

Crypto Fundamentals

By [Richard D. Bartlett](#), April 24 2021

Crypto is in another bull market: imagine a horny bull running through the streets making enormous up-thrusts of enthusiasm. The total [market cap](#) of the [global cryptocurrency market](#) has increased by more than 1 trillion US Dollars in the past 2 months.

Much of this interest is fuelled by a potent combination of get-rich-quick and techno-utopian mythologies. I know a little bit about the tech, so my friends have been asking me for a “101” introduction to the space. Instead of having the same conversation 15 times, I’m writing this primer. I’ll try to make a very high-level summary of the parts of the system that I sorta-kinda understand.

Honestly I am pretty clueless, so this doc will be riddled with errors and oversimplifications. Think of me as the “one-eyed man in the land of the blind”. Please improve this paper with comments, and use it as a jumping off point to do your own research. Asking “dumb questions” is fine, I enjoy explaining things. This will be thick with unfamiliar concepts, so just take it one chunk at a time. If you prefer practical hands-on experience instead of reading a document by yourself, check out [this excellent online course](#) from my friend Stephen Reid.

What’s all the fuss about?

Think of a spreadsheet: a familiar way to store data. One of the reasons you use a bank is you feel confident that the spreadsheet that “contains your life savings” is not going to accidentally get deleted. You can trust that their security protocols will prevent me from impersonating you and making transactions without your permission. This is literally why banks exist: we trust that they can manage very important data and prevent people from tampering with it.

It’s not just banks, there are a lot of institutions in contemporary society that are mostly just a very important spreadsheet with a lot of security around it: insurance companies, the stock market, real estate agencies, the tax department... All these institutions need rock-solid trustworthy data integrity that cannot be tampered with.

This is why people are excited about crypto: the nerds have figured out how to create tamper-proof high-security spreadsheets that don’t require institutions. There are various words for these new-fangled spreadsheets: blockchains, distributed ledgers, hash tables etc. Each of those is a slightly different approach to the problem of creating a trustworthy list of data,

identities, and transactions, with no central node, no headquarters or home base. Instead of having a single spreadsheet in a high-security office, we make a million copies of the spreadsheet and put it on a million computers around the world.

That's what all the fuss is about. We don't know exactly what is coming, but a lot of people believe that banks are going the way of video-rental stores: made obsolete by new technology. People are betting trillions of dollars on this possibility.

Right now, most of the activity in the crypto space is focussed on financial applications, but some people expect it to eventually infiltrate the entire digital universe: social media, supply chain logistics, gaming, medicine, citizenship... everything. We refer to them as "cryptocurrency" projects, but the currency is just the incentive to participate: it's the reward you get for being one of the millions of computers sharing the work. The currency also gives you the right to participate in governance decisions about how each project evolves.

It's called "crypto" because it relies on a lot of clever [cryptographic math](#) to validate the data integrity, but that is out of scope for this paper. You don't need to understand the math. But you do need to understand the incentives that are driving this transition. I'm going to scan across some of the popular crypto projects to give you a taste of what they are up to.

#1: Bitcoin

Bitcoin is “digital gold”: it’s valuable because it is scarce and it is hard to mine.



The orange line is the total supply: there’s currently about 18 million Bitcoins in existence. It’s getting progressively more difficult to create more, with a hard limit at 21 million coins (because: math).

The blue line shows the total market cap for Bitcoin (the price per coin multiplied by the number of coins). This is a logarithmic chart: each step up is 10 times bigger than the last one. The 2014 peak was about US\$10B, then in 2018 it crossed \$100B, and the latest peak has taken us over one thousand-billion: i.e. the total value of all the Bitcoins in the world is more than a trillion US Dollars.

The price of one Bitcoin (BTC) is about \$50,000 today. Basically everyone in the crypto space believes that in the long term, the price of Bitcoin is going to keep increasing exponentially and probably stabilise somewhere around [\\$100,000 to \\$1M per coin](#). (They could be wrong of course.)

Nobody knows who invented Bitcoin. An anonymous genius put some code into the world, and then this happened. There are millions of computers in the world maintaining the Bitcoin blockchain: validating transactions, keeping tabs on who owns all the coins, and making sure that the coins [can’t be duplicated](#) (unlike normal digital files). I mean the “official spreadsheet”

that keeps track of all the Bitcoins doesn't live in an office or a vault, it lives on millions of computers. Why would people do this? Because the system is designed with incentives that reward them for participating.

