's trajectory. However, analysts say the maturity of cryptocurrency investing ecosystems and the development of new markets for these coins will make price movements for altcoins independent of Bitcoin's trading signals.

"Altcoin" is a combination of the two words "alt" and "coin" and includes all alternatives to Bitcoin. The basic framework for Bitcoin and altcoins is similar. Thus, they share code and function as peer-to-peer systems or as a giant computer capable of processing large amounts of data and transactions at the same time. In some instances, altcoins also aspire to become the next Bitcoin by becoming an inexpensive method for digital transactions.

But there are also several differences between the two entities.

Bitcoin is among the first iterations of a cryptocurrency and its philosophy and design set the benchmark for the development of other coins. However, its implementation has several shortcomings. For example, Proof-of-Work (PoW), the consensus mechanism used to create blocks, is energy-intensive and time-consuming. Bitcoin's smart contract capabilities are also limited.

Altcoins improve upon Bitcoin's perceived limitations to establish a competitive advantage. Several altcoins use the Proof-of-Stake (PoS) consensus method to

minimize energy consumption and the time required to create blocks and validate new transactions.

Another example is that of ether, the world's second-biggest cryptocurrency by market cap, which is used as gas (or payment for transaction costs) in smart contracts on Ethereum. Altcoins also address traditional critiques against Bitcoin. For example, stablecoins do not exhibit Bitcoin's price volatility, making them ideal vehicles for daily transactions.

By distinguishing themselves from Bitcoin in this manner, altcoins have created a market for themselves. In turn, this has attracted investors who see potential in them as alternatives to Bitcoin. The investors expect to profit as altcoins garner more traction and users and appreciate in price.

Depending on their functionalities and consensus mechanisms, altcoins come in various flavors and categories. Here's a summary of some of the more important ones: It is possible for an altcoin to fall into more than one category.

Mining-Based

As their name indicates, mining-based altcoins are mined into existence. Most mining-based altcoins use Proof-of-Work (PoW), a method in which systems generate new coins by solving difficult problems, to create blocks. Examples of mining-based Altcoins are **Litecoin**, **Monero**, and **Zcash**. Most of the top altcoins in early 2020 fell into the mining-based category. The alternative to mining-based altcoins is pre-mined coins. Such coins are not produced through an algorithm but are distributed before they are listed in cryptocurrency markets. An example of a pre-mined coin is **Ripple's XRP**.

Stablecoins

Cryptocurrency trading and use have been marked by volatility since launch. Stablecoins aim to reduce this overall volatility by pegging their value to a basket of goods, such as fiat currencies, precious metals, or other cryptocurrencies. The basket is meant to act as a reserve to redeem holders if the cryptocurrency fails or faces problems. Price fluctuations for stablecoins are not meant to exceed a narrow range.

Social media behemoth Facebook's (FB) Diem is the best known stablecoin. It is a dollar-backed coin. Other examples of stablecoins are **USDC** based on the US dollar and **MakerDAO.**

Security Tokens

Security tokens are like securities traded in stock markets except they have a digital provenance. Security tokens resemble traditional stocks, and they often promise equity, in the form of ownership, or a dividend payout to holders. The prospect of price appreciation for such tokens is a major draw for investors to put money into them. Security tokens are generally offered to investors through **initial coin offerings**, or **ICOs**.

Utility Tokens

Utility tokens are used to provide services within a network. For example, they might be used to purchase services or redeem rewards. Unlike security tokens, utility tokens do not pay out dividends or part with an ownership stake. **Filecoin**, which is used to purchase storage space on a network, is an example of a utility token.

The market for altcoins is nascent. It is an unequal pairing. The number of altcoins listed in cryptocurrency markets has rapidly multiplied in the last decade and attracted hordes of retail investors, feverishly betting on their price movements to amass short-term profits. But such investors do not have the capital necessary to generate sufficient market liquidity.

Thin markets and an absence of regulation produces quicksilver volatility in altcoin valuations.

Consider the case of Ethereum's ether, which reached a peak of $1299.95 on Jan 12, 2018. Less than a month later, it was down to $597.36 and by the year's end, ether's price had crashed to $89.52, or down by 93%. The altcoin reached record prices of above $3,000 three years later. Timed trades can provide a wealth of profits for traders.

But there is a problem. Cryptocurrency markets are not yet mature. Despite several attempts, there are no defined investment criteria or metrics to evaluate cryptocurrencies. For the most part, the altcoin market is driven by speculation. Several cases of dead cryptocurrencies, those which failed to gain enough traction or simply vanished after collecting investors' money, exist.

Therefore, the altcoin market is for investors willing to take on the outsized risk of operating in an unregulated and emerging market that is prone to volatility. They should also be able to handle stress resulting from wild price swings. For such investors, cryptocurrency markets offer great returns.

There are obvious pros and cons to altcoins. The pros include:

- Altcoins are “better versions” of Bitcoin because they aim to plug the cryptocurrency’s shortcomings.
- Altcoins like stablecoins can potentially fulfill Bitcoin’s original promise of a medium for daily transactions.
- Certain altcoins, such as Ethereum’s **ether** and Ripple’s **XRP**, have already gained traction among mainstream institutions, resulting in high valuations.
- Investors can choose from a wide variety of altcoins that perform different functions in the crypto economy.

The cons include:

- Altcoins have a smaller investment market compared to Bitcoin. As of April 2021, Bitcoin has a 60% share of the overall cryptocurrency market.
- The absence of regulation and defined criteria for investment means that the altcoin market is characterized by fewer investors and thin liquidity. As a result, their prices are more volatile as compared to Bitcoin.
- It is not always easy to distinguish between different altcoins and their respective use cases, making investing decisions even more difficult and confusing.
- There are several “dead” altcoins that ended up sinking investor dollars, possibly as much as 60% of those ever issued.

The earliest notable altcoin, Namecoin, was based on the Bitcoin code and used the same proof-of-work algorithm. Like Bitcoin, Namecoin is limited to 21 million coins. Introduced in April 2011, Namecoin primarily diverged from Bitcoin by making user domains less visible. Namecoin allowed users to register and mine using their own bit domains, which was intended to increase anonymity and censorship resistance.

Introduced in October 2011, **Litecoin** was branded as the "silver to Bitcoin's gold." While fundamentally similar in code and functionality to Bitcoin, Litecoin differs from Bitcoin in several essential ways. It allows mining transactions to be approved more frequently. It also provides for a total of 84 million coins to be created—exactly four times Bitcoin's 21-million-coin limit.

Discussions about the future for altcoins and, indeed, cryptocurrencies, have a precedent in the circumstances that led to the issue of a federally issued dollar in the 19th century, known as the “greenback.”. Back then, there were various forms and types of local currencies circulating in the United States, with each state issuing its own. Each had unique characteristics and was backed by a different instrument. For example, **Gold Certificates** were backed by deposits of gold at the

Treasury. US notes, which were used to finance the Civil War, were backed by the government.

Local banks were also issuing their own currency, in some cases backed by fictitious reserves. That multiplicity of currencies and financial instruments parallels the current situation in altcoin markets. There are thousands of altcoins available in the markets today, each one claiming to serve a different purpose and market.

The current situation in the altcoin markets is unlikely to consolidate into a single cryptocurrency. But it is also likely that a majority of the more than 2,000 altcoins listed in crypto markets will not survive. The altcoin market will coalesce around a bunch of altcoins, those with strong utility and use cases, which will dominate the markets.

For investors looking to diversify within crypto markets, altcoins are an inexpensive way to expand their horizons beyond Bitcoin. Rallies in cryptocurrency markets have produced returns that are multiples of those produced by Bitcoin. But there are risks involved in altcoin investing, not least of which is the absence of regulation. The maturation of cryptocurrency markets will likely bring more sophistication and capital into the industry, paving the way for regulation and less volatility.

Altcoins are good alternatives to cryptocurrency market investors interested in diversifying their portfolio. While some, like Ethereum's ether, are recognizable by name, a majority of the almost 9,000 altcoins are still to make a mark. Altcoins are representative of the potential for cryptocurrencies to reshape modern finance. But investors should do their research before investing in them. The risks associated with altcoins are similar or, in some cases, greater than those for Bitcoin investing.

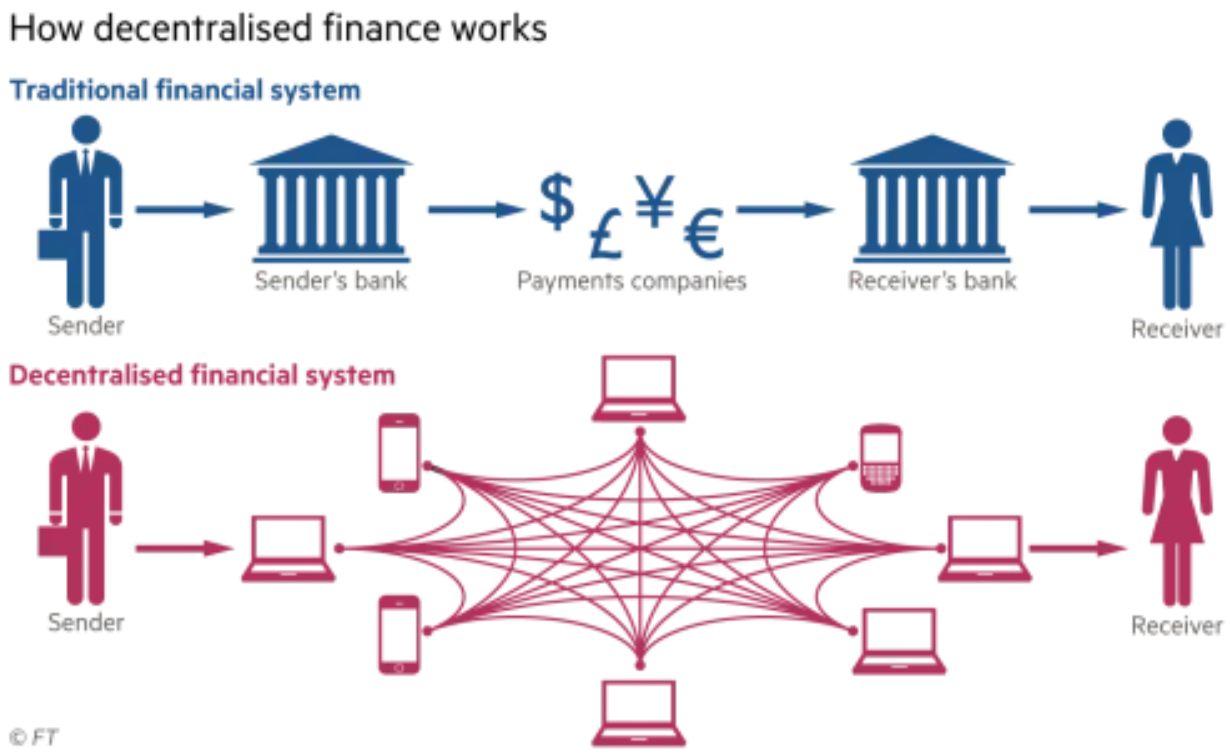
Chapter 14: Decentralized Exchanges

A decentralized exchange (better known as a DEX) is a peer-to-peer marketplace where transactions occur directly between crypto traders.

DEXs fulfill one of crypto's core possibilities: fostering financial transactions that aren't officiated by banks, brokers, payment processors, or any other kind of intermediary. The most popular DEXs — like **Uniswap** and **Sushiswap** — utilize the Ethereum blockchain and are part of the growing suite of Decentralized Finance (DeFi) tools, which make a huge range of financial services available directly from a compatible crypto wallet.

DEXs are booming. In the first quarter of 2021, $217 billion in transactions flowed through decentralized exchanges. As of April 2021, there were more than two million DeFi traders, a ten-fold increase from May 2020.

How do DEXs work? Unlike centralized exchanges like Coinbase, DEXs don't allow for exchanges between fiat and crypto — instead, they exclusively trade cryptocurrency tokens for other cryptocurrency tokens. Via a centralized exchange (or CEX), you can trade fiat for crypto (and vice versa) or crypto-crypto pairs — say some of your bitcoin for ETH.



You can also often make more advanced moves, like margin trades or setting limit orders. But all these transactions are handled by the exchange itself via an "order book" that establishes the price for a particular cryptocurrency based on current buy and sell orders — the same method used by stock exchanges like Nasdaq.

Decentralized exchanges, on the other hand, are simply a set of smart contracts. They establish the prices of various cryptocurrencies against each algorithmically and use "liquidity pools" — in which investors lock funds in exchange for interest-like rewards — to facilitate trades.

While transactions on a centralized exchange are recorded on that exchange's internal database, DEX transactions are settled directly on the blockchain.

DEXs are usually built on open-source code, meaning that anyone interested can see exactly how they work. That also means that developers can adapt existing code to create new competing projects — which is how Uniswap's code has been adapted by an entire host of DEXs with "swap" in their names like **Sushiswap** and **Pancakeswap**.

What are potential benefits of using a DEX? There is a vast variety. If you're interested in finding a hot token in its infancy, DeFi is the place to be. DEXs offer a virtually limitless range of tokens, from the well-known to the weird and totally random. That's because anyone can mint an Ethereum-based token and create a liquidity pool for it, so you'll find a greater array of projects, both vetted and unvetted. (Buyer beware!)

Hacking risks can be reduced: Because all the funds in a DEX trade are stored in the traders' own wallets, they are theoretically less susceptible to a hack. DEXs also reduce what is known as "counterparty risk," which is the likelihood that one of the involved parties — including potentially the central authority in a non-DeFi transaction — will default.

Anonymity. No personal information is required to use most popular DEXs.

