Cryptocurrency 101 - Jeremy Tunnell

Updated Jan 17, 2018

For latest version: http://www.jeremytunnell.com

Cryptocurrency 101 - Jeremy Tunnell

Updated Jan 17, 2018

For latest version: http://www.jeremytunnell.com

What is cryptocurrency?

Most cryptocurrencies are based on the concept of a blockchain, which is like a huge spreadsheet that is shared with everyone that contains a list of all of the payments everyone has made to each other. The block “chain”, is an ordered string of blocks, and each block contains a number of transactions.

In contrast to private databases, like your bank's database of account balances, blockchains eliminate the need to trust a centralized third-party to keep the database safe and accurate Instead, we spread the “database”, or blockchain, across hundreds or thousands of nodes, and we use various strategies for making sure that all of these nodes can agree about the current state of things.

Briefly, this consensus system works by incentivizing users to solve a complicated math problem, called “mining”. The first miner to solve the math problem gets the privilege of writing a block onto the blockchain, which results in them receiving a pre-determined reward of “new” bitcoin and all the transaction fees users pay to place their transactions in a block. After the block is written, the miners move on to solving the next math problem for the next block. Using a cryptographic technique called “hashing”, anyone can verify that previous blocks have not been tampered with. This whole process is referred to as “Proof of Work” (PoW), because in order to write a block to the blockchain, users have to prove they have done a certain amount of work in order to receive the privilege of writing the block.

One thing that you need to understand is that Bitcoin and most other cryptocurrencies (other than Monero and Zcash) are *not anonymous*. Even though your name isn’t on your public addresses, the activity is on the blockchain forever. If anyone ever finds out that you are connected with one of your addresses, someone can use various tools to crawl through the blockchain and figure out all of the other addresses that you own. Never treat it as if it’s anonymous (that means pay your taxes, covered later)

What is Bitcoin?

Bitcoin is a digital currency that functions as both a store of value, like gold, and a payment system, like the dollar. Most people think of these as the same thing, but they are really quite different.

For something to be a store of value, it must be durable, divisible, consistent, and scarce. The classic store of value is gold. Gold doesn’t tarnish or disappear, can be melted down and minted into coins of various sizes, is uniform between one piece and another, and has a relatively fixed supply (the supply of gold increases by a couple of percent every year due to

mining). Because there is a fixed supply, we referred to it as “deflationary”, which means it will never experience inflation, like you have every year with the dollar

Storing value is very useful, but one can’t very well carry gold coins around to purchase coffee in the morning. For that, we need currency, and for something to be used as currency it must be portable, fungible, and convenient. The most widely used currency in the United States is the dollar. A $100 bill fits nicely in your wallet, spends just as well as someone else’s $100 bill, and can be exchanged at almost any merchant for various goods and services.

A lot of people in the cryptocurrency community, and especially Bitcoin, will refer to the “original vision” of the creator, in the case of Bitcoin it is Satoshi Nakamoto (a fake name). However, for all we know, Satoshi is dead and Bitcoin is what it is, regardless of what was written a decade ago. We will talk about how Bitcoin works a bit later, but because of transaction costs, Bitcoin appears to be becoming more of a store of value and less of a payment system.

Bitcoin also has the capability of running small computer programs based on events on the blockchain, called Smart Contracts. An example of a smart contract would be some code which accepts rent payments from several roommates and then sends one payment to the landlord when everyone has paid.

What is Ethereum?

After Bitcoin came on the scene, a few people including a guy named Vitalik Buterin had a vision for a cryptocurrency based on a blockchain that instead of being a payment system or a store of value, it instead served as a platform for running distributed applications.

In one of the earliest Initial Coin Offerings (ICO), Ethereum was offered to the public and was launched.

Ethereum works similarly to Bitcoin, in that it has miners and mines via Proof of Work (PoW).