But isn't it incredibly energy intensive? Yes, it has a similar [energy footprint](#) to a medium-sized country. *But isn't it incredibly inequitable?* Yes, it has more [extreme wealth inequality](#) than any country on Earth.

If you think these are significant problems, congratulations for having good opinions. Everybody agrees that Bitcoin would be better if it didn't waste so much energy doing the equivalent of solving Sudoku puzzles. The question is: what do we do about it? There is no Bitcoin HQ to protest outside, it's not subject to any legislative jurisdiction, there is no founder to sue for environmental negligence. I'm not trying to belittle the concerns here: I'm trying to show you that we are in extremely unfamiliar territory. This is an invention that has ripped a hole in how we think about institutions and governance.

Bitcoin is the first, the granddaddy of the scene. In crypto-years it is ancient technology, so it is comparatively quite rudimentary. It doesn't do much, but it does with absolute reliability. Bitcoin was the first cryptocurrency to reach mass adoption, so it has a special role in the ecosystem. It's like the dollar of the crypto world: you might be invested in 30 different crypto projects, but you measure your wealth in Bitcoins. I find it quite boring so I don't know much about it. If you want more informed opinions check out [Willy Woo](#) (very enthusiastic) and [Brett Scott](#) (very critical).

I only got interested in crypto once we got more interesting projects, like Ethereum for instance.

#2: Ethereum

Ethereum is the “world computer”. It does the tamper-proof data storage thing like Bitcoin, but it adds a layer: “[smart contracts](#)”.

You can use a smart contract to do anything a computer program can do: like sending [chat messages](#), [exchanging currencies](#), or [playing videogames](#).

The Ethereum currency (ETH) is currently worth about \$250B (second only to BTC). But it is much more than a currency, it’s an ecosystem of interacting projects. Right now, most of the activity is in decentralised finance (DeFi), but over the coming years the ecosystem could conceivably expand to include anything that you currently use software for (work, social media, games, video, etc).

[Here’s a good overview](#) of the current state of some of the popular Ethereum projects (also known as “dApps”: decentralised applications).

Because the tech is still in its infancy, interacting with a dApp is quite a complicated procedure. I’ll explain with an example:

Holochain fundraising example

I’m an early supporter of a project called [Holochain](#): I believe in their values and I like what they’re trying to achieve. So I wanted to contribute to their first fundraising round back in April 2018.

First I had to install [Metamask](#) on my computer. Metamask is a wallet for interacting with the Ethereum blockchain. I used Metamask to create an account in the Ethereum ecosystem. Then I had to buy some ETH (Ethereum coins): I sent dollars to a company and they sent me ETH.

When I say they “sent me ETH”, I mean, they made a transaction on the Ethereum blockchain, creating a public record on the decentralised “world computer” that says “these coins now belong to Richard’s account”. Now I have sole custody of the coins, nobody can deny I own them, nobody can take them off me, and there’s nobody I can ask for help if I lose my password.

The Holochain programmers created a smart contract: a small program that lives on the Ethereum blockchain. It’s public, anyone can view it [here](#). That program includes all the rules for the fundraising round: who can participate and how. I believed it was trustworthy, so I sent them about \$300 worth of ETH: I mean I transferred ownership of my ETH to the smart contract, and the contract automatically rewarded me with a handful of magic beans called “Holo tokens”.

Holochain is not connected to Ethereum in any longterm way, they just used it as a launchpad to get funding into their own ecosystem. The Holo token (HOT) uses the ERC-20 protocol, which is

























a standard that anyone can use to create tokens that can be transacted on the Ethereum blockchain.

At the time of the initial fundraising, they brought in about \$20M worth of ETH, which they've used to pay the development team for the past three years. As more people learn about Holochain and confidence in the project increases, so does the value of their token. Today the total market cap of HOT is about \$2.5B. My initial \$300 investment is worth about \$30,000.