Utility in the developing world: The peer-to-peer lending, speedy transactions, and anonymity made possible by DEXs have made them increasingly popular in developing economies — where solid banking infrastructure might not be available. Anyone with a smartphone and an internet connection can trade via a DEX.

What are some potential downsides? Trickier user interfaces navigating decentralized exchanges requires some specialized knowledge and the interfaces aren't always easy — be prepared to do a lot of research and don't expect the DEX itself to offer much handholding. You'll generally have to look offsite for a

walk-through or explainer.

Caution is required because it's possible to make an unfixable error, like sending coins to the wrong wallet. Another common issue is known as "impermanent loss," which can result from pairing a more volatile cryptocurrency with a less volatile one in a liquidity pool. The main takeaway here? Do your own research.

Smart contract vulnerability. Any DeFi protocol is only as secure as the smart contracts that power it — and code can have exploitable bugs (despite lengthy testing) that can result in the loss of your tokens. And while a smart contract might work as intended under normal circumstances, not all rare events, human factors, and hacks can be anticipated by developers.

Riskier coins with the unvetted, vast array of tokens available on most DEXs, there are also a greater number of scams and schemes to be wary of. A token that's on a hot streak could suddenly be "rug pulled," when its creator mints a bunch of new tokens, overwhelming the liquidity pool and tanking the value of the coin.

Before you buy a new-to-you cryptocurrency or experiment with a new protocol it's important to learn as much as you can — read white papers, visit developer Twitter feeds, or Discord channels, and look for audits of any particular project you're interested in (some bigger **auditors** include **Certik**, **Consensys**, **Chain Security**, and **Trail of Bits**).

How do you interact with a DEX? You can connect to a DEX like Uniswap using a crypto wallet such as **Metamask** (for your web browser) or Coinbase Wallet (for mobile).

While you can interact with DEXs directly from the browser built into Coinbase Wallet, an easier way is to pull up the website on your computer's web browser (in the case of Uniswap, the address is app.uniswap.org) and click "Connect to a Wallet."

A QR code should pop up, which you can scan with your phone's camera (tap the upper-right corner of the Coinbase Wallet app to access the camera). Once scanned, your wallet will be connected to the DEX.

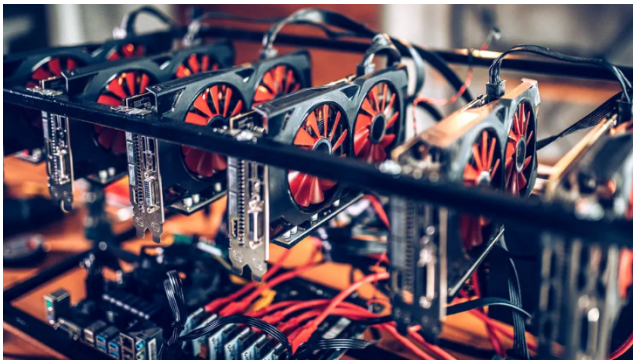
You'll also need a supply of Ethereum to start trading on most DEXs, which you can get from an exchange like Coinbase. The reason you need some ETH is for paying fees (known as gas) that are required for any transaction that happens on the Ethereum blockchain. These are separate from the fees the DEX itself charges.

How do DEX fees work? Fees vary. Uniswap charges a 0.3% fee that is split between liquidity providers, and a protocol fee could be added in the future. But

it’s important to note that the fees the DEX charges can be dwarfed by gas fees to use the Ethereum network. The ongoing ETH2 upgrade (as well as several “layer 2” solutions like **Optimism** and **Polygon**) are designed in part to lower fees and speed up transactions.

Chapter 15: How to Mine

What Is Bitcoin Mining?



Bitcoin mining is the way in which new coins are added to the existing supply of the cryptocurrency like Bitcoin (BTC), Ethereum, and Cardano.

These transactions are confirmed by the network and represent a critical component of the maintenance and development of the blockchain ledger.

Cryptocurrency mining is attractive to many investors interested in cryptocurrency and the most profitable can do it on a large scale incorporating an industrial mindset.

How Do I Mine Bitcoin?

Mining Bitcoin is not for the faint of heart. Your computer must solve complicated math problems that verify transactions in the currency. When a Bitcoin is successfully mined — the miner receives Bitcoin as payment.

In the beginning, one could use a normal computer that has a CPU, motherboard, RAM, and storage to mine Bitcoin. The only difference and the most important requirement here is the graphics processing unit (GPU) or the video card. A high-performance GPU is a must if a person wants to mine Bitcoin.

Bitcoin mining is done using hardware called ASICs that is short for Application-Specific Integrated Circuits. Another obligatory requirement is electricity for mining machines. The largest Bitcoin miners are usually found in countries with low-cost electricity. Miners need robust infrastructure to mine mainly energy and equipment.

How do I Mine at Home?

A company called **Compass Mining** is betting that individuals will want to partake in Bitcoin mining. There's a lucrative payout — if you're lucky enough to mine a coin. But the hassle of operating a mining rig can certainly cut into profits.

Compass Mining's new retail program will allow purchase of a single application-specific integrated circuit **(ASIC)** mining rig that they can set up at home.

Mining corporations usually buy in bulk — this finally gives the little guy a chance. Brands include top of the line ASICs **WhatsMiner** series from **MicroBT** and the **Antminer** series from **Bitmain**, offering 78 to 95 terahashes per second and ranging in price from $8,100 to $10,400.

Profitability calculators can help you estimate your potential ROI. Rigs are noisy and hot so it's not for everyone. Potential miners really need to do their due diligence if they want that sort of environment in their house.

About the size of a desktop computer tower, they can emit between 50 and 75 decibels of noise, which is roughly the same level as a vacuum cleaner or a hairdryer.

Just like the work-from-home paradigm was borne out of the pandemic, many who want to mine Bitcoin, wish to do it from the confines of their couch and man cave.

The demand for mining hosting sites in North America has been outstripping supply. Encouraging Bitcoin enthusiasts to set up their own operations at home is one way to relieve the pressure on existing hosting infrastructures.

China has now initiated a blanket ban on crypto currencies, opening opportunities for alternative miners before these Chinese mining operations relocate abroad. The crackdown nearly halved the mining difficulty for the entire Bitcoin network. Miners outside China have been able to mine more Bitcoin given the record low mining difficulty, raking in high revenue.

Corporate self-mining companies, such as **Marathon** and **Riot**, as well as third-party hosting sites, are facing a shortage of infrastructure to support more mining operations. Higher Bitcoin prices also mean more incentive for potential miners to flood this industry.

If Compass doesn't seem right for you, then buying mining machines either from Chinese miners or from mining machine manufacturers through e-commerce platforms such as Alibaba (BABA) and eBay (EBAY) could be a great option.

Individual mining rigs from Compass Mining are expected to deliver very soon.

Chapter 16: Tokens

Technically, a “token” is just another word for “cryptocurrency” or “cryptoasset.” But increasingly it has taken on a couple of more specific meanings depending on context.

The first is to describe all cryptocurrencies besides Bitcoin and Ethereum (even though they are technically also tokens). The second is to describe certain digital assets that run on top of other cryptocurrencies’ blockchain, as many decentralized finance (or DeFi) tokens do.

Tokens have a huge range of potential functions, from helping make decentralized exchanges possible to selling rare items in video games. But they can all be traded or held like any other cryptocurrency.

“Token” is a word that you hear a lot about with cryptocurrency. In fact, you might hear Bitcoin described as a “crypto token” or something similar, because — technically — all cryptoassets can also be described as tokens. But the word has increasingly taken on two specific meanings that are common enough that there’s a good chance you’ll encounter them.

The other increasingly common meaning for “token” has an even more specific connotation, which is to describe cryptoassets that run on top of another cryptocurrency’s blockchain. You’ll encounter this usage if you become interested in decentralized finance (or DeFi).

While a cryptocurrency like Bitcoin has its own dedicated blockchain, DeFi tokens like **Chainlink** and **Aave** run on top of, or leverage, an existing blockchain, most commonly Ethereum’s. Tokens in this second category help decentralized applications to do everything from automate interest rates to sell virtual real estate. But they can also be held or traded like any other cryptocurrency.

Why are tokens important? Given that you’ll come across the word a lot while researching cryptocurrencies, it’s useful to understand some common connotations. But besides the big-picture definitions in the section above, there are also some categories of crypto assets that have “token” in their name. Here are a few examples of those:

- DeFi tokens: A new world of cryptocurrency-based protocols that aim to reproduce traditional financial-system functions (lending and saving, insurance, trading) has emerged in recent years. These protocols issue tokens that perform a wide variety of functions but can also be traded or held like any other cryptocurrency.

- Governance tokens: These are specialized DeFi tokens that give holders a say in the future of a protocol or app, which (being decentralized) don't have boards of directors or any other central authority. The popular savings protocol **Compound**, for example, issues all users a token called **COMP**. This token gives holders a vote in how Compound is upgraded. The more **COMP** tokens you have, the more votes you get.

- Non-Fungible Tokens: (NFTs) NFTs represent ownership rights to a unique digital or real-world asset. They can be used to make it more difficult for digital creations to be copied and shared (an issue anyone who has ever visited a **Torrent** site full of the latest movies and video games understands). They've also been used to issue a limited number of digital artworks or sell unique virtual assets like rare items in a video game.

- Security tokens: Security tokens are a new class of assets that aim to be the crypto equivalent of traditional securities like stocks and bonds. Their main use case is to sell shares in a company (very much like the shares or fractional shares sold via conventional markets) or other enterprises (for instance, real estate) without the need for a broker. Major companies and startups have been reported to be investigating security tokens as a potential alternative to other methods of fundraising.

Chapter 17: Non-Fungible Tokens

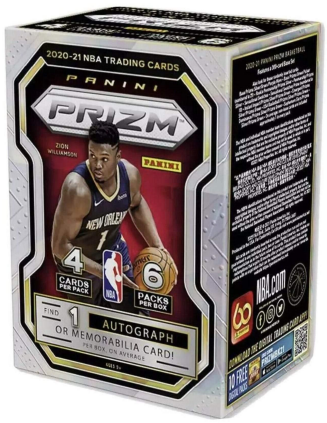
NFTs (or “non-fungible tokens”) are a special kind of crypto asset in which each token is unique — as opposed to “fungible” assets like Bitcoin and dollar bills, which are all worth the same amount.

Because every NFT is unique, they can be used to authenticate ownership of digital assets like artworks, recordings, and virtual real estate or pets.

In February 2021, a 10-second video by an artist named Beeple sold online for $6.6 million. Around the same time, Christie’s announced that it would be selling a collage of 5,000 “all-digital” works by the Wisconsin based artist, whose real name is Mike Winkelmann. It was put on a virtual auction block with a starting price of $100 — and on March 11 it sold for a staggering $69 million.

Beyond the high prices, there was one other fact that observers found fascinating. In exchange for their money, collectors who buy Beeples don’t receive any physical manifestation of the artwork. Not even a framed print. What they do get is an increasingly popular kind of crypto asset called an NFT — short for non-fungible token.

Each Beeple piece is paired with a unique NFT — a token attesting that each owner’s version is the real one. “We are in a very unknown territory,” said Christie’s contemporary art specialist Noah Davis. “In the first 10 minutes of bidding we had more than a hundred bids from 21 bidders, and we were at a million dollars.”



Why are NFTs important? You can think of NFTs as being kind of like certificates of authenticity for digital artifacts. They’re currently being used to sell a huge range of virtual collectibles, including:

- NBA virtual trading cards
- Music and video clips from EDM stars like Deadmau5
- Video art by Grimes
- The original “nyan cat” meme
- A tweet by Dallas Mavericks owner and entrepreneur Mark Cuban
- Virtual real estate in a place called Decentraland


Nyan Cat

As Bitcoin and other crypto has boomed in popularity over the last year, NFTs have also soared, growing to an estimated $2.5 billion during the first half of 2021. Each NFT is stored on

an open blockchain, often Ethereum's, and anyone interested can track them as they're created, sold, and resold.

Because they use smart contract technology, NFTs can be set up so that the original artist continues to earn a percentage of all subsequent sales.

Along the way, NFTs have raised fascinating philosophical questions about the nature of ownership. Wondering why digital artifacts that can be endlessly copied and pasted have any value at all?

Proponents would point out that most kinds of collecting aren't based on inherent value. Old comic books were produced for pennies' worth of ink and paper. Rare sneakers are often made from the same materials as worthless ones. Some paintings hang in the Louvre, others end up in thrift shops.

As the collector who sold the $6.6 million Beeple piece noted, you can take a nice picture of the Mona Lisa, but it's not the Mona Lisa. "It doesn't have any value because it doesn't have the provenance or the history of the work." "The reality here is that this is very, very valuable because of who is behind it."

What does "non-fungible" mean? Every Bitcoin is worth as much as every other Bitcoin. NFTs, on the other hand, are all unique. "Fungibility" refers to goods or assets that are all the same and can be swapped interchangeably. A dollar bill is another perfect example — each is worth exactly one dollar.

Concert tickets, by contrast, are non-fungible. Even if every Radiohead ticket is the same price, they aren't directly exchangeable. Each represents a specific seat and a specific date — no other ticket will have those exact characteristics.

Where do you buy or sell NFTs? Digital-artwork NFTs are mostly sold on specialized marketplaces like **Zora**, **Rarible**, and **Opensea**. If you're more interested in games and sports collectibles, developers like **Dapper Labs** have created experiences including NBA Top Shot (virtual trading cards) and **Cryptokitties** (a Pokemon-ish digital-cat collecting app that was the first NFT hit in late-2017).