However, it also has a much more complex built-in programming language which allows for not only smart contracts but working computer programs on the blockchain. The idea is that someday we could run fully distributed programs like Facebook or Ebay on the blockchain… without servers or a company behind it.

Because miners run the computer programs, they have to be compensated for the electricity and processing power, and this is done using a commodity called gas. When someone sends a transaction to the Ethereum blockchain, they have to include enough gas to write the transaction to the blockchain and to run the computer program attached to completion. Because everyone has to pay for computation it ensures that one person doesn’t hoard all of the processing power for themselves.

Ethereum also has this concept called ERC-20, which is basically just a standard that allows anyone to create their own token which runs on the Ethereum blockchain. Most modern ICOs are done as ERC-20 tokens and issued on Ethereum. These tokens can be bought, sold, transferred, and the underlying applications can run on top of Ethereum. There are thousands of tokens of varying quality.

Future:

Why bitcoin vs dollar, vs gold, inflation, fiat currency etc,

Wallets

Each user on a blockchain starts with a wallet. A cryptocurrency wallet is not like a regular wallet, because it doesn't actually hold any coins; it just holds your private key, which is basically your password to all of your coins.

So, then, what is a wallet anyway?

A wallet is created from a seed, which is just a random number. Because of some properties of cryptography, you can take this random number and you can create a pair of numbers. The first number is your private key and the second number is your public key. Because of how these numbers interact with each other, your private key controls whether your coins can be sent to someone else, and your public key generates a bunch of addresses that you can give out to people when they want to send you coins. The wallet doesn't even really store your balance; your balance is on the blockchain. To get your balance, all you have to do is add up all of the incoming transactions to all of your addresses on the blockchain and subtract all of the outgoing transactions.

If you want to send somebody some cryptocurrency, you log onto your wallet. Your wallet looks at the blockchain and sees how much money you have, and then you create a transaction and you "sign" the transaction with your private key which is stored in your wallet.

Camp to summarize, your wallet is made up of the following pieces of information:

- seed - the random number that generates your wallet
- private keys - this is the secret passphrase that allows you to send money to others. It is stored in your wallet.
- public keys - Addresses that you can safely hand out to anyone. People send you money here

- wallet password (optional) - Most wallets allow you to set a password that you have to type in before you can access the wallet. This has nothing to do with the blockchain and is just a password to open the program.
- wallet backup password (optional) - Some wallets will also encrypt your backups to protect the information inside, and that often requires an additional password

Kinds of Wallets

Many people don't understand that the type of wallet that you use will affect the security and flexibility of your coins.

A cryptocurrency bank

In the United States, a common entry point into cryptocurrency is through Coinbase. Coinbase is an exchange that provides a very easy to use interface where consumers can purchase cryptocurrency with credit and debit cards as well as ACH transactions from bank accounts.

As part of the service, Coinbase provides you with a wallet which holds your coins. In this particular configuration, Coinbase is operating as a cryptocurrency bank. The coins in your Coinbase account are not actually yours; they belong to Coinbase and Coinbase has an agreement that anytime you want your coins they will provide them to you. As veterans say in the cryptocurrency space, "you don't hold your private key".

Because your private key is managed by Coinbase, your cryptocurrency is only as secure as Coinbase's security. In effect, your coins are piled in with everyone else's coins and kept in Coinbase's wallet. Now, of course, Coinbase is very careful with its wallet, and probably keeps a large amount of coins in "cold storage" which is another name for "not connected to the internet".

Even so, bugs happen, and several exchanges have been hacked in the past. In general, it is not advisable to leave your coins on an exchange wallet.

A cryptocurrency bank vault

Coinbase has another option, called a "vault", with additional security measures where you can place your coins for longer-term storage. Not to make things more complicated, but if you choose this option, you have another choice: let Coinbase manage your keys or manage your own keys. If you choose to let Coinbase manager keys, then you have the same safety profile as what we discussed before. If you manage your own keys, they will display them to you, and you have to save them, very carefully, somewhere where you will not lose them or where attackers may be able to find them (and that is not in a text file on your computer!)