Ethereum still mostly sucks

It's important to grasp that we're still in Ethereum 1.0, which is essentially a crap first prototype. I tried to buy something with ETH last night and it charged me a \$20 transaction fee. Four hours later, the transaction was still pending, so I spent another \$20 to cancel it. But my request to cancel is still pending! The network is completely over stretched. Ethereum 2.0 is due sometime next year, promising much more efficiency and much less energy usage.

But it has been a slow and frustrating process, which has opened up space for a lot of competition. Here's a list of the biggest cryptocurrencies, from [CoinGecko](#).

| # | ↓ | Coin | ↓ | Price | 1h | 24h | 7d | 24h Volume | Mkt Cap | Last 7 Days |
|------|---|---|------|-------------|-------|-------|--------|-------------------|-------------------|---|
| ☆ 1 | |  Bitcoin | BTC | \$49,308.98 | -0.5% | -0.4% | -19.7% | \$58,794,636,811 | \$921,318,500,428 |  |
| ☆ 2 | |  Ethereum | ETH | \$2,228.65 | -1.9% | -2.1% | -8.1% | \$41,958,906,265 | \$258,075,242,408 |  |
| ☆ 3 | |  Binance Coin | BNB | \$503.65 | -1.3% | -0.3% | -1.5% | \$6,340,947,320 | \$77,831,586,265 |  |
| ☆ 4 | |  XRP | XRP | \$1.08 | -3.8% | -2.8% | -31.2% | \$10,438,231,287 | \$50,061,589,746 |  |
| ☆ 5 | |  Tether | USDT | \$0.993594 | -0.1% | -0.4% | 0.0% | \$125,451,291,444 | \$49,255,685,422 |  |
| ☆ 6 | |  Cardano | ADA | \$1.14 | -2.7% | 4.6% | -19.3% | \$4,005,880,052 | \$36,712,603,431 |  |
| ☆ 7 | |  Dogecoin | DOGE | \$0.267385 | -3.4% | 9.8% | -28.4% | \$12,375,483,798 | \$34,769,999,281 |  |
| ☆ 8 | |  Polkadot | DOT | \$30.82 | -2.2% | 0.7% | -25.9% | \$1,903,216,406 | \$30,365,154,597 |  |
| ☆ 9 | |  Uniswap | UNI | \$31.24 | -2.7% | -3.1% | -13.9% | \$1,018,333,018 | \$16,283,909,244 |  |
| ☆ 10 | |  Litecoin | LTC | \$226.57 | -2.1% | -3.8% | -27.2% | \$6,929,748,673 | \$15,137,657,797 |  |
| ☆ 11 | |  Bitcoin Cash | BCH | \$775.14 | -2.5% | -2.8% | -31.2% | \$6,923,586,009 | \$14,570,362,433 |  |
| ☆ 12 | |  Chainlink | LINK | \$32.72 | -1.9% | -0.4% | -21.7% | \$1,928,953,260 | \$13,827,507,660 |  |

You see Bitcoin is ranked #1, and Ethereum is #2. At #6 you have Cardano and #8 is Polkadot: both of these projects were created by people who were part of the original Ethereum team, but split off to do their own thing. Each of them are creating their own ecosystem, building their own “world computers”, based on different philosophies.