Online games including **Gods Unchained** are starting to use NFTs to sell in-game assets like weapons or cosmetic upgrades. Real estate in new virtual worlds is sold via markets including **Decentraland** and The Sandbox. You can also buy or sell some NFTs directly via a compatible crypto wallet.

How do NFTs work? If you're interested in DeFi, you might have heard of the **ERC-20 standard**, which allows anyone to create a token compatible with the Ethereum blockchain. Those are "fungible" tokens. Most non-fungible tokens are built using the ERC-721 and ERC-1155 standards, which allow creators to issue unique crypto assets via smart contract.

Because each NFT is stored on a blockchain, there is an immutable record starting with the token's creation and including every sale. (Some NFT-focused developers have also built their own alternative blockchains, including Dapper Lab's **Flow**.)

What can you do with NFTs once you buy them? Good question! Some people display their digital artworks on large monitors. Some buy virtual real estate (via NFT, of course) in which they're able to build virtual galleries or museums. You can also roam virtual worlds like Decentraland and check out other people's collections.

For some fans, the appeal is in the buying and selling — much like any other asset class. (The collector who sold the $6.9 million Beeple paid less than $70,000 for it in October 2020).

More and more mainstream artists have also gotten involved in the space — especially from the world of music. In early March, the Nashville band ***Kings of Leon*** announced their next album would arrive in the form of multiple NFTs. Depending on which a fan buys, various perks will be unlocked — like alternate cover art, limited-edition vinyl, and even a "golden ticket" to a VIP concert experience.

Kings of Leon


QUEEN
of the
SHORT
LINES
R.R.

Chapter 18: Smart Contracts

A smart contract, like any contract, establishes the terms of an agreement. But unlike a traditional contract, a smart contract's terms are executed as code running on a blockchain like Ethereum.

Smart contracts allow developers to build apps that take advantage of blockchain security, reliability, and accessibility while offering sophisticated peer-to-peer functionality — everything from loans and insurance to logistics and gaming.

Just like any contract, smart contracts lay out the terms of an agreement or deal. What makes smart contracts "smart," however, is that the terms are established and executed as code running on a blockchain, rather than on paper sitting on a lawyer's desk.

Smart contracts expand on the basic idea behind Bitcoin — sending and receiving money without a "trusted intermediary" like a bank in the middle — to make it possible to securely automate and decentralize virtually any kind of deal or transaction, no matter how complex. And because they run on a blockchain like Ethereum, they offer security, reliability, and borderless accessibility.

Why are smart contracts important? Smart contracts allow developers to build a wide variety of decentralized apps and tokens. They're used in everything from new financial tools to logistics and game experiences, and they're stored on a blockchain like any other crypto transaction. Once a smart-contract app has been added to the blockchain, it generally can't be reversed or changed.

Smart-contract-powered apps are often referred to **as "decentralized applications"** or **"dapps"** – and they include decentralized finance (or DeFi) tech that aims to transform the banking industry. DeFi apps allow cryptocurrency holders to engage in complex financial transactions — saving, loans, insurance — without a bank or other financial institution taking a cut and from anywhere in the world. Some of the more popular current smart contract powered applications include:

- Uniswap: A decentralized exchange that allows users, via smart contract, to trade certain kinds of crypto without any central authority setting the exchange rates.

- Compound: A platform that uses smart contracts to let investors earn interest and borrowers to instantly get a loan without the need for a bank in the middle.

- USDC: A cryptocurrency that is pegged via smart contract to the US dollar, making one USDC worth one U.S. dollar. UDDC is part of a newer category of digital money known as stablecoins.

So how would you use these smart contract-powered tools? Imagine you're holding some Ethereum that you'd like to trade for USDC. You could put some Ethereum into Uniswap, which, via smart contract, can automatically find you the best exchange rate, make the trade, and send you your USDC. You could then put some of your USDC into Compound to lend to others and receive an algorithmically determined rate of interest — all without using a bank or other financial institution.

In traditional finance, swapping currencies is expensive and time consuming. And it isn't easy or secure for individuals to loan out their liquid assets to strangers on the other side of the world. But smart contracts make both of those scenarios, and a vast variety of others, possible.

How do smart contracts work? Smart contracts were first proposed in the 1990s by a computer scientist and lawyer named **Nick Szabo**. Szabo famously compared a smart contract to a vending machine. Imagine a machine that sells cans of soda for a quarter. If you put a dollar into the machine and select a soda, the machine is hardwired to either produce your drink and 75 cents in change, or (if your choice is sold out) to prompt you to make another selection or get your dollar back.

This is an example of a simple smart contract. Just like a soda machine can automate a sale without a human intermediary, smart contracts can automate virtually any kind of exchange.

Currently, Ethereum is the most popular smart contract platform, but many other cryptocurrency blockchains (including EOS, Neo, Tezos, Tron, Polkadot, and Algorand) can run them. A smart contract can be created and deployed to a blockchain by anyone. Their code is transparent and publicly verifiable, which means that any interested party can see exactly what logic a smart contract follows when it receives digital assets.

Smart contracts are written in a variety of programming languages (including Solidity, Web Assembly, and Michelson). On the Ethereum network, each smart contract's code is stored on the blockchain, allowing any interested party to inspect the contract's code and current state to verify its functionality.

Each computer on the network (or "node") stores a copy of all existing smart contracts and their current state alongside the blockchain and transaction data.

When a smart contract receives funds from a user, its code is executed by all nodes in the network to reach a consensus about the outcome and resulting flow of value. This is what allows smart contracts to securely run without any central authority, even when users are making complex financial transactions with unknown entities.

To execute a smart contract on the Ethereum network, you will generally have to pay a fee called "gas" (so named because these fees keep the blockchain running).

Once deployed onto a blockchain, smart contracts generally can't be altered, even by their creator. (There are exceptions to this rule.) This helps ensure that they can't be censored or shut down.

In the White House

Chapter 19: Security

As crypto trading becomes increasingly mainstream; security teams everywhere have seen cybercriminals getting even more creative and persistent in their attempts to steal assets. Quite simply, the greater the value of the object, the greater the attempts to steal it.

While that can sound a little scary at first, the good news is that you can dramatically improve your digital security with just a few easy steps. Not only can you protect your funds, but it can also be applied to the rest of your digital life as well!

When someone is able to log into one of your accounts to perform fraudulent activity, this is called an **"account takeover",** or **"ATO"** for short. But how do these fraudsters get into your account in the first place?

One common method is called a **"SIM-swap."** In a SIM-swap attack, fraudsters will contact your wireless carrier pretending to be you and persuade the customer service agent to redirect your cell service to a different device, by changing the SIM card number associated with your account (hence the name of the attack.)

Once they succeed, they are able to receive all calls and SMS messages sent to your phone number — including any two-factor authentication codes sent to you via SMS. From there, fraudsters will frequently pair those SMS 2FA codes with stolen passwords to try and log into your email account, social media profiles, cloud storage accounts like Dropbox, or financial accounts.

Using SMS-based two-factor authentication (2FA) is better than using no 2FA at all. That said, I encourage everyone to follow the two simple steps below and apply them to all the accounts they care about.

Use a password manager

Your passwords should be at least 16 characters, extremely complex and unique for your accounts. Birthdays don't work anymore. That's hard to do by yourself, but password managers like **1Password** or **Dashlane** can be used to create and remember your passwords.

Are you currently using a password that has been exposed in a third-party data breach somewhere? You can check to see if you're using a risky password by visiting haveibeenpwned.com/Passwords.

Use 2-factor authentication (2FA)

In addition to strong passwords, where available, use two-factor authentication (2FA). And always use the strongest type of 2FA the platform allows, ideally a **Yubikey** or similar hardware security key. If a service provider doesn't allow Yubikey, use an authentication app like Google Authenticator or Duo Security instead of SMS-based 2FA if possible.

If SMS-based 2FA is the only thing available, at the very least require a one-time 2FA code to be sent to your device every time you login — so someone can't access your account if they have stolen your password.

If an organization doesn't offer any of these options, consider not using that service.

Stay smart out there. It's not only important to play defense with the right security tools when protecting your accounts, but it's also important to stay vigilant in the wild. Here are some guidelines:

- Don't make yourself a target
- Don't brag about your cryptocurrency holdings online, just like you wouldn't advertise inheriting a billion dollars.
- Review your online presence with this easy self-assessment.
- Don't fall for tricks. Hackers posing as tech support — even bad actors posing as customer support specifically — may pressure you for account credentials. Any respectable organization will never ask you for passwords, 2FA codes, PIN numbers or for remote access to your computer. They will never ask you to create test accounts on other platforms or provide your ID or banking information over email or social media.
- Remember, Microsoft, Google, and Apple will never call you about your computer.
- Check the URL. Scammers create fake sites that look like real exchanges but are designed to steal account information. Double check the web address before you login into your account or input any of your credentials.


WARNING
UNDER TEXAS LAW (CHAPTER 87, CIVIL PRACTICE AND REMEDIES CODE), A FARM ANIMAL PROFESSIONAL IS NOT LIABLE FOR AN INJURY TO OR THE DEATH OF A PARTICIPANT IN FARM ANIMAL ACTIVITIES RESULTING FROM THE INHERENT RISKS OF FARM ANIMAL ACTIVITIES.

Chapter 20: Sending Crypto to Your Friends

Sending crypto to friends and family, and using crypto to pay for goods and services, is easy once you get the hang of it.

Why would you want to send crypto instead of cash? Since crypto is digital, sending crypto can be as easy as sending an email. Crypto also doesn't have any physical borders the way dollars, pesos, or euros do, so you can send crypto to friends, family, or merchants overseas as easily as sending it to someone sitting next to you.

Lastly, you can send crypto without sharing your personal or banking info, making it more secure.

To send crypto, you'll need the recipient's wallet address. A wallet address is a long string of characters, like a bank account number, that identifies where the crypto should go. Since crypto wallet addresses are long, they're often shown as a **QR code** that you can scan in your crypto app.

Once you have the wallet address, you just need to open your crypto wallet, enter the wallet address, select how much crypto you want to send, and you're done.

There's usually a small fee to send crypto, called the "gas fee", but this fee is often much lower than other methods like wire transfers or Western Union.

A few things to keep in mind when sending crypto:

- Each type of crypto has its own address, so make sure you're sending Bitcoin to a Bitcoin address, and Ethereum to an Ethereum address.

- Once your transaction is verified and confirmed, the crypto will show up in the recipient's account. This can take anywhere from a few seconds to a few minutes.

Chapter 21: Taxation

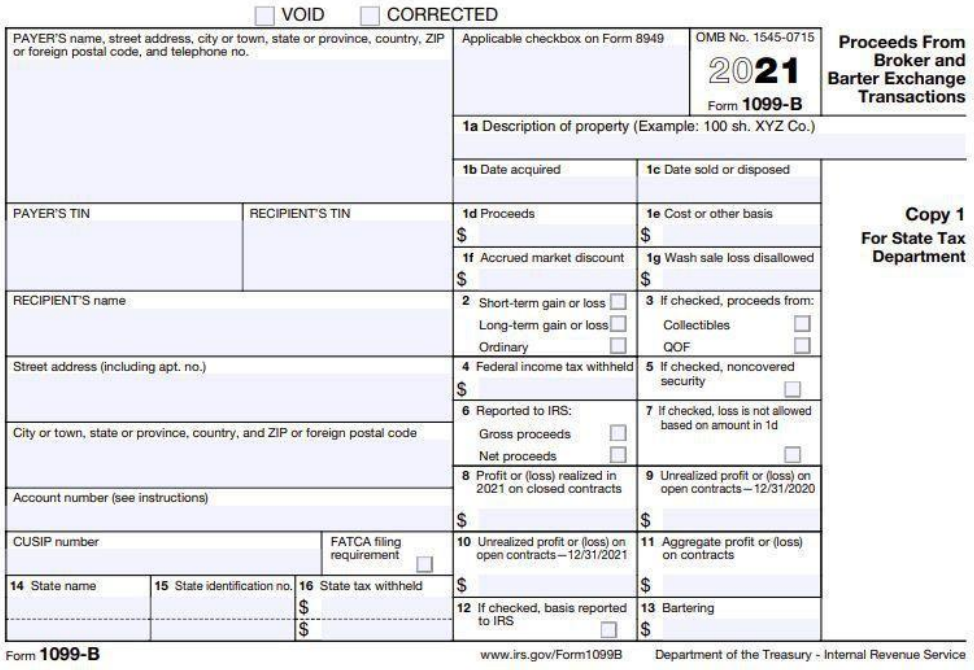
In the early days of Bitcoin it was widely assumed that all profits earned in the space were free money and tax free. Once the profits made topped billions of dollars, that did not turn out to be the case.

The American International Revenue Service (IRS) calculated that of the $2 trillion in total market capitalization, some $1 trillion is unreported or unrealized capital gain.

It gets even harder to make the tax-free argument in 2021 - crypto exchanges, brokers, and conventional banks and brokers are required to file Form 1099b's with the government. If your realized Bitcoin profits don't show up on your annual tax return on Schedule "B" you may have a problem.

The Form 1099b will show the amount of money received from the sale of crypto. It is up to you to document the cost basis and report the profit.

Under current tax law short term capital gains are treated as "ordinary income' and taxed at a maximum 37% rate. Long term gains, positions held for more than 12 months, are taxed at a lower 20% rate for profits up to $200,000. This may change as the current administration has targeted all tax rates for an increase.