If you choose to manage your own keys, that combined with the additional safety protections like the several day delay between withdrawals means that it's a very safe way to store your coins.

A desktop or mobile wallet

There are desktop and mobile wallets available to store cryptocurrencies. A list is provided below. Regardless of the quality of these wallets, they just shouldn't be considered for storing any significant portion of cryptocurrency.

If you hold an amount of cryptocurrency that would cause you to lose sleep over, don't keep it on a desktop wallet.

Here's why: Desktop wallets necessarily have to keep your private key somewhere on your computer. For most of them, this is in a very predictable location. Virus authors have gotten very good at writing viruses that exploit weaknesses in wallets. In addition to viruses, your computer could be compromised by a keylogger, which just reports your keystrokes back to a hacker. This can very easily reveal your password, and thus your coins. Even mobile wallets are susceptible to bugs in mobile operating systems like iOS and Android.

Just don't do it unless it's walking around money.

Web wallets

There are web-based wallets which will create a private key and several public keys for you for you to save and use later. A popular web-based wallet which is used for Ethereum and ERC-20 tokens is called MyEtherWallet (Be careful you go to the right place because there is a scam site with a very similar name!).

What is very important about these wallets is that they do not save anything. They simply give you all of your keys, which you are expected to save, and provide an interface to make transactions to your wallet. If you fail to save the information it gives you, the wallet will not be there when you come back to the website.

Hardware wallets

Hardware wallets, like a Trezor or a Ledger, are dedicated pieces of hardware that look like little thumb drives. They are an extremely secure way to store your coins, *as long as you store the seed securely*.

Hardware wallets are extremely secure because they generate and hold your private key inside of the hardware, and there is no way to get the key out. Often, the software involved is open

sourced so anyone can examine it for flaws, and the hardware is built around secure chips to prevent hackers with physical access.

If you want to send a transaction from your wallet (most of them use a web based wallet), you plug your hardware wallet into your USB drive and the wallet sends the transaction to the hardware device to be signed.

The signature function is protected by a PIN, which you choose at setup. So, if someone steals your hardware wallet, they get about 15 guesses at your PIN before the device becomes inoperable. You, on the other hand, just need to purchase another hardware wallet and then type in the seed and you have your coins back.

How to buy cryptocurrency

If you want to buy Bitcoin, Ethereum, or Litecoin, things are fairly easy.

These days, the only way to acquire any of the largest coins is to buy them from someone else. Especially for Bitcoin, but also for other large coins, mining them isn't really an option.

You can buy them directly from other users, but note that selling Bitcoin in exchange for dollars without using an approved exchange is technically illegal on the federal level.
So, what the vast majority of people do is sign up for an account on an exchange, which is basically just a market for buying and selling cryptocurrency. You will sign up, transfer some dollars to the exchange, and then purchase your cryptocurrency with those dollars.

A list of all of the coins, their market cap, and where they are bought and sold can be found at Coin Market Cap https://coinmarketcap.com/

Exchanges

Coinbase

By far the easiest way to buy is to use Coinbase. They have a website and also mobile apps, and quickly you can be up and running, purchasing cryptocurrency with a credit card or debit card. You can also use ACH to buy from your bank account. The interface is very easy to use, and you can use the vault functionality to store your coins pretty securely.

Unfortunately, your purchases don't appear in your account until the purchase completely clears the financial system, which could be up to a week. The only way around this is to pre-fund your account with dollars and have them sitting, cleared, in your account.. Also, the purchases are not extremely reliable, and Coinbase has been known to cancel purchases for no reason. It is also expensive. You pay a premium over the market price and also a large

transaction fee. Altogether you could pay as much as a 6% premium. Due to the large number of new subscribers, Coinbase's support is basically nonexistent.