#3: Binance

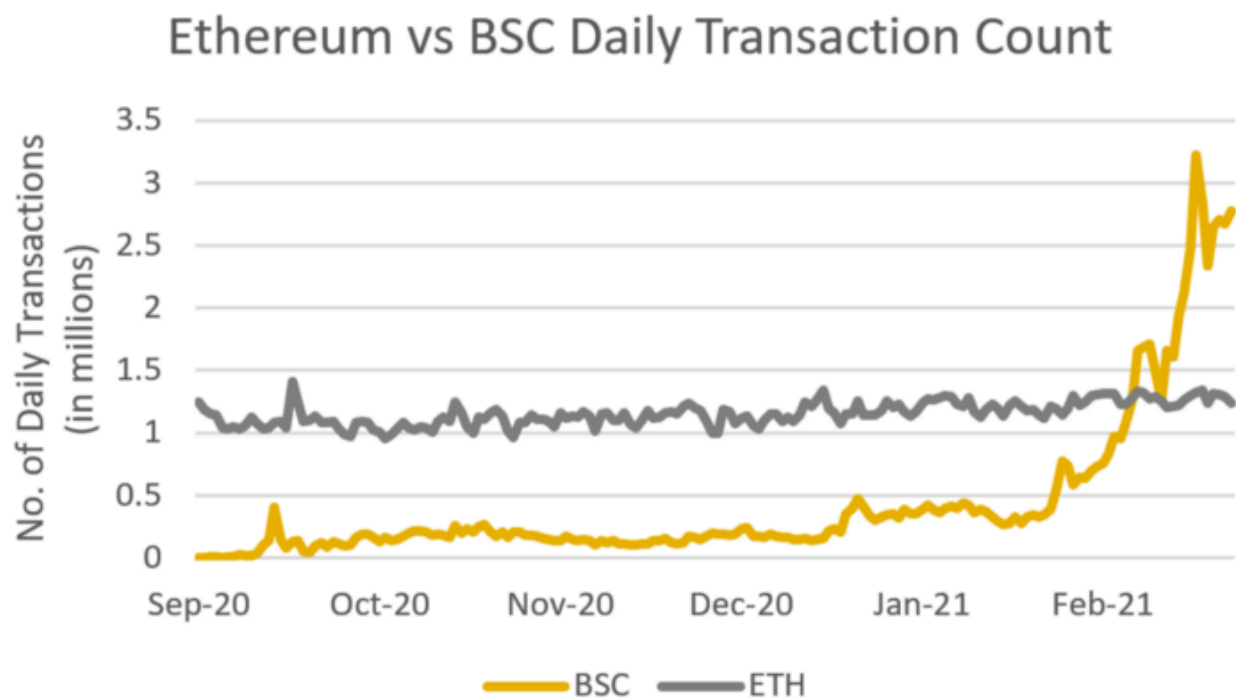
Currently the third-largest cryptocurrency, Binance Coin (BNB) was initially just a token you could use to pay for transaction fees on the Binance exchange. It started out as an ERC-20 token, meaning it was part of the Ethereum system.

The Binance cryptocurrency exchange is a [website](#) where you can trade one coin for another, just like a stock market or traditional currency exchange.

I bought some BNB tokens a couple of years ago because I wanted to use the Binance exchange: they offer a 25% discount on transaction fees for people who pay in BNB. Today those coins are worth 10X what I paid for them in 2018.

Binance Smart Chain (BSC)

In September 2020, the [Binance Smart Chain](#) launched. It's yet another blockchain ecosystem. While Ethereum has been hovering between 0.5 to 1.5 million [daily transactions](#) since 2017, BSC immediately outpaced it due to being much faster and cheaper to use (like 100X cheaper). One day this week they had 9 million [transactions](#). (Compared to 100 million [daily credit card transactions](#) in the USA.)