☐ VOID ☐ CORRECTED

PAYER'S name, street address, city or town, state or province, country, ZIP or foreign postal code, and telephone no.	Applicable checkbox on Form 8949	OMB No. 1545-0715 2021 Form 1099-B	Proceeds From Broker and Barter Exchange Transactions
	1a Description of property (Example: 100 sh. XYZ Co.)		
	1b Date acquired	1c Date sold or disposed	
PAYER'S TIN / RECIPIENT'S TIN	1d Proceeds $	1e Cost or other basis $	Copy 1 For State Tax Department
	1f Accrued market discount $	1g Wash sale loss disallowed $	
RECIPIENT'S name	2 Short-term gain or loss ☐ Long-term gain or loss ☐ Ordinary ☐	3 If checked, proceeds from: Collectibles ☐ QOF ☐	
Street address (including apt. no.)	4 Federal income tax withheld $	5 If checked, noncovered security ☐	
City or town, state or province, country, and ZIP or foreign postal code	6 Reported to IRS: Gross proceeds ☐ Net proceeds ☐	7 If checked, loss is not allowed based on amount in 1d ☐	
Account number (see instructions)	8 Profit or (loss) realized in 2021 on closed contracts $	9 Unrealized profit or (loss) on open contracts – 12/31/2020 $	
CUSIP number / FATCA filing requirement ☐	10 Unrealized profit or (loss) on open contracts – 12/31/2021 $	11 Aggregate profit or (loss) on contracts $	
14 State name / 15 State identification no. / 16 State tax withheld $ $	12 If checked, basis reported to IRS ☐	13 Bartering $	

Form 1099-B www.irs.gov/Form1099B Department of the Treasury - Internal Revenue Service


NEW YORK ATHLETIC CLUB
PRIVATE
CLUB

Chapter 22: Bitcoin Myths

With Bitcoin attracting increasing amounts of attention every day, it seems like a good time to look at some of the biggest myths and misconceptions people tend to have about the world's first cryptocurrency, to see if they have any merit, and correct the record.

If you think, for instance, that Bitcoin's value is "based on nothing" or that it's too volatile to have any real-world use, this guide is for you. We're separating fact from fiction — without shying away from legitimate risks — to get to the truth about the world's most popular cryptocurrency.

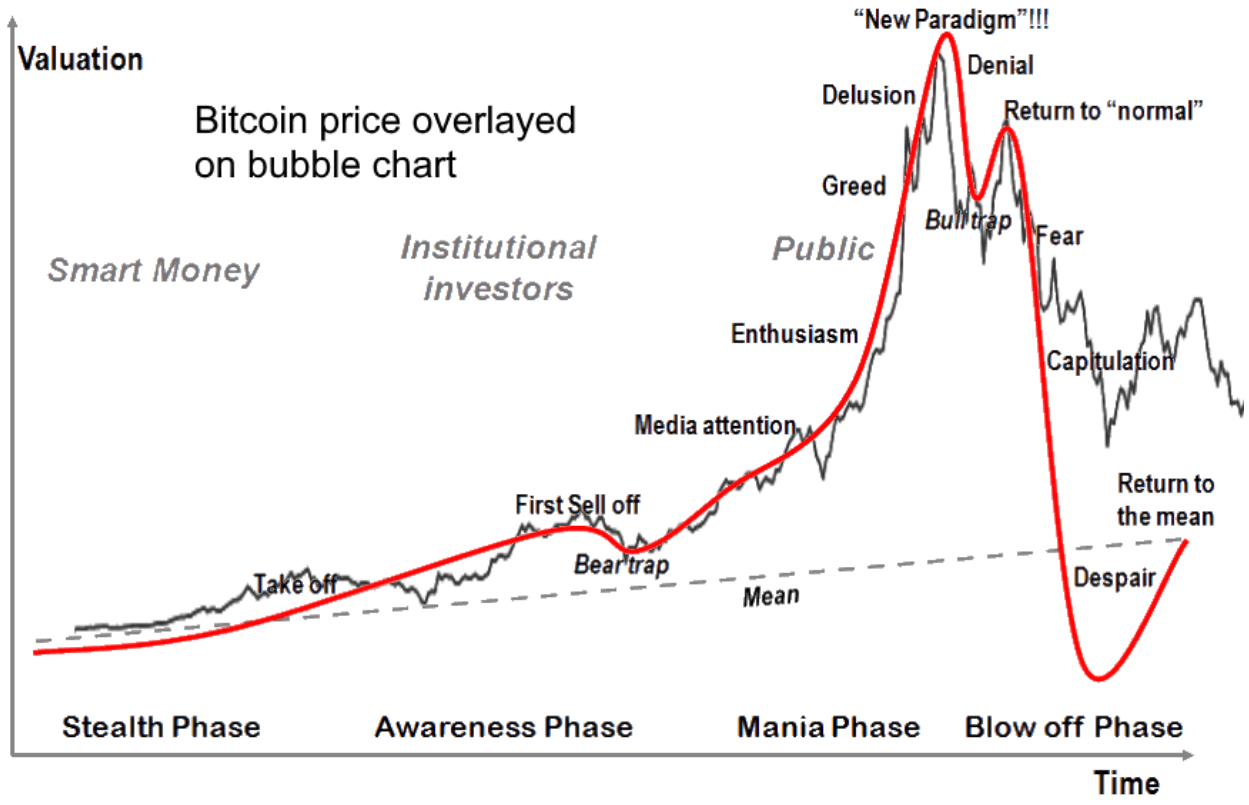
Myth #1: Bitcoin is a bubble

While it's true that some people buy Bitcoin as a speculative investment seeking big returns, that doesn't mean that Bitcoin itself is a bubble. Bubbles are economic cycles characterized by unsustainable rises in market value. They eventually pop when investors realize prices are much higher than an asset's fundamental value. Bitcoin is occasionally compared to an infamous early speculative bubble: the 17th century Dutch "tulip mania." In 1637, speculators caused prices for some tulip varieties to surge 26-fold. The bubble lasted six months, crashed, and never recovered.

The real story:

Bitcoin has gone through multiple price cycles over the course of over 12 years — and has recovered each time to achieve new highs. As with any new technology, boom and bust cycles are expected. For example, at the end of the dot.com era in the nineties, Amazon stock nosedived from around $100 to just $5, only to become one of the most valuable companies in the world in the subsequent decades.

Some major Bitcoin investors believe that Bitcoin's oscillations form a pattern typical of young markets. Bitcoin, they say, will surge and recede with smaller swings and longer durations between them until at some point in the future it settles into relative stability. But only time will tell.



Myth #2: Bitcoin has no real-world uses

Critics like to claim that Bitcoin isn't useful in the real world — or if it does have a use, it's mostly useful for illicit activity. Neither of those statements are true. Bitcoin has a long history as a means of making payments to anyone in the world, all without a bank or payment processor in the middle. And it is increasingly being used as a gold-like hedge against inflation by major institutional investors.

The real story:

In recent years, Bitcoin has become increasingly popular as an inflation-resistant store of value much like gold — leading to Bitcoin's "digital gold" nickname. A growing number of major funds and publicly traded companies (Tesla (TSLA), Square (SQ), MicroStrategy (MSTR)) have bought millions or even billions of dollars' worth of Bitcoin to better manage their assets.

Much like gold, Bitcoin is scarce (there will never be more than 21 million Bitcoin). Gold, of course, is heavy, bulky, and difficult to transport and store. Bitcoin, on the other hand, can be sent digitally as easily as sending an email.

Bitcoin received negative attention in early years as a means of payment on the dark web. But when the first big dark-web market was shuttered, Bitcoin prices appreciated after just a few days — and continued to rise.

Like any form of money, some of it will be misused. But compared to US dollars, illicit use of Bitcoin is a drop in the bucket. According to a recent report, 2.1% of Bitcoin transaction volume in 2019 was related to criminal enterprise. By comparison, 50% of dollar bills circulating in the US test positive for cocaine. The Federal Reserve believes that half of all dollar bills ever issued are held by foreigners outside the US largely for illegal purposes.

Because all Bitcoin transactions happen on an open blockchain, it's often easier for authorities to track illegal activity than it would be in the traditional financial system.

Myth #3: Bitcoin doesn't have real value

While Bitcoin might not be backed by a physical asset like gold, neither is the US dollar or virtually any other modern fiat currency. Bitcoin is hard coded to be scarce, which helps make it resistant to inflation. Inflation with fiat currencies can occur when large quantities are created, thus diluting the existing supply.

The real story:


F STREET RESTAURANT
1427 F STREET
Friday's Menu
Dinner, 65c
SERVED DAILY, 4 to 8 P.M.
Hot Biscuit
Cold Slaw
Clam Chowder
Choice
Cod Fish Cakes—Tomato Sauce
Hot or Cold Roast Beef au Jus
Fried Trout
Stuffed Shad
Haricot of Veal.
Veal Cutlet, Breaded, Tomato Sauce
Fried Sweet Potatoes
New Squash or Spring Egg Plant
Choice
Cake Ice Cream Pie
Coffee or Pot of Tea

Anyone who doesn't believe this should check out a 100-year-old restaurant menu to find coffee for 5 cents, a hamburger for 25 cents, and a steak for $1.00.

There will only ever be 21 million Bitcoins. This scarcity is a major driver of its value.

Not only is the supply capped, but the amount of new Bitcoin being mined is declining over time in a predictable way. Every four years, an event called a "halving" takes place where block rewards paid to miners in the network are cut in half. This helps ensure that the supply is always reducing which, by the basic economic principle of scarcity, has worked to keep the price of Bitcoin broadly trending upwards over the long-term — from less than a penny at the start to more than $66,000 as of February 2021.

Bitcoin also derives value from the work of computers on the network which contribute via a process called mining. Powerful computers all over the world

supply a vast amount of processing power towards the work of validating and securing every transaction. In exchange they're rewarded with new Bitcoin.

Myth #4: Bitcoin will just be replaced by a competitor

Bitcoin was the first successful digital money. And while new cryptocurrencies have long promised to overtake Bitcoin via new features or other advantages, none have come close.

The real story:

Though thousands of rival cryptocurrencies have been created over the past decade, Bitcoin has always been, and remains, the most valuable cryptocurrency by market capitalization by a significant margin. It's also the most popular, making up around 60% of the crypto market. Reasons include Bitcoin's "first-mover" advantage, along with the purity of its mission as a decentralized and open currency.

Which isn't to say that competitors aren't welcome to try. Bitcoin is decentralized, meaning it's operated by a global community of miners and nodes, instead of a central authority. For example, if Bitcoin's underlying architecture has to change in order to add new functionality, features, or to protect against a newly discovered bug, the community can initiate a "fork" to upgrade the network.

For the upgrade to be accepted, a 51% majority of the community must support the change. This allows Bitcoin to adapt and evolve as required, as seen with Bitcoin's Segregated Witness (SegWit) upgrade in 2017.

Because the software is open-source, developers who can't gain community consensus can even create a hard-fork of the Bitcoin blockchain and make an entirely new cryptocurrency. For instance, Bitcoin Cash was created this way — but so far, no Bitcoin clones have come anywhere close to replacing the original.

Of course, a huge amount of innovation is happening in the space, so it's conceivable that a bigger rival could emerge. But given current circumstances most experts don't think Bitcoin being replaced anytime soon, is a likely outcome.

Myth #5: Investing in Bitcoin is gambling

While it's true that Bitcoin has experienced significant price volatility over the last decade, that's to be expected of a young and growing market. Since Bitcoin's genesis block in 2010, it

has steadily gained long-term value — with a market cap exceeding $1 trillion as of February 2021. And as Bitcoin has continued to mature, a robust regulatory structure in countries around the world has helped to attract a wave of institutional investment (Tesla, hedge funds).

The whole story:

There is a fundamental rationale for a Bitcoin investor to believe that the value of their holdings should rise — whereas in a casino you know the odds are tilted in favor of the house. Of course, there is no guarantee about future performance or continued results, but Bitcoin's long term trendline over the last decade has been upward.

One popular investing strategy for reducing the impact of volatility is **dollar cost averaging**— in which you invest a fixed amount every week or month no matter what the market is doing. This strategy typically results in positive returns regardless of volatility in a positive trendline environment.

Bitcoin volatility appears to be on the decline. A recent Bloomberg analysis compared Bitcoin's recent bull run to the 2017 boom — and found that volatility is considerably lower this time around. Why? The rise of institutional participants and the general stabilizing effect of crypto "going mainstream."

Whether Bitcoin or any other cryptocurrency has a place in your investment portfolio depends on your personal circumstances, risk tolerance, and investment time horizon. And even though Bitcoin has trended steadily upwards over the past decade, it also has had substantial down cycles. Investors should be careful navigating volatile markets (and consider working with a financial advisor before making major investments).

Myth #6: Bitcoin isn't secure

The Bitcoin network has never been hacked. Its open-source code has been scrutinized by countless security experts and computer scientists. Bitcoin was also the first digital currency to solve **the double-spend problem**, making "trustless" peer-to-peer currencies a reality. Further, all Bitcoin transactions are irreversible.

The real story:

Many misconceptions around the security of Bitcoin stem from attacks on third-party businesses and services that make use of Bitcoin, and **not the Bitcoin network itself**. High-profile hacks of early Bitcoin companies with flawed security procedures (like the one that hit the early Japan-based exchange Mt. Gox) and occasional data breaches (like the one that impacted users of the wallet provider Ledger) have made some users question the security of Bitcoin.

Bitcoin's core protocol has functioned securely with 99.9% uptime since its creation in 2009.

A vast amount of computing power secures the network. And the miners that power the network are distributed throughout the world, with nodes in 100 countries — which means there are no single points of failure.

Myth #7: Bitcoin is bad for the environment

Bitcoin mining is an energy-intensive process. But determining the environmental impact is hard. For one thing, all aspects of the digital economy require energy. Consider the entire global banking system, and all the energy required to process bank transactions and power office buildings, ATMs, local branches, and much more.