Beyond Coinbase, there are two other good options in the US: GDAX and Gemini.

GDAX

GDAX, is the same company as Coinbase, and your login to Coinbase will work on GDAX. You basically just go to a different address. GDAX is a much more complicated user interface and only accepts ACH transfers or wires. If you are or can get comfortable with the difference between market and limit orders and you are comfortable using ACH or wire to fund your account, then GDAX is a great option because fees are 0-.25%. Note, that you only pay 0% in fees if you execute a market maker order, which is basically a limit order.

A couple of things that always trip people up when moving from Coinbase to GDAX are that if you have dollars sitting on Coinbase you have to use the deposit button on GDAX to move it over. It won't show up in both places. Also, if you are doing a wire transfer, you *must* include the string of letters they give you in your wire transfer, or your money will be delayed or rejected.

Gemini

Gemini is also a great option. The exchange was founded by the Winklevoss brothers, of Facebook fame. They are early investors in cryptocurrency, and they continue to be active. The Gemini exchange is based in New York, highly regulated and insured, and perhaps the safest exchange. They also accept ACH and wire transfers, are fairly quick at crediting dollars, and their support is decent. No 0% trades though. Everything is .25%

For altcoins/tokens: If you want to buy tokens or altcoins, things become more difficult.

The large, stable, exchanges I mentioned above do not sell other altcoins or tokens. For that you have to go elsewhere, and the quality of these secondary exchanges drops quickly.

Bittrex

Probably the best of the bunch is Bittrex. It lists a wide variety of coins, is fairly good about quickly crediting deposits and withdrawals, and has a passable user interface. Basically, it works.

Binance

Binance is a new exchange. I believe it is based in South Korea (or Hong Kong?). It has a wide variety of coins, really great liquidity, a good user interface, and good security practices.

The fact that it is based outside of the United States means that I don't keep any money on it for very long. I don't trust foreign exchanges, but sign-ups are relatively quick when they are accepting them.

Kraken and Poloniex

Distant options are Kraken and Poloniex.

Both are unstable, slow, have poor user interfaces, and nonexistent support. I don't use them if I can avoid it, and actually I'm still waiting on an account verification from Poloniex from nine months ago so I couldn't use it if I wanted to. Poloniex claims to have fixed their account verification process, but I see now evidence of it.

Other mentions

Bitfinex is the largest exchange in the world but is no longer accepting US customers. There are rumors that they are not solvent.

Etherdelta is a decentralized exchange. That means there's nobody that actually runs it and no server that performs the trades. It is the first exchange to list newly released tokens, so it's often the only place to go, but it is painfully slow and has very little liquidity. It seems unusable for anyone but a hobbyist.

Cryptocurrency ATMs - Throughout the world, there is an ATM network where you can buy and sell cryptocurrency. I've never used one, so I can't say what the experience is like

https://www.youtube.com/watch?v=xajKjxxRL04

Localbitcoins isn't an exchange. It's a website where you can find other people who will sell you cryptocurrency directly. I've never used the service, so I can't speak to its convenience, but you should know that it's technically federally illegal to sell Bitcoin for US dollars to someone else without a money transmitter license. A lot of the people who use these sites are trying to avoid taxes and keep their coins private. That's mostly delusional, because if you cryptocurrencies are truly anonymous.

Also exist, but no thoughts on: Bitthumb, Bitflyer, Bitstamp, Bitmex.

Notes about exchanges

When you first sign up for an exchange that handles dollars you will have to go through what the industry calls a KYC/AML process, which stands for "Know Your Customer, Anti Money Laundering". These are federal laws, and so the process will be roughly the same no matter which exchange you are on (unless the exchange is foreign or it doesn't handle dollars).

Basically, you will have to type in a bunch of information, scan a passport or driver's license, and probably upload a picture of you holding the passport or license with a dated piece of paper. Most of the large exchanges have automated this process, but sometimes it takes a while, maybe weeks.