The real story:

Recent research by New York-based fund Ark Investment Management concludes that "Bitcoin is much more efficient than traditional banking and gold mining on a global scale." A significant portion of Bitcoin mining is powered by renewable-energy sources (including wind, hydro, and solar). The actual number ranges from 20 percent to more than 70 percent, according to the Cambridge Bitcoin Electricity Consumption Index. The Cambridge researchers concluded: "Bitcoin's environmental footprint currently remains marginal at best."

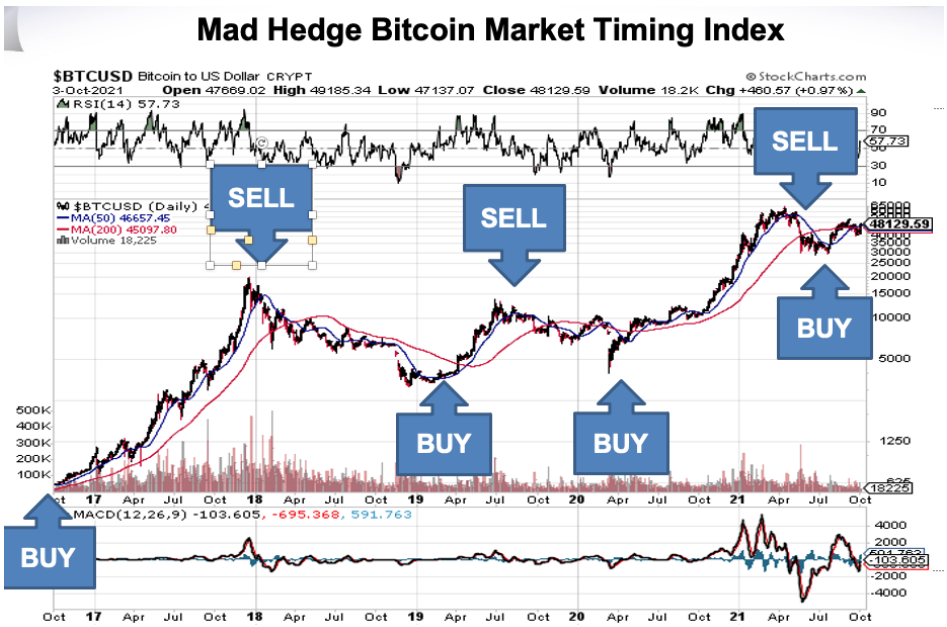
An argument can even be made that the economic incentives inherent to Bitcoin mining are helping drive sustainable energy innovation, as miners constantly seek to increase profits by lowering their electricity costs — in a world where renewable energy is fast becoming the cheapest option.

Chapter 23: The Mad Hedge Bitcoin Market Timing Index

It helps to have some state-of-the-art algorithms and strict quantitative discipline when trading in the modern era. A tool like the **Mad Hedge Market Timing Index** has proved wildly successful.

Bitcoin is no different. In fact, crypto currencies are particularly well suited for algorithmic trading. That's because they are completely transparent. Any miner can log into the network and see what other participants are doing. That means you can identify the whales and who has been making the most money and simply ride on their coattails.

This also means that technical analysis is much more important in trading crypto than with any other financial instruments. Available fundamentals outside the mining community are minimal. Charts are everything. When a multi month double bottom holds, you can take that to the bank.



Taking all these factors in mind I have created the **Mad Hedge Bitcoin Market Timing Index**. The index sends out "BUY" and "SELL" signals monthly. The index gives you the unfair advantage you need to succeed in this market. Included in the daily calculation of the index are:

traditional technical analysis, including moving averages and RSI's
flow of funds withing the crypto mining community
actions of the "whales"- 20% of Bitcoin is owned by the top 100 accounts
growth of the global money supply and other liquidity measures
action of other highly correlating assets

Chapter 24: Crypto Dictionary

If you've spent any time reading crypto Reddit or Twitter, there's a 100 percent chance you've encountered — and were potentially baffled – by a dense thicket of acronyms, misspelled words, gamer memes, and more. From FOMO and FUD to laser eyes and whales, get crypto literate with this beginner's guide to eleven of the most common pieces of slang.

Diamond hands

Or as Elon Musk put it in a May tweet: 💎🙌. Diamond hands is a meme popularized by crypto and stock traders on Reddit. It connotes a hardcore adherence to the HODL philosophy (see below) — and is often used by online groups that have banded together to try to drive up the price of a memecoin or another asset. (The related-but-derogatory term for skittish traders? "Paper hands"/🧻🤲.)

FOMO

Stands for "fear of missing out" — and is generally most intense when markets are rising fast. FOMO can lead to emotional trading and bad decision making — it's dangerous because hindsight is 20/20, making it all too easy to regret the gains you would have made if you had only timed all your trades perfectly.
(Nobody times all their trades perfectly.)

A good way to reduce FOMO is to have a strategy and stick to it, especially if you believe that the asset you're investing in will rise in value over the longer term. One popular option is dollar cost averaging (or DCA), in which you invest the same amount every week or month without worrying about what the market is doing.

FUD

Stands for "fear, uncertainty, and doubt." It's a classic public relations and propaganda tactic. The idea is to warp public perception about a product, technology, or candidate by strategically releasing misinformation designed to create a negative emotional response.

Mainframe-computer architect and entrepreneur Gene Amdahl is often credited with popularizing the term in the 1980s. He used it to describe the way IBM salespeople of the era worked to delegitimize competitors' products, painting them as unreliable and untrustworthy.

In the crypto space, FUD often refers to general skepticism around the technology (from the media or from traditional-finance analysts), but the idea can also be used by proponents of a specific token or protocol to disarm criticism.

What should you do when faced with FUD? Embrace another popular crypto acronym, and DYOR. Do your own research.

The Flippening

The Flippening is a hypothetical event in which Ethereum's market cap will one day eclipse Bitcoin's. It can also be used to describe any similar situation where a smaller or less-established token or protocol might overtake a larger rival.

HODL

HODL is probably the most prevalent piece of crypto slang. It originally came from a drunken typo in the subject line of a post "I AM HODLING". (It should have read "holding.") HODL — usually pronounced "hoddle" — simply means to buy and hold for the long term, no matter what the market is doing. Bitcoin fans have even retroactively turned it into an acronym that stands for "hold on for dear life."

The original forum post is riddled with typos, but the underlying message was prescient. At the time, Bitcoin's value had plummeted from $1242 to $480 in a month. Panicked traders were bailing out, but GameKyuuubi — real name Mike, a programmer — wasn't selling: "In a zero-sum game such as this," he wrote, "traders can only take your money if you sell."

The sentiment soon spread throughout the Bitcoin community and countless memes ensued. Crypto has experienced multiple bull and bear cycles, but so far at least, HODL has been good advice — with Bitcoin emerging as one of the best performing assets of the past decade. As mentioned in the FOMO entry above, one good way to HODL is via (DCA).

Laser Eyes

In 2021, avid Bitcoin proponents began signaling their support for the cryptocurrency by adding "laser eyes" to their Twitter photo. NFL superstar Tom Brady, Paris Hilton, Elon Musk, Wyoming senator Cynthia Lummis, and MicroStrategy CEO Michael Saylor are a few of the famous names who have taken part. The meme is often associated with the hashtag **#LaserRayUntil100K** — indicating support for the cryptocurrency's potential to break the $100,000 mark.

Memecoin

Dogecoin (DOGE) is the original memecoin — it's literally a cryptocurrency based on a meme that was popular at the time it was invented. But in 2021, when Dogecoin dramatically rose in value, a huge wave of other tokens with absurd names emerged (in part made possible by decentralized exchanges like Sushiswap, which allow anyone to easily list a token).

In May 2021, Ethereum cofounder Vitalik Buterin donated more than $1 billion in DOGE-inspired memecoins like AKITA, SHIB, and Dogelon Mars (ELON) towards COVID-relief efforts in India and other causes. The coins had been deposited in Buterin's crypto wallet to make traders believe he was an investor.

Moon (or mooning)

When a cryptocurrency is seeing strong upward momentum, traders tend to describe it as going "to the moon" or "mooning."

Pump and Dump

A coordinated effort to artificially inflate the price of an asset and cash out before it tumbles back to earth. Cryptocurrencies with smaller market caps are particularly vulnerable to pump and dump schemes. A group of traders will work together to drive up the price of a specific small-cap altcoin. As prices rise, the schemers will promote the opportunity on Twitter, Reddit, Discord, Facebook, YouTube comments, and elsewhere, attracting more investors and driving the price up further. When the asset hits their target value, the original group will cash out — taking big profits and leaving everyone else "holding the bag" as the token collapses.

Rekt

What happens if you get swept up by FOMO and end up becoming the victim of a pump and dump? You get rekt. Getting rekt in its original gaming context means to lose badly, and the definition is pretty much the same in crypto.

Whale

The biggest holders of crypto are known as whales. For Bitcoin, anyone with more than 1,000 BTC is generally considered a whale. Unlike most crypto traders, whales have the potential to move markets with their trades. As of mid-May 2021, the top 100 Bitcoin addresses (out of more than 800,000 active addresses) held more than 20 percent of all BTC according to www.bitinfocharts.com .

Chapter 25: Dictionary of Altcoins & DeFi Tokens

Whether you're just starting your crypto journey, or you've been trading Bitcoin for years, there's a good chance you've tried to dig into the world beyond Bitcoin and Ethereum only to find yourself confused by all the different cryptocurrencies out there.

After all, in the decade since Bitcoin began to catch on, thousands of alternatives have emerged — with an ever-growing selection. In the last few years, tokens that help power decentralized finance (or DeFi) protocols have become increasingly popular — and so several the cryptocurrencies on this list come from that world.

If you're ready to figure out the difference between XTZ and XLM, you've come to the right place. Here (presented in alphabetical order) is key information about some of the biggest and most important cryptocurrencies that aren't Bitcoin or Ethereum. Each of these "altcoins" (short for "alternative coins") is tradable via Coinbase and other major exchanges, and they all have unique features, goals, and use cases.

Aave (AAVE)

Released: November 2017

Aave is a decentralized lending protocol (part of the broader group of protocols known as DeFi) that allows users to deposit crypto assets to earn APY rewards, and to borrow other crypto assets against that collateral. It makes it possible for users to borrow, lend, and earn interest on their crypto — making use of smart contracts instead of intermediaries like banks.

AAVE is a "governance token" that gives holders a say in the future of the protocol. It can also be staked, thus earning rewards for holders.

The Aave protocol facilitates the creation of lending pools. If you want to lend some of your crypto, you can deposit it into a pool. Anyone who wants to borrow deposited assets can draw from Aave pools as long as they provide sufficient collateral. (Fun fact: "Aave" means ghost in Finnish.)

How it works: There are two types of tokens issued by the protocol: the native AAVE token and aTokens. AAVE tokens, beyond giving holders a say in the protocol's governance, offer advantages including discounts on fees or free use of some of the protocol's services. aTokens are received by lenders depositing to the

lending pools, and they entitle them to earn interest payments. (If you deposit, say, ETH, you'll receive aETH in return. When you pull your ETH out of Aave, your aETH will automatically be converted back to ETH.)

To help users take advantage of arbitrage opportunities (where a crypto might be valued higher on one exchange than it is on another) and maximize profits in the DeFi ecosystems, Aave also provides flash loans. These loans require no collateral and are settled instantly. The condition is that the borrowed amount needs to be paid back within the same transaction, along with a 0.09% fee, or the whole process will be cancelled, and no funds are borrowed.

You can connect your crypto wallet to Aave at app.aave.com.

Keep in mind: Standard loans on Aave require collateral (such as Ethereum) provided by the borrower. Because crypto can be volatile, it's important to choose the collateral carefully if you use Aave to borrow crypto. If your collateral's value drops below a certain threshold, it can be liquidated (as in - you won't get your money back) and you might be subject to added fees. For this reason, stablecoins are a popular collateral option. Be sure to carefully read Aave's terms and conditions.

Algorand (ALGO)

Released: June 2019

Algorand seeks to build on similar projects like Ethereum by improving scalability, security, and reducing the amount of time it takes for transactions on the network to be considered "final."

Developers can use Algorand to create decentralized applications — for loans, decentralized trading, and many other uses — that can take advantage of fast, low-cost transaction processing while scaling to many users.

How it works: Algorand nodes reach consensus about what should appear in the blockchain through a process called PPoS (or "Pure Proof of Stake") — which uses a staking system (instead of a Proof of Work mining system like Bitcoin's) to verify new transactions and produce new crypto tokens.

Algorand network participants (or nodes) can stake some of their ALGO in exchange for the chance to be randomly selected to propose a new block of verified transaction. The winner is awarded new ALGO.

Keep in mind: PPoS systems like Algorand's are more efficient than Proof of Work blockchains like Bitcoin in terms of electricity consumption, because they don't rely on thousands of miners spending energy to solve cryptographic puzzles for the chance to win a block reward and earn transaction fees.

Bitcoin Cash (BCH)

Released: August 2017

Bitcoin, in its original conception, was designed to be a form of digital cash people could use to make transactions online. Over time it has evolved into a "store of wealth" more like digital gold. Bitcoin Cash was created to continue the original peer-to-peer cash idea — via a high-volume, low-fee network that would be accessible to anyone with an internet connection.

How it works: The Bitcoin Cash blockchain is based on the original Bitcoin blockchain, but it has some distinct differences. A major one is an increased maximum block size of 32MB, compared to just 1MB on Bitcoin. Increased block size allows Bitcoin Cash to process transactions faster than Bitcoin, with lower fees and an increased per-second transaction capacity.

Keep in mind: Bitcoin Cash is available via virtually all exchanges and is supported by PayPal. But remember that even though it was designed to be faster and cheaper than Bitcoin, that doesn't mean that Bitcoin users have abandoned the original for a newer version.

Cardano (ADA)

Released: September 2017

Cardano is designed to be a next-gen evolution of the Ethereum idea. It's intended to be a flexible, sustainable, and scalable platform for running smart contracts, which will allow the development of a wide range of decentralized finance apps, new crypto tokens, games, and more.

Cardano's native cryptocurrency is ADA, which can be used to store value, to send and receive payments, and for staking and paying transaction fees on the Cardano network.

How it works: Cardano's goal is to be the most environmentally sustainable blockchain platform. It uses a unique proof-of-stake consensus mechanism called Ouroboros, as opposed to the energy-intensive proof-of-work system currently used by Bitcoin and Ethereum. (Ethereum is also moving to a proof-of-stake system via the ETH2 upgrade.

The Cardano blockchain is also divided into two separate layers: the Cardano Settlement Layer (CSL) and the Cardano Computing Layer (CCL). The CSL contains the ledger of accounts and balances (and is where the transactions are validated by the Ouroboros consensus mechanism). The CCL layer is where all the computations for apps running on the blockchain are executed — via the operations of smart contracts.

The idea of splitting the blockchain into two layers is to help the Cardano network process as many as a million transactions a second.

Keep in mind: As of May 2021, smart contact functionality has yet to be rolled out on Cardano. Developers say it will happen this year.

Chainlink (LINK)

Released: November 2017

Chainlink is a decentralized oracle network that is powered by the LINK Ethereum token. Oracles are an important part of the DeFi landscape: in the absence of a centralized authority, they're the main mechanism by which DeFi apps receive accurate external data (especially prices). Until Chainlink was developed, there was no reliable solution that allowed smart contracts and DeFi apps to access external market prices.

How it works: Chainlink was designed to incentivize a global network of computers (or "nodes") to provide accurate data to Chainlink's oracles. There are many oracles operating today, including ones that provide price data across a wide range of assets, weather data, and location data.

LINK is the token used to pay for services on the network and to incentivize nodes to perform verifiably honest work and provide accurate data. Keep in mind: To become a node and start providing data to Chainlink oracles, holders must stake LINK tokens into a smart contract to act as an incentive against misbehaving or submitting false data to the network.

Compound (COMP)

Released: September 2018

Compound is a decentralized lending protocol that allows users to deposit crypto assets to earn APY rewards, and to borrow other crypto assets against that collateral. It's part of the growing suite of DeFi apps that primarily run on the Ethereum blockchain.

How it works: When you supply an asset to Compound, you immediately begin receiving interest on that deposit. A borrowing limit is then determined, based on the value of the collateral you've supplied.

When you deposit funds into Compound, you receive a special cToken in return. For example, if you deposit USD Coin into Compound, you'll find cUSDC in your wallet — and when you withdraw your USDC, the cUSDC will disappear from your wallet. (cUSDC can also be held, transferred, and traded just like any other token.)

The yield on the crypto you deposit into Compound currently comes in two forms: interest in the form of cTokens and rewards in native COMP token. The interest rate for each Compound market is dynamic and based purely on supply and demand.

Holders of COMP tokens also get to vote on the future of the protocol itself, enabling Compound to operate in a fully decentralized way. You can connect your crypto wallet to Compound at https://app.compound.finance

Keep in mind: In traditional finance, the model of supplying one asset to borrow another is called "over-collateralized lending." It can help investors to gain exposure to more markets and enable advanced trading strategies like leveraging borrowed crypto to invest in other assets (but keep in mind that there are risks associated with collateralized lending, including potentially losing your collateral).

Cosmos (ATOM)

Released: March 2019

Cosmos aims to be the "internet of blockchains" by allowing developers to build their own blockchains, each of which are interconnected via the Cosmos network. ATOM is the native cryptocurrency, used for staking and securing the "Global Hub," which connects all these blockchains.

How it works: The main idea of Cosmos is to allow for faster and cheaper decentralized applications — anything from an NFT marketplaces to decentralized exchanged — by allowing them to run on their own dedicated blockchains.

All these independent blockchains (called "zones") are interconnected by the Inter-Blockchain Communication protocol, or IBC.

Cosmos also provides developers with prebuilt modules that allow them to quickly create blockchains that are completely customizable for their specific use case.

The Cosmos consensus engine, IBC protocol, and software developer kit are designed to enable ease of use and interoperability between chains, while

maintaining the security and transaction cost and speed developers would expect from other leading blockchain platforms.

Dash (DASH)

Released: January 2014

When Dash — the name combines Digital and Cash — was first launched, its developers' focus was on total user privacy and anonymity. (In fact, for a while it was called Darkcoin.) But in recent years, the mission has evolved towards positioning the currency as a useful method of payment for daily transactions, although it does still offer strong encryption and privacy features.

How it works: Dash uses a unique consensus mechanism that isn't quite like Bitcoin's proof of work or like Cardano's proof of stake (even though it is based on staking). Instead of requiring transaction confirmation from all the network's nodes, special validators called "Masternodes" can instantly verify a transaction.

All Masternodes are incentivized to be honest because they must have at least 1,000 of their own DASH staked. This staked DASH can be "slashed" if the Masternodes validates an improper transaction.

In exchange for doing the work of verifying transactions, Masternodes earn rewards. Keep in mind: Dash is designed to be also self-governing and self-funding, which helps position DASH as a sustainable and useful cryptocurrency for sending and receiving payments.

Dogecoin (DOGE)

Released: December 2013

For most of its existence, Dogecoin (pronounced "dohj coin") was considered to be an amusing "memecoin" beloved by its community — but with relatively little value. That changed in 2021, when DOGE became one of the larger cryptocurrencies by market cap — with a total value that has topped $50 billion, even though each individual coin is worth pennies.

Abundance is a key part of the idea — Dogecoin was created as a fun, low-stakes Bitcoin alternative. As soon as it was launched in late 2013, it began attracting an enthusiastic online community that famously once used DOGE to help send the Jamaican bobsled team to the 2014 Winter Olympics in Sochi.
Keep in mind: Unlike Bitcoin, which is designed to be scarce and resistant to inflation, Dogecoin was created to be abundant. There are about 130 billion DOGE circulating, and miners produce another 10,000 every minute.

Enjin Coin (ENJ)

Released: July 2018

Enjin is an ecosystem that aids in the creation and management of virtual goods, better known as NFTs. It provides tools for building and selling unique digital items. The Enjin platform aims to give users access to the true ownership of their digital collectibles and allow easy trading.

How it works: The ENJ token is the platform's native currency. When a new NFT is minted on the network, a chosen amount of ENJ is minted into the token. The locked funds give the newly built goods real world value, as each item can be at any point melted back into the underlying ENJ backing.

The Enjin platform also provides software developer kits (SDKs) that equip developers with tools to build their own NFTs on the Ethereum blockchain and enable their integration into the gaming ecosystems or apps of their choice.

The platform also maintains its own native NFT marketplace and a wallet with NFT support.

Keep in mind: NFTs created with Enjin use a standard called ERC-1155, which was developed by Enjin's team and is distinct from the more common ERC-721 standard pioneered by the NFT art project Cryptopunks.

EOSIO (EOS)

Released: July 2017

EOSIO aims to be an alternative to Ethereum. It provides blockchain infrastructure for decentralized applications, acting as a "blockchain computer," and allows developers to create, deploy, and host their own smart contracts and decentralized apps (or dapps).

How it works: EOSIO claims to be able to support thousands of dapps without experiencing any negative network effects like high fees or slow confirmation times, thanks to innovations like parallel processing. This may be appealing for commercial developers and financial institutions looking to adopt blockchain technologies for large-scale use cases.

The network's native token, EOS, is used to power transactions and applications on the blockchain and can be staked for a reward in a consensus model called Delegated Proof of Stake (DPoS.)

Keep in mind: EOSIO was created to be easy for developers and end-users to adopt, with a specific focus on the pain points faced by developers of blockchain applications today – particularly those of speed, scalability, and flexibility in program design.

Filecoin (FIL)

Released: October 2020

Filecoin (FIL) is a cryptocurrency that powers the Filecoin network, which is a decentralized, peer-to-peer competitor to cloud storage products like Dropbox or Amazon Web Services. Data stored via Filecoin is distributed across the entire network — as opposed to traditional centralized-server storage.

FIL tokens are used as both payment for using and supplying storage services as well as an economic incentive to ensure files are stored reliably over time.

How it works: Filecoin aims to provide a faster, cheaper, and more reliable distributed infrastructure for storing and retrieving data. It functions as a marketplace where developers can rent storage space — like a traditional cloud storage. But instead of trusting one provider with your files, they're split up and served by a globally distributed network of computers.

The Filecoin network uses two types of miners — storage miners, who store the data, and retrieval miners, who supply the bandwidth used to retrieve the files.

The communication between clients and the network happens via two types of "deals": storage and retrieval deals.

In a storage deal, the client chooses a miner to store their data and locks up the funds necessary to pay for storage. Once the agreement is accepted, the file is transferred and stored by the miner. The miner provides continuous proof of storage to the chain to receive rewards from the funds locked up by a client. If they fail to provide a proof (or if proof is delayed) the miner gets penalized.

In a retrieval deal, the client makes a payment to a retrieval miner to extract the data from the network. (Retrieval miners can also be storage miners, but they don't have to be.) These deals are executed "off-chain" — using micropayment channels to reward miners for data retrieval.

Keep in mind: Anyone with a compatible computer can start mining FIL by becoming a storage provider, making their hard-drive space available for use by the network in return for rewards. Mining configurations can range from a single desktop computer to a large-scale server farm.

The Graph (GRT)

Released: January 2019

The Graph is a decentralized and open-source protocol for indexing and querying blockchain data. GRT is the Ethereum token that fuels The Graph's ecosystem. It's used to pay participants on the network that contribute by submitting or verifying data.

How it works: Much in the way search engines index the web, The Graph aims to index blockchain data within networks like Ethereum and Filecoin. This data is grouped into open APIs called subgraphs that make it easy for developers to query the data via the GraphQL API. By making data accessible, The Graph provides DeFi applications like DEX's the data they need to operate effectively.

Indexers stake GRT tokens in exchange for the right to process queries, choose subgraphs to be indexed, and earn APY rewards for doing that work. Curators help by validating the quality of subgraphs on the network.

Keep in mind: Indexing requires a large contribution of GRT and technical knowledge — but anyone can delegate some GRT to an Indexer and receive a cut of their query and indexing rewards.

Internet Computer (ICP)

Released: May 2021

Internet Computer's basic idea is to create a new kind of decentralized internet and global computing system — with independent data centers all over the world joining together to create an alternative to the cloud services (from companies like Amazon Web Services and Google Cloud) that power most of the current internet. The ICP token has several major uses: it acts as a governance token (allowing holders to "lock" some of their ICP into the network in exchange for having a say in the future development of the ICP protocol), is rewarded by the network to participating data centers for good behavior and is used to pay transaction fees on the network.

How it works: You can think of ICP as a way of converting crypto into processing power. The network will establish a fee based on the amount of computing power required by a developer's project. As long as the fee is paid, the website will run directly on the public internet.

Keep in mind: In a truly decentralized network, who can be held accountable for hosting abusive content? Corporations running the Internet today employ some degree of moderation, although the flip side is that they can also arbitrarily de-platform anyone at any time. Ideally, Internet Computer can use decentralized governance to create solutions to these tricky issues.

Litecoin (LTC)

Released: October 2011

Litecoin is one of the oldest cryptocurrencies. It was created as a fork of Bitcoin in 2011 and offers faster transaction times and lower costs.

How it works: As a fork of Bitcoin, Litecoin did not aim to change the fundamental logic or architecture – being nearly identical to Bitcoin in terms of use and design — but it has a reduced transaction confirmation time and much lower cost (as much as 50 times lower, depending on market conditions).

Keep in mind: Litecoin's speed and relatively low fees make it appealing as a payment option and means of transferring value, but the network has significantly fewer miners than Bitcoin, which has negative effects in terms of overall network security.

MakerDAO (MKR, DAI)

Released: December 2017

MakerDAO is a decentralized organization built on the Ethereum blockchain that runs a DeFi platform that allows users to lend and borrow crypto. Its native token is a stablecoin called DAI. DAI is an ERC-20 token, which means it runs on the Ethereum blockchain. It is designed to maintain a stable value of one US dollar. MKR is a governance token issued to users of MakerDAO DeFi services. It gives holders a say in the future of the organization.

How it works: MakerDAO works through a process called "overcollateralization", where assets supplied by users are locked up in smart contracts as collateral in exchange for newly created DAI tokens.

The MakerDAO DeFi lending platform works via a collection of smart contracts that allow users to supply and borrow cryptocurrencies without a centralized loan provider.

Users create DAI by depositing some of their crypto into a smart contract on the platform. Once DAI is created, it functions as a token on the Ethereum blockchain

that can be transferred between wallets to facilitate the transfer of value like any other cryptocurrency. DAI is useful as a medium for transfers because each token always aims to be worth one U.S. dollar — which means the value won't swing wildly during the duration of the transaction. This type of stable cryptocurrency is known as a stablecoin.

Funds deposited to create DAI can be instantly re-acquired by paying off the DAI loan plus any fees.

Keep in mind: MakerDAO was the first DeFi protocol to reach a total value locked (or "TVL") of $1 billion in 2020.

Orchid (OXT)

Released: December 2019

What is OXT With digital privacy and censorship growing as concerns for people around the world, VPN services ("Virtual Private Network") has become a popular tool for privately and securely browsing the internet and interacting with online services.