After you are approved through the KYC/AML process you will have a set of limits on your account. These limits are the amount of money or coins that you can deposit or withdraw during any time period, usually days. If you want to be able to move more money, you'll have to apply for higher limits, which requires more information and more time.

Security on Exchanges (IMPORTANT)

When your money sits on an exchange, it is only as safe as the security practices of the exchange. Cryptocurrency sitting on an exchange is not FDIC insured. Some exchanges, like Coinbase and Gemini have private insurance that covers a portion of their deposits, but as a general rule you should never trust exchanges. The history of Bitcoin is riddled with exchanges that have been hacked, including MtGox, Bitfinex, BTC-E, and others.

General Security Practices

When it comes to security in cryptocurrency, it should be a very top priority.

You have risks like exchanges being hacked, private keys being stolen, phishing websites, viruses, and social engineering.

Here are some best practices:

- Never keep large amounts of cryptocurrency on a computer or a phone
- Never keep large amounts of cryptocurrency on exchanges for longer than you need to finish your transactions
- Never search for the name of exchanges on search engines because scammers have registered misspellings and buy ads trying to get you to access their scam sites
- Always double check the address bar to make sure you are on the correct website before putting in any sensitive information
- Never give your private key out to anyone, except web wallets that require it, and you should be using a hardware wallet anyway.
- Always quadruple check your addresses before you hit the send button on cryptocurrency transfers. Only cut and paste (never type it out), check it after you paste several times and on the confirmation screen. **If you send cryptocurrency to a mistyped address it is gone forever and no one can get it back.**

- If necessary, send a test transaction with a very small amount of cryptocurrency first to make sure it reaches the other side
- Keep your computer up to date with updates, firewalls, and antivirus software
- Don't click on links or attachments in emails that you don't recognize
- Always use two factor authentication on any site that allows it, and use a long and secure password.
- Always use a different password for every site. If you have trouble remembering or storing passwords, use a password database like Keepass. If you use the same password everywhere, and one of the sites gets hacked, the hacker has all of your passwords to all of your sites

How to sell/taxes

In order to sell your cryptocurrency, you will basically do the opposite of what you did to buy it.

Whatever you do, make sure that you have a plan to sell your cryptocurrency and make sure that it works. The worst thing in the world is to try to sell $5000 worth of Bitcoin and find out that your incoming limits are $2000 per day.

Once you execute the sell orders on the exchange, you will then have dollars in your account, which will then be sent to your bank account via ACH or wire.

Taxes (US)

I am not a tax professional, and this is not tax advice.

I am simply sharing what I have found on the Internet and through speaking to professionals.

Any exchange between dollars and cryptocurrency or cryptocurrency and other cryptocurrency is taxable. If you held the cryptocurrency for under a year, you will be paying short term capital gains, which is basically your ordinary income tax bracket, ranging from 15-39.6%, and if you held for over a year, you will be paying long-term capital gains, from 15-23.8%.

I am not completely aware of how the AMT affects these sales.

A quick note about like kind exchanges. Like kind exchanges are a special tax benefit for property, which is what the IRS calls cryptocurrency. It allows you to defer gains on your sell until you sell the replacement coins. In short, there appears to be no way to do a like kind exchange with cryptocurrency. There are specific requirements, including reporting to a third party within 45 days, and most people wouldn't even try this without an advisory letter from their lawyer, and lawyers won't give you one. So just forget it.

If you don't pay your taxes, you should know that the IRS will eventually find you because all of the transactions are on the blockchain.

How to make money in cryptocurrency?

Making money is simple to understand. The price of Bitcoin, for example, is simply supply and demand. Where there is a fixed supply, and demand increases, the price has to increase. You buy it at a low price and you sell it at a high price, and the difference is your profit (and also what you pay taxes on).