Orchid is a crypto-powered VPN service that aims to extend the functionality of traditional VPN services with the security and anonymity benefits of blockchain technologies. OXT is an Ethereum token that serves as a secure means of paying for the use of Orchid's VPN service.

How it works: There are two categories of users in the Orchid network:

Bandwidth users are the customers who use the VPN. (It's available for Android, iOS, and Mac.)

Bandwidth providers are Orchid Nodes that have staked OXT tokens in order to supply their surplus internet bandwidth to users. In exchange, they receive compensation in OXT tokens. The more OXT staked, the greater the chances for a reward. Bandwidth providers are required to stake OXT to give them incentive to behave responsibly.

But you don't need to be a full bandwidth provider to benefit from staking OXT. Any holder of OXT can stake some of their tokens in a pool with a full bandwidth provider.

Keep in mind: Orchid aims to provide a distributed network of trusted, high quality bandwidth providers, allowing users to access the internet privately, and instead of relying on relying on one centralized VPN service.

OMG Network (OMG)

Released: July 2017

Purpose: OMG was designed to be used by businesses and DeFi apps to create systems that use a blockchain to transfer value between various digital and fiat currencies, and to create financial tools and services that are fast, cheap, and secure.

Built on top of the Ethereum blockchain, OMG intends to integrate with other blockchain networks and traditional payment providers to allow businesses to transfer value from one blockchain to another, or to transfer funds between blockchains and traditional payment settlement companies like Visa and Swift.

How it works: Formally known as OmiseGo, OMG is a layer-2 Ethereum scaling solution designed to be integrated into mainstream wallets. It works on top of the Ethereum blockchain to allow users to transfer Ethereum tokens faster and more cheaply than transferring them on the Ethereum blockchain directly.

OMG holders can also stake some of their tokens, which helps the network stay secure. When you stake some OMG, you earn a percentage of the overall fees that the OMG Network generates from end users.

Keep in mind: OMG claims to be “currency agnostic.” Fees remain the same no matter which currencies are and blockchains are involved in each transaction. This feature could be particularly useful for payment processors and financial institutions.

Polkadot (DOT)

Released: May 2020

Polkadot is a protocol that connects blockchains — allowing value and data to be sent across previously incompatible networks (Bitcoin and Ethereum, for example). It’s also designed to be fast and scalable. The DOT token is used for staking and governance; it can be bought or sold on Coinbase and other exchanges.

Polkadot’s developers include Ethereum co-creator Gavin Wood. It launched on May 26, 2020. The nonprofit Web3 Foundation is the primary research organization that maintains Polkadot’s open-source code.

How does Polkadot work? The Polkadot network includes a main blockchain called the “relay chain” and many user-created parallel chains (or “parachains”). It also has a connecting layer, or “bridge,” that allows value and data to be transferred between most blockchains — and can even be used to connect to non-blockchain databases.

The reason Polkadot can process so much information is because the many parachains do a lot of the heavy lifting for the main relay chain. As a result, the Polkadot network can process more than 1,000 transactions per second, compared to about 7 for Bitcoin and 30 for Ethereum. As the network grows and more parachains are added, Polkadot should get even faster, with speeds that could hit a million transactions per second.

Keep in mind… The Polkadot token (DOT) serves two main functions within the Polkadot network: it’s a governance token, which allows holders to have a say in the future of the protocol, and it’s used for staking, which is the way the Polkadot network verifies transactions and issues new DOT. DOT can be bought and sold on exchanges like Coinbase.

Polygon (MATIC)

Released: October 2017

Polygon is a “layer two” or “sidechain” scaling solution that runs alongside the Ethereum blockchain — allowing for speedy transactions and low fees. MATIC is the network’s native cryptocurrency, which is used for fees, staking, and more.

You can buy or sell MATIC via exchanges. The name MATIC comes from an earlier stage in Polygon’s development. After launching as Matic Network in October 2017, developers rebranded as Polygon early in 2021.

How does Polygon work? Picture Polygon as being like an express train on a subway — it travels along the same route as the regular train, but it makes fewer stops and thus moves much faster. (In this analogy the main Ethereum blockchain is the local train.)

To create new MATIC and secure the network, Polygon uses a proof of stake consensus mechanism— which means that one way you earn money on MATIC you hold is via staking.

Validators do the heavy lifting — they verify new transactions and add them to the blockchain. In exchange, they may receive a cut of fees and newly created MATIC. Becoming a validator is a commitment that requires running a full-time node (or computer) and staking your own MATIC. If you make an error or act maliciously (or

even if your internet connection is glitchy) you could lose some of your staked MATIC.

Delegators stake their MATIC indirectly via a trusted validator. This is a much lower-commitment version of staking. But it still requires research — if the validator you pick acts maliciously or makes errors you could lose some or all your staked MATIC.

Keep in mind: The Polygon network allows you to do many of the same things the main Ethereum network allows, but with fees that are often a fraction of a cent. You can try decentralized exchanges like QuikSwap or SushiSwap, yield generating lending and savings protocols like Aave, NFT markets like OpenSea, or even "no-loss prize games" like Pooltogether.

To try the Polygon network, you need to send some crypto to a compatible crypto wallet. You can then "bridge" some of your crypto — stablecoins are a popular choice for this — to the Polygon network. You'll also need to bridge some MATIC to make transactions, but even a dollar's worth is plenty because fees are so low.

Solana (SOL)

Released: February 2018

Solana is one of several newer cryptocurrencies designed to compete with Ethereum. Like Ethereum, Solana is both a cryptocurrency and a flexible platform for running crypto apps — everything from NFT projects like Degenerate Apes to the Serum DeFi (or DEX).

Its major innovation is speed. Solana can process around 50,000 transactions per second — compared to 15 or fewer for Ethereum. (The Ethereum 2 upgrade, which is currently underway, is designed to make Ethereum much faster than it is now).

Solana's native cryptocurrency is SOL. It's used to pay transaction fees and for staking. It also serves as a "governance token," meaning that holders also can vote on future upgrades and governance proposals that are submitted by the Solana community. SOL is available to buy and sell via exchanges like Coinbase.

How it works: One way Solana achieves high transaction speeds is via a combination of the proof of stake consensus mechanism and a new mechanism called "proof of history." Proof of history is designed to keep time between computers on a decentralized network without all the computers having to communicate about it and come to an agreement.

Keep in mind... Like Ethereum, Solana is a computing platform that can interact with smart contracts. Smart contracts power a wide range of applications, from NFT markets and DeFi to games and decentralized lotteries.

One reason a user might choose an app that runs on Solana over, say, Ethereum, is that speeds are high, and congestion is low — resulting in very low fees. (But always remember that there can be risks associated with emerging crypto applications and technologies, from volatility to the potential for undiscovered smart-contract bugs to be exploited.)

Stellar Lumens (XLM)

Released: July 2014

Stellar is a blockchain payment platform originally launched as a hard fork of the Ripple network in 2014. Created by the nonprofit Stellar Development Foundation, XLM aims to connect businesses and financial institutions around the world via blockchain — allowing them to quickly settle payments and make low-cost currency exchanges.

How it works: XLM (or Lumens), fuels activity on the Stellar network. The Stellar network is a system designed to help payments cross borders (and currencies) much faster and more cheaply than with traditional financial-system networks.

For example, a bank in Japan might use Stellar to send money to a bank in Mexico. Stellar would automatically convert yen to XLM, send the payment via blockchain, and reconvert XLM to pesos at the best current exchange rate.

Stellar was intended to work alongside existing assets and cryptocurrencies, allowing users to create digital representations of any asset as a Stellar token. These can then be used to transact on the blockchain and can be redeemed at any time for the base asset.

Keep in mind: XLM is positioned to be particularly useful in developing markets, where it aims to serve as a low-cost bridge for cross-border transactions — allowing users to send and receive payments in their preferred currency. In early 2021, the Ukrainian government selected Stellar as its partner in the development of a national digital currency.

SushiSwap (SUSHI)

Released: August 2020

SushiSwap is a decentralized exchange built on the Ethereum network. Originally forked from Uniswap, SushiSwap leverages smart contracts to provide liquidity pools that allow users to directly trade crypto assets — with no intermediary. Users can also become liquidity pool providers, supplying an equal value pair of two cryptocurrencies in order to receive rewards whenever anyone utilizes that pool. It is a DeFi protocol.

How it works: You can use Sushiswap to trade one cryptocurrency for another directly — it can't be used to trade fiat for crypto or vice versa. It uses the Automated Market Maker model pioneered by Uniswap.

You can connect your crypto wallet to Sushiswap at https://app.sushi.com/

To add liquidity, users send equal value amounts of two cryptocurrencies to SushiSwap. In exchange, they receive Liquidity Provider (or LP) tokens and begin receiving rewards.

Users can deposit their newly created LP tokens into yield farms to earn further APY rewards. This creates extra incentive for users to continue to be part of the liquidity pool over time.

Keep in mind: Users of Ethereum-based apps like SushiSwap must pay transaction fees (also called gas) that can vary widely in price and can make it expensive to use the network. DEXs have a range of risks, so do your research. "Impermanent loss" can result from pairing a more volatile cryptocurrency with a less volatile one in a liquidity pool. Bugs in smart contracts can be exploited. And anyone can create a token, so watch out for "rug pulls."

Synthetix (SNX)

Released: February 2018

Synthetix is a crypto protocol that allows users to create crypto assets called Synths that track the price of other assets — anything from stocks and commodities to "index fund"-like baskets of assets or other cryptocurrencies.

Synthetix also allows investors to buy and sell Synths, potentially making it possible to gain exposure to a huge range of investment opportunities without the need for a traditional brokerage account, bank, or fund manager.

How it works: The platform allows users to create synthetic assets called Synths on the Ethereum blockchain. Synths, in the form of ERC-20 tokens, track the value of their underlying assets. The price data is fed acquired from Chainlink oracles (see the Chainlink entry in this guide).

To create new Synths, users provide collateral in the form of SNX — the platform's native token. SNX holders are also incentivized to actively participate in maintaining the health of the system via staking.

Keep in mind: Synths can provide exposure to the underlying asset's price but investing in a Synth isn't the same as owning the asset itself — for one, you don't gain any of the voting rights that shareholders may receive.

Tezos (XTZ)

Released: June 2018

Tezos is a blockchain network and smart contract platform like Ethereum. Using Tezos, developers can create decentralized applications (lending apps, decentralized exchange apps, and much more).

Tezos's mission is to create a "self-amending blockchain." In this model, all upgrades and changes to the protocol are managed on-chain through decentralized governance.

That governance is managed entirely by the community. XTZ is the governance token that gives holders a say in future decisions about how Tezos should evolve.

How it works: Voting on proposed changes and upgrades to the protocol is conducted via a process called "baking", in which users lock up XTZ tokens to secure governance rights. This process is a form of proof of stake. Bakers can also earn rewards for submitting proposals that are successfully implemented.

Keep in mind: Tezos was among the first projects to go "fully decentralized", allowing token-holders to vote on changes to the protocol that would automatically be integrated by smart contracts, drastically reducing the chances for disputes and hard forks. It launched off the back of record-breaking $232M token sale in 2017.

USD Coin (USDC)

Released: September 2018

Cryptocurrencies are now used to make payments, to engage with decentralized services and tools, and to store value. But they tend to have a trait that limits their day-to-day usability: volatility. Even Bitcoin, which has seen less volatility compared to its earliest years, moves too much relative to fiat currencies to be a comfortable everyday currency for most users.

A new class of cryptocurrencies called “stablecoins” have their price fixed to a reserve asset (often the US dollar) at a one-to-one ratio. USDC, as its name would suggest, is one such dollar-pegged cryptocurrency. The launch of USDC was powered by a collaboration between Coinbase and Circle through the co-founding of the CENTRE Consortium.

How it works: USDC can be redeemed on a one-to-one basis for the US dollar and is backed by dollar-denominated assets held in segregated accounts with US regulated financial institutions. Its goal is to make crypto payments via the blockchain more reliable by reducing price fluctuations.

USDC is an Ethereum token and can be used to facilitate blockchain payments and transfer of value in the context of Ethereum smart contracts. This allows users to keep cryptocurrencies in a wallet, ready to send to a friend or interact with decentralized financial tools and services, and with minimal exposure to the risk of their holdings falling in price before they get a chance to spend them.

Keep in mind: By providing assurances that token holders can redeem one USDC for exactly one US dollar at any time, the potential for price speculation is significantly reduced – resulting in a crypto asset that maintains a fixed value.

Uniswap (UNI)

Released: November 2018

Uniswap was one of the first DeFi applications to gain significant traction on Ethereum. Since then, numerous other decentralized exchanges have launched (including Curve, Sushiswap, and Balancer), but Uniswap remains among the most popular.

As of April 2021, Uniswap had processed over $10 billion in weekly trading volume. Uniswap allows users anywhere in the world to trade crypto without an intermediary (but doesn’t allow for crypto-fiat trades, or vice versa). Users can also become liquidity pool providers, supplying a pair of two cryptocurrencies to receive rewards whenever anyone utilizes that pool.

UNI is a governance token that allows holders to vote on key protocol changes.

How it works: Uniswap pioneered the Automated Market Maker model, in which users supply Ethereum tokens to Uniswap “liquidity pools” and algorithms set market prices (as opposed to order books, which match bids and asks on a centralized exchange).

You can connect your crypto wallet to Uniswap at https://app.uniswap.org/

By supplying tokens to Uniswap liquidity pools, users can earn rewards while enabling peer-to-peer trading.