There are several different kinds of investors and traders in the cryptocurrency space, covered briefly below:

Long term holders - Long-term holders are people that bought the cryptocurrency early and held it for a long time. There is an inside joke where everyone calls themselves HODLers, because some drunk guy in a reddit board misspelled the word one night and it was funny and stuck. This is the easiest way to try to make money because you don't really have to do anything except keep your coins safe and don't panic sell.

Value investors - We will cover this more later, but value investors try to buy an asset when they think it is undervalued and then sell it when they believe it is overvalued. This is difficult in cryptocurrency because every valuation has an "irrational exuberance" premium, and nobody really knows how to value cryptocurrency yet.

Day trading - Day traders attempt to make purchases every day or every few days which result in selling higher than they buy. Some people are really good at this and others are not so good. It requires really steady emotions.

Day traders will do things like sit in chat rooms all day attempting to get word of breaking news so that they can trade before the market reacts or they try to get inside information on certain coins (cryptocurrency is not currently regulated and therefore insider trading is legal).

Others use trading strategies like "momentum", where you buy on an upturn and hope to ride the crowd to the top. Or some even subscribe to a field called Technical Analysis (TA), which promises to give traders an edge by looking at the shape of the price history chart in order to predict future prices. There is some degree of evidence that technical analysis provides a leg up on the competition, but it is by no means a crystal ball.

Unless you really know what you're doing, a simple buy-and-hold strategy is probably the smartest way to go.

Never panic sell your coins. There is lots of volatility and you have to be prepared for as much as 50% drops in one day. If this is not something you can handle, then you shouldn't be in cryptocurrency.

What do I buy?

I am not an investment advisor and I am not giving investment advice. This is simply my opinion and is only one of many strategies for investing in this market.

The oldest, biggest, and most tested cryptocurrency is still Bitcoin. It is easier to buy, more liquid, less volatile, and more battle tested than the other coins and tokens. Bitcoin is potentially a replacement for gold in the digital world and potentially a replacement for various currencies for payments and transfers.

A lot of people, when they are deciding how much a coin could be worth, look at how big the possible market is for the coin. In the case of Bitcoin, if one thinks that it will be digital gold, then the total market cap could be as much as 6 trillion. If you take 6 trillion and divided by 21 million Bitcoins you get something around $300,000 per coin, which is what Bitcoin COULD be worth some day.

In the case of Ethereum, you could get a possible price by estimating the value of all of the possible distributed applications that could run on it. That's a big number.

Here are some rules of thumb for evaluating coins and tokens:

- Read the whitepaper. Is it filled with buzzwords or does it sound reasonable? Does it make large but realistic promises?
- Look at how far along the product is. Do they have an existing product or are they attempting to start from scratch? How hard is it to build the type of product they are trying to build?
- Look at the team. What is their history? To they have a history of successful projects? Do they seem to have the needed expertise?
- Check the telegram chat. There is an app called telegram, and most coins have a chat room where you can go and monitor news and speak with the team. Are they professional and/or responsive?
- Check the website. Does it look professional? Is it filled with misspellings and mistranslations?
- Where is the team from? If you are dealing with a coin or team from a foreign country, realize that there is additional risk depending on that country.
- Search the Internet for reviews and/or complaints. Look carefully if anyone has used the word scam or ponzi when referring to it.
- Join Facebook groups built around sharing research about coins and tokens

- Look at the structure of the token and how it is marketed. Does it have suspicious features like referral programs, guaranteed returns, or an over emphasis on making money on appreciation?

Known scam coins/tokens:

1. BCC Cash (note that this is different from Bitcoin Cash)
2. Binary Coin
3. BitAI
4. Bitclub
5. Bitconnect X
6. Bitfinite
7. Bitglare Coin
8. Chrysos
9. Coinrium
10. Cointeum
11. Coinspace
12. Davor
13. Eigencoin
14. Ethconnect
15. Etherbanking
16. Exacoin
17. Falcon Coin
18. Ficoin
19. Forzacoin
20. Futurecoin
21. Gold Reward Token
22. Goldgate
23. Hextracoin
24. Home Block Coin
25. HotCrypto
26. Hydrocoin
27. Ibiscoin
28. Ideacoin
29. Knox Coin
30. Legendcoin
31. Lendconnect
32. Lendera
33. Libra Coin
34. LoopX
35. Martcoin
36. Moneroconnect

37. Monetize Coin
38. Monyx
39. Neoconnect
40. Numiv
41. Onecoin
42. Pagarex
43. Regalcoin
44. Secular Coin
45. SFICoin
46. Steneum
47. Stepium (actually a pyramid scheme)
48. TEX Coin
49. Thorn Coin
50. Ucoin Cash
51. Unix Coin
52. USI Tech
53. Western Coin

Possible scam coins/tokens

1. Tron (TRX)

Defunct scam coins/tokens

1. Ambis
2. Bitcoinly
3. Bitconnect
4. Bitlake
5. Bitpetite
6. Chain.Group
7. Coinreum
8. Cryptodouble
9. Metizer
10. Microhash
11. Thunderbit
12. Vixice
13. Vone

Frequently Asked Questions

Bitcoin isn't backed by anything, it's only worth what someone is willing to pay for it. Is that a reason why it will not be successful?

The best way to answer this question is to work backwards from the dollar.

Most people have forgotten that it was only until very recently that the US dollar was backed by gold. If you walked into a bank and turned in a dollar, they could give you a dollar worth of gold in return. All of that ended with Richard Nixon and the fall of the gold standard.

Today, the dollar is simply backed by the federal government. When people say this, they usually mean two things: that the federal government can force you to pay taxes in dollars and that the dollar supply is controlled by the Federal Reserve.

The former claim, while correct, doesn't set a very high bar on the minimum value of the dollar. If, for some reason, people started using the dollar only for paying taxes, that would represent a huge drop in circulation and demand, and thus a huge drop in the world's appetite for dollars. Lower demand would force the value of the dollar to plummet.

To the latter claim, the Federal Reserve does in fact have a lot of control over the value of the dollar, but it's ability to prop up the value of the dollar in a situation where people suddenly decide that it's not worth very much is exaggerated.

When they say that gold is backed by something, they usually claim that it is backed by the fact that it's a useful material, used in things like jewelry and electronics. However, if we had to rely on just the industrial value of gold, it would be nowhere near the value it is today because it's a store of value.

Like any other store of value, Bitcoin is also only worth what people are willing to pay for it. But to say that it's not backed by anything is not true. Bitcoin has all of the intrinsic properties of gold that make it a great store of value, with the addition of some extra ones that make it better. It is, again, protected by a fixed supply, a distributed group of miners, and a governance structure that prevents changes in Bitcoin without the overwhelming consensus of the whole network.

Can I buy a fraction of a Bitcoin or anything else?

Yes, with many coins and tokens you can buy a fraction of the coin. You don't have to spend $12,000 at a time to buy a whole Bitcoin.

Why are prices so different? Why are some coins $10,000 and other coins $0.10?

It's very important to understand that the price of a coin is calculated by supply and demand. And every coin has a different supply. Bitcoin has 21 million coins. Litecoin has several times as many. If Bitcoin and Litecoin were the same price, then the total market cap of Litecoin would be several times more.

Please do not confuse a low price with a good deal. Bitcoin may be a good deal at $10,000, but ripple may not be a good deal at one dollar because ripple has something like 40 billion coins instead of 21 million.

This is very important. You cannot compare one coin with another based on its price.

Is Bitcoin a ponzi scheme?

https://prestonbyrne.com/2017/12/08/bitcoin_ponzi/

Future additions:
Bitcoin history
- Mtgox
- Other hacks
- Scaling debate
- Forks

Bitcoin risks
- Regulation
- Another mtgox
- Forks
- Other coins
- Government coins