Anyone, anywhere, can supply tokens to liquidity pools, trade tokens, or even create and list their own tokens (using Ethereum's ERC-20 protocol).

There are currently hundreds of tokens available on Uniswap, and some of the most popular trading pairs are stablecoins like USDC and Wrapped Bitcoin (WBTC).

Keep in mind: One issue users of Ethereum-based apps like Uniswap face are transaction fees (also called gas) that can vary widely in price and can make it expensive to use the network. Multiple solutions to this issue are in the works, from the long-planned transition to the ETH2 blockchain (scheduled for some time in 2022) to the nearer-term rollout of a "Layer 2" scaling solution called Optimism later this year. Uniswap developers are confident that Optimism will allow for significantly cheaper Uniswap transactions.

In early May 2021, Uniswap v3 launched with the goal of making transactions faster and cheaper.

DEXs have a range of risks, so do your research. "Impermanent loss" can result from pairing a more volatile cryptocurrency with a less volatile one in a liquidity pool. Bugs in smart contracts can be exploited. And anyone can create a token, so watch out for "rug pulls."

Yearn.finance (YFI)

Released: July 2020

YFI is an Ethereum-based token that powers Yearn.finance — which is designed to simplify the process of depositing funds into DeFi projects. DeFi typically requires a fairly high degree of technical knowledge. Yearn.finance (or yEarn) aims to solve this by creating a simple, streamlined portal via which less technically skilled users can access DeFi platforms. Think of it as a "robo-advisor" of sorts.

How it works: yEarn aims to be a sophisticated "yield farming" automation tool with a streamlined interface. It automatically moves funds supplied by investors between the liquidity pools of various DeFi projects via smart contract, to achieve the highest possible return for investors.

It also enables investors to use automation to drive decisions about which projects they should invest their funds into in order to get the best deal possible and maximize their profits.

Keep in mind YFI is a governance token, which means that holders can vote on changes to the protocol's structure or operational model. It has only been rarely distributed to users, but existing YFI can be bought or sold like any other cryptocurrency.

Zcash (ZEC)

Released: October 2016

ZEC is known as a "privacy coin" due to its focus on anonymity for users and the transactions they make on the ZCash blockchain. It was developed by cryptography experts to address what they saw as privacy issues with the Bitcoin network.

How it works: ZCash enables a range of public and private transaction types. Public addresses can send "shielded" transactions to private addresses, or transactions can either be fully private or fully public. ZCash makes use of Zero-Knowledge proofs (or "zk-SNARKS") in order to keep information about the sender, receiver, and the transacted amount private whenever a "shielded" ZEC transaction is made. An optional "Memo" field can also be filled in whenever a user makes a payment. This field can only be accessed by the recipient, which could prove useful for a number of interesting use cases across the FinTech and DeFi spaces.

Keep in mind: The Zcash protocol was designed to evolve in-line with the needs of the community over time. Governed by the Zcash Improvement Proposal process, ZCash token holders can vote towards proposed changes and upgrades to the protocol.

Chapter 26: Third Party Research Sources

A little more than a decade ago, Bitcoin emerged as a new kind of money designed for the internet – giving people on opposite sides of the world the ability to exchange value without governments, banks, or anyone else in the middle.

In the years since, it's evolved into an asset worth trillions of dollars and sparked an entirely new, constantly evolving crypto universe.

If you're seeking a deeper understanding of all things crypto, you've come to the right place. I've gathered some of the smartest, most essential resources the internet has to offer: YouTube clips that can help you grapple with arcane concepts, podcast interviews with foundational figures, and the Bitcoin white paper — the document that started it all.

The best way to understand crypto — how a blockchain works, why it matters, how the space has evolved — is to start with Bitcoin. The original cryptocurrency continues to dominate all other forms of digital money—it's most people's gateway to the wider crypto world, and its technology provides the foundation for a lot of what came after.

Here are some of the best explanations of what Bitcoin is and how it gave rise to the entire crypto ecosystem.

Explain Bitcoin Like I'm Five (Angel investor Nik Custodio does exactly what the title says)

Ben Horowitz explains the rise of crypto (a 3-minute explanation of crypto's potential)

But how does Bitcoin actually work? (Invaluable, easy-to-understand YouTube explainer)

An Intro to Crypto: Building Blocks (Crypto venture-fund founder and former Coinbase Product Manager Linda Xie breaks down the core concepts linking Bitcoin, Ethereum, and more)

Why Bitcoin Matters (Marc Andreessen, investor and Coinbase board member, makes the case for digital money in a 2014 New York Times essay)

The Internet of Money (Investor Naval Ravikant's Wired article that introduced a lot of people to Bitcoin's wider potential)

Bitcoin whitepaper: A Peer-to-Peer Electronic Cash System (Satoshi Nakamoto's 2009 whitepaper that started it all – technical, but more readable than you'd assume)

Cryptocurrency: The Future of Finance and Money (In this four-minute video, experts from Coinbase and across the crypto universe dive into the democratizing potential of cryptocurrency). Why (and how) you should think about investing in Bitcoin. In a remarkably short period of time, Bitcoin's market cap has gone from essentially zero to nearly $2 trillion. If you want to understand where Bitcoin has been and where it's headed, we've gathered insights from some of crypto's biggest and smartest investors.

Bitcoin for the open minded skeptic (Crypto VC specialists Paradigm break down the essentials of Bitcoin for investors)

The Great Monetary Inflation (Hedge fund pioneer Paul Tudor Jones shares his crypto strategy in this much-circulated investors' letter)

The Case for Bitcoin (Excellent, useful, and constantly updated mix of data and analysis)

Bitcoin's Killer App (Deep dive on investing and blockchains from crypto fund Pantera Capital)

Why MicroStrategy invested $500 million in bitcoin (Thorough YouTube interview with MicroStrategy CEO Michael Saylor)

What will happen to cryptocurrency in the 2020s? (Coinbase CEO Brian Armstrong on how the decade might unfold)

Ethereum and other coins

Ethereum took Bitcoin's blockchain idea and made it more flexible – allowing it to power everything from games to tools that are creating an entire decentralized alternative to the financial system. But while it might be the second-biggest digital currency by market cap, it's certainly not the only Bitcoin alternative. Learn about Ether and other altcoins here.

Ethereum in 25 minutes (Ethereum cofounder Vitalik Buterin explains the basics in this YouTube talk)

The evolution of Ethereum (Want to go deeper? This guide from the Ethereum Foundation will take you there.)

Ethereum whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform (The original 2013 document proposing the world's first programmable blockchain)

Beginners Guide to Cryptoassets (Linda Xie's guide to Monero, Tezos, Zcash and more)

The 10 Most Important Cryptocurrencies other than Bitcoin (Investopedia's guide to some of the most popular altcoins)

Core concepts

If you want to really understand crypto you need to understand the technology behind it. Get up to speed on concepts ranging from blockchains and decentralization to smart contracts and more.

1729.com (Newsletter created by crypto venture-fund investor and former Coinbase CTO Balaji Srinivasan that schools readers on key concepts from DAOs to building DeFi apps)

What is Blockchain: The Complete Wired Guide (Highly readable explainer from the tech magazine)

Why (TF) Blockchain? (Interesting take from software engineer and crypto investment fund manager Aleksandr Bulkin)

The Meaning of Decentralization (Vitalik Buterin explains why it's more than just a crypto buzzword)

Why decentralization matters (a16z partner Chris Dixon explores the next phase of the internet)

Thoughts on tokens (More writing from Balaji Srinivasan — how Bitcoin's token concept could change the internet)

A Beginner's Guide to Decentralized Finance (DeFi)

Best crypto podcasts

Want to take your crypto education offscreen and hear about the latest developments? These crypto podcasts offer behind-the-scenes stories and interviews with key players.

Hash Power: A documentary on blockchains and cryptocurrencies (Three-part audio documentary - the crypto universe)

Bankless ("Guide to crypto finance" in podcast form)

Epicenter (Long-running podcast on all things crypto)

Unchained (Laura Shin's popular "no hype" crypto resource)

And more...

Check out the lists that inspired this guide created and maintained by crypto investors. They're full of valuable material.

a16z Crypto Canon (Venture giant Andreessen Horowitz's crypto fun maintains this mega list of crypto articles)

Dan Romero's Crypto Reading (Angel investor and former Coinbase Vice President Dan Romero chronicles crypto history via his list of essential links)

Chapter 27: Third Party Research Sources

A little more than a decade ago, Bitcoin emerged as a new kind of money designed for the internet – giving people on opposite sides of the world the ability to exchange value without governments, banks, or anyone else in the middle.

In the years since, it's evolved into an asset worth trillions of dollars and sparked an entirely new, constantly evolving crypto universe.

If you're seeking a deeper understanding of all things crypto, you've come to the right place. I've gathered some of the smartest, most essential resources the internet has to offer: YouTube clips that can help you grapple with arcane concepts, podcast interviews with foundational figures, and the Bitcoin white paper — the document that started it all.

The best way to understand crypto — how a blockchain works, why it matters, how the space has evolved — is to start with Bitcoin. The original cryptocurrency continues to dominate all other forms of digital money—it's most people's gateway to the wider crypto world, and its technology provides the foundation for a lot of what came after.

Here are some of the best explanations of what Bitcoin is and how it gave rise to the entire crypto ecosystem.

Explain Bitcoin Like I'm Five (Angel investor Nik Custodio does exactly what the title says)

Ben Horowitz explains the rise of crypto (a 3-minute explanation of crypto's potential)

But how does Bitcoin actually work? (Invaluable, easy-to-understand YouTube explainer)

An Intro to Crypto: Building Blocks (Crypto venture-fund founder and former Coinbase Product Manager Linda Xie breaks down the core concepts linking Bitcoin, Ethereum, and more)

Why Bitcoin Matters (Marc Andreessen, investor and Coinbase board member, makes the case for digital money in a 2014 New York Times essay)

The Internet of Money (Investor Naval Ravikant's Wired article that introduced a lot of people to Bitcoin's wider potential)

Bitcoin whitepaper: A Peer-to-Peer Electronic Cash System (Satoshi Nakamoto's 2009 whitepaper that started it all – technical, but more readable than you'd assume)

Cryptocurrency: The Future of Finance and Money (In this four-minute video, experts from Coinbase and across the crypto universe dive into the democratizing potential of cryptocurrency). Why (and how) you should think about investing in Bitcoin. In a remarkably short period of time, Bitcoin's market cap has gone from essentially zero to nearly $2 trillion. If you want to understand where Bitcoin has been and where it's headed, we've gathered insights from some of crypto's biggest and smartest investors.

Bitcoin for the open minded skeptic (Crypto VC specialists Paradigm break down the essentials of Bitcoin for investors)

The Great Monetary Inflation (Hedge fund pioneer Paul Tudor Jones shares his crypto strategy in this much-circulated investors' letter)

The Case for Bitcoin (Excellent, useful, and constantly updated mix of data and analysis)

Bitcoin's Killer App (Deep dive on investing and blockchains from crypto fund Pantera Capital)

Why MicroStrategy invested $500 million in bitcoin (Thorough YouTube interview with MicroStrategy CEO Michael Saylor)

What will happen to cryptocurrency in the 2020s? (Coinbase CEO Brian Armstrong on how the decade might unfold)

Ethereum and other coins

Ethereum took Bitcoin's blockchain idea and made it more flexible – allowing it to power everything from games to tools that are creating an entire decentralized alternative to the financial system. But while it might be the second-biggest digital currency by market cap, it's certainly not the only Bitcoin alternative. Learn about Ether and other altcoins here.

Ethereum in 25 minutes (Ethereum cofounder Vitalik Buterin explains the basics in this YouTube talk)

The evolution of Ethereum (Want to go deeper? This guide from the Ethereum Foundation will take you there.)

Ethereum whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform (The original 2013 document proposing the world's first programmable blockchain)

Beginners Guide to Cryptoassets (Linda Xie's guide to Monero, Tezos, Zcash and more)

The 10 Most Important Cryptocurrencies other than Bitcoin (Investopedia's guide to some of the most popular altcoins)

Core concepts

If you want to really understand crypto you need to understand the technology behind it. Get up to speed on concepts ranging from blockchains and decentralization to smart contracts and more.

1729.com (Newsletter created by crypto venture-fund investor and former Coinbase CTO Balaji Srinivasan that schools readers on key concepts from DAOs to building DeFi apps)

What is Blockchain: the Complete Wired Guide (Highly readable explainer from the tech magazine)

Why (TF) Blockchain? (Interesting take from software engineer and crypto investment fund manager Aleksandr Bulkin)

The Meaning of Decentralization (Vitalik Buterin explains why it's more than just a crypto buzzword)

Why decentralization matters (a16z partner Chris Dixon explores the next phase of the internet)

Thoughts on tokens (More writing from Balaji Srinivasan — how Bitcoin's token concept could change the internet)

A Beginner's Guide to Decentralized Finance (DeFi)

Best crypto podcasts

Want to take your crypto education offscreen and hear about the latest developments? These crypto podcasts offer behind-the-scenes stories and interviews with key players.

Hash Power: A documentary on blockchains and cryptocurrencies (Three-part audio documentary the crypto universe)

Bankless ("Guide to crypto finance" in podcast form)

Epicenter (Long-running podcast on all things crypto)

Unchained (Laura Shin's popular "no hype" crypto resource)

And more...

Check out the lists that inspired this guide created and maintained by crypto investors. They're full of valuable material.

a16z Crypto Canon (Venture giant Andreessen Horowitz's crypto fun maintains this mega list of crypto articles)

Dan Romero's Crypto Reading (Angel investor and former Coinbase Vice President Dan Romero chronicles crypto history via his list of essential links)