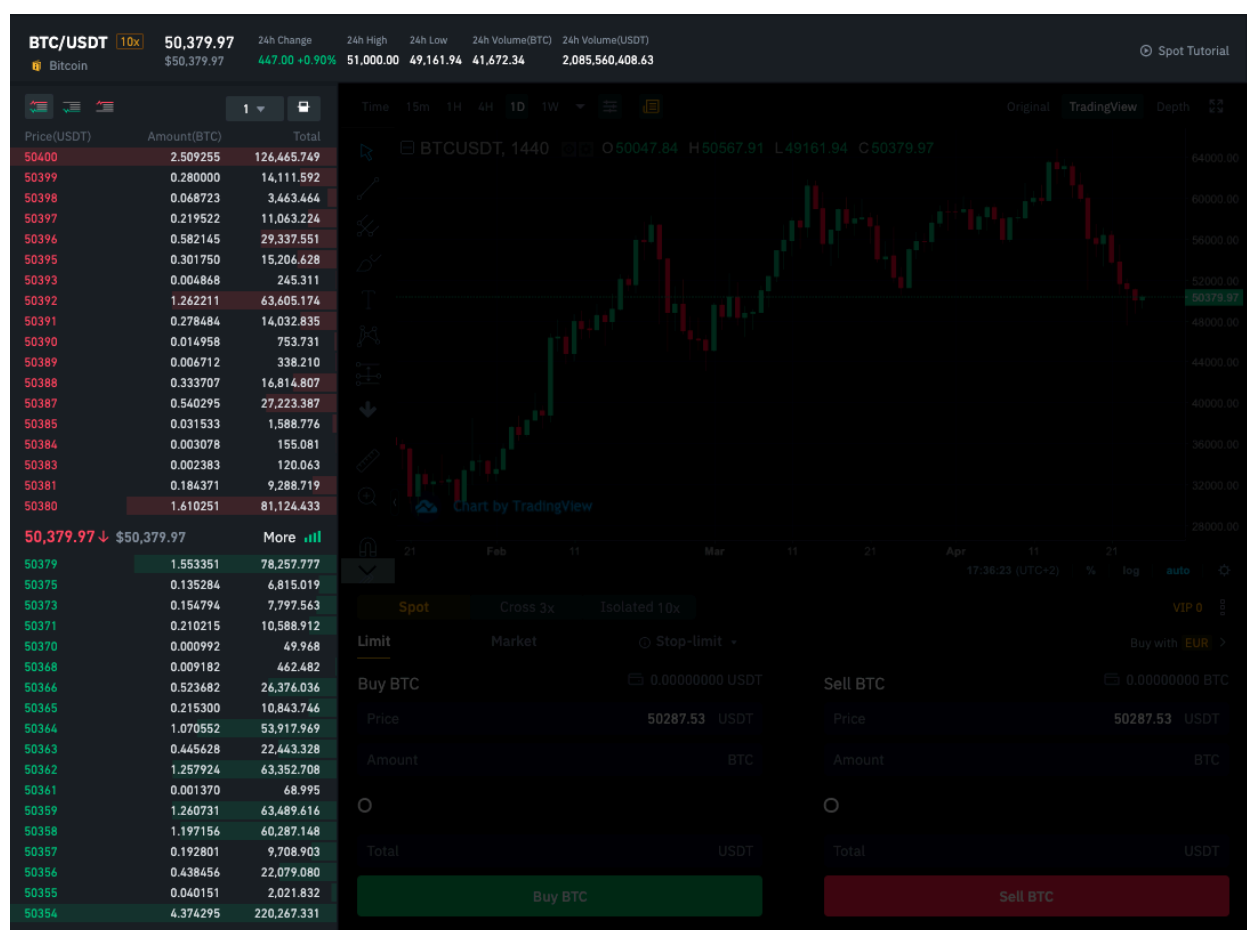
[Chart source](#)

Remember I said tokens in the Ethereum blockchain use the “ERC-20” standard? Tokens in the Binance Smart Chain use the “BEP-20” standard. You can use your Metamask wallet to hold both kinds of tokens.

Centralised Exchanges

The initial product [Binance](#) was known for was as a cryptocurrency exchange. It’s an example of a **centralised** exchange: they have an office and a bank account and a website. (See also: Crypto.com, Coinbase, Blockfi, and many more.) I’ll explain decentralised exchanges later.

Let’s say I have some USD and I want to trade it for Bitcoin (BTC). I’ll show you what the Binance market interface looks like. Unless you’re a stock market trader, this is probably unfamiliar so I’ll show one piece at a time:

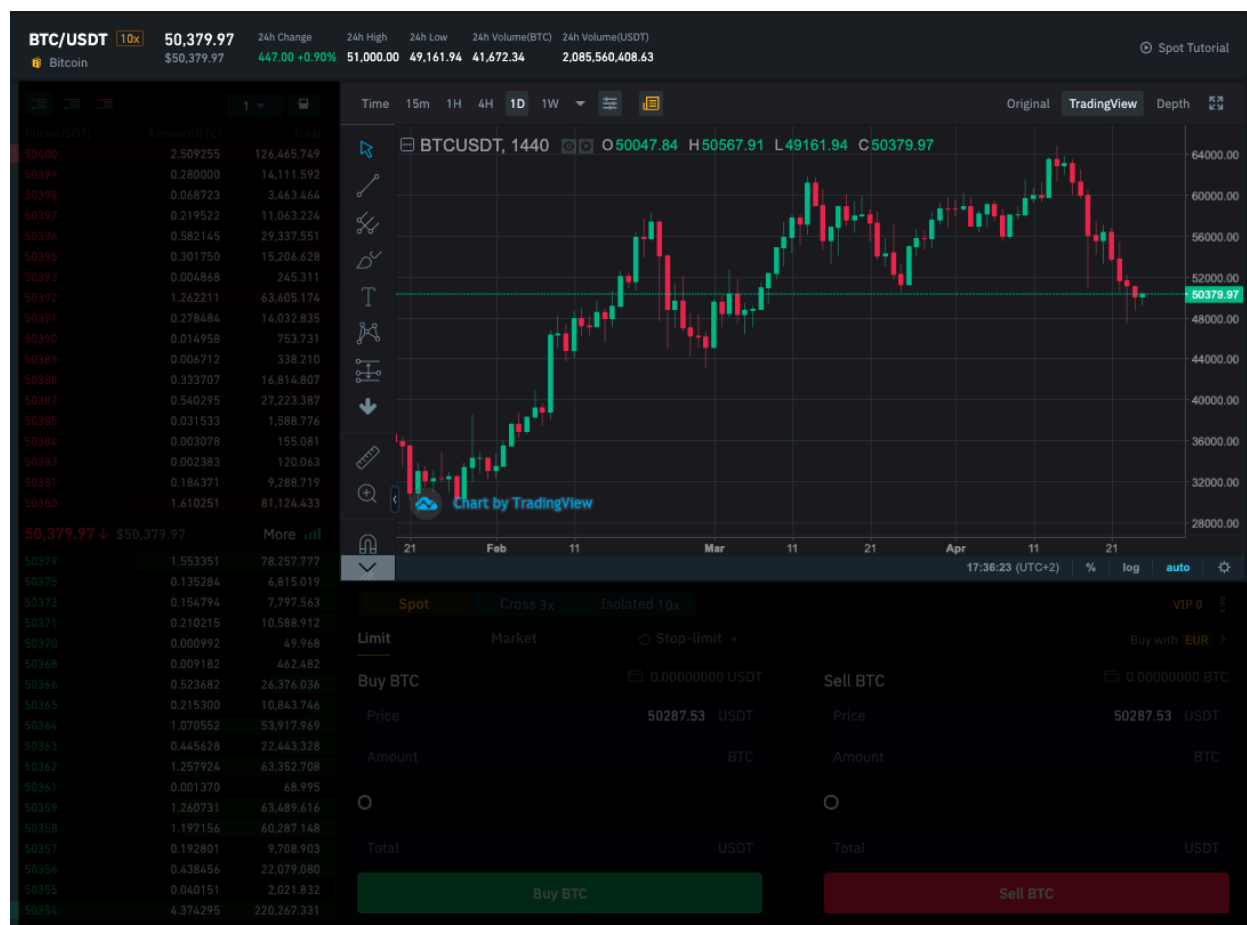


On the left is the order book. The first row is an order that someone has placed, they’re saying: “I’m willing to **sell** my BTC at a price of \$50,400”. At the bottom of the list you have someone saying “I want to **buy** BTC but I am only willing to pay \$50,354”. That’s a price gap of \$46, so neither of those orders are going to be filled right now. To complete a trade, buyers and sellers

need to agree on a price. At the moment I took the screenshot, the current **market price** was \$50,379.97 per BTC (you can see it at the middle of the list, where it switches from red to green).

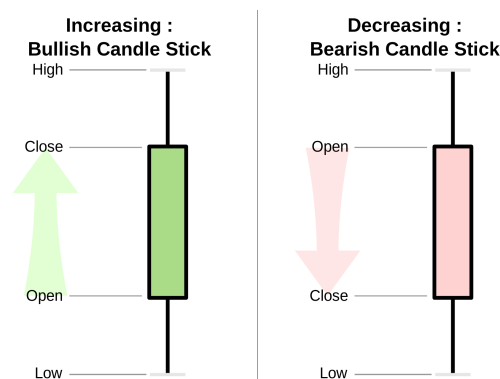
This is the “normal” way that market pricing works: people show up to a central place and make offers until they find agreement. The price at any given moment reflects the smallest amount that suppliers are willing to sell for, and the highest amount buyers are willing to pay.

Next, you have the “candlestick” chart showing how the price has changed over time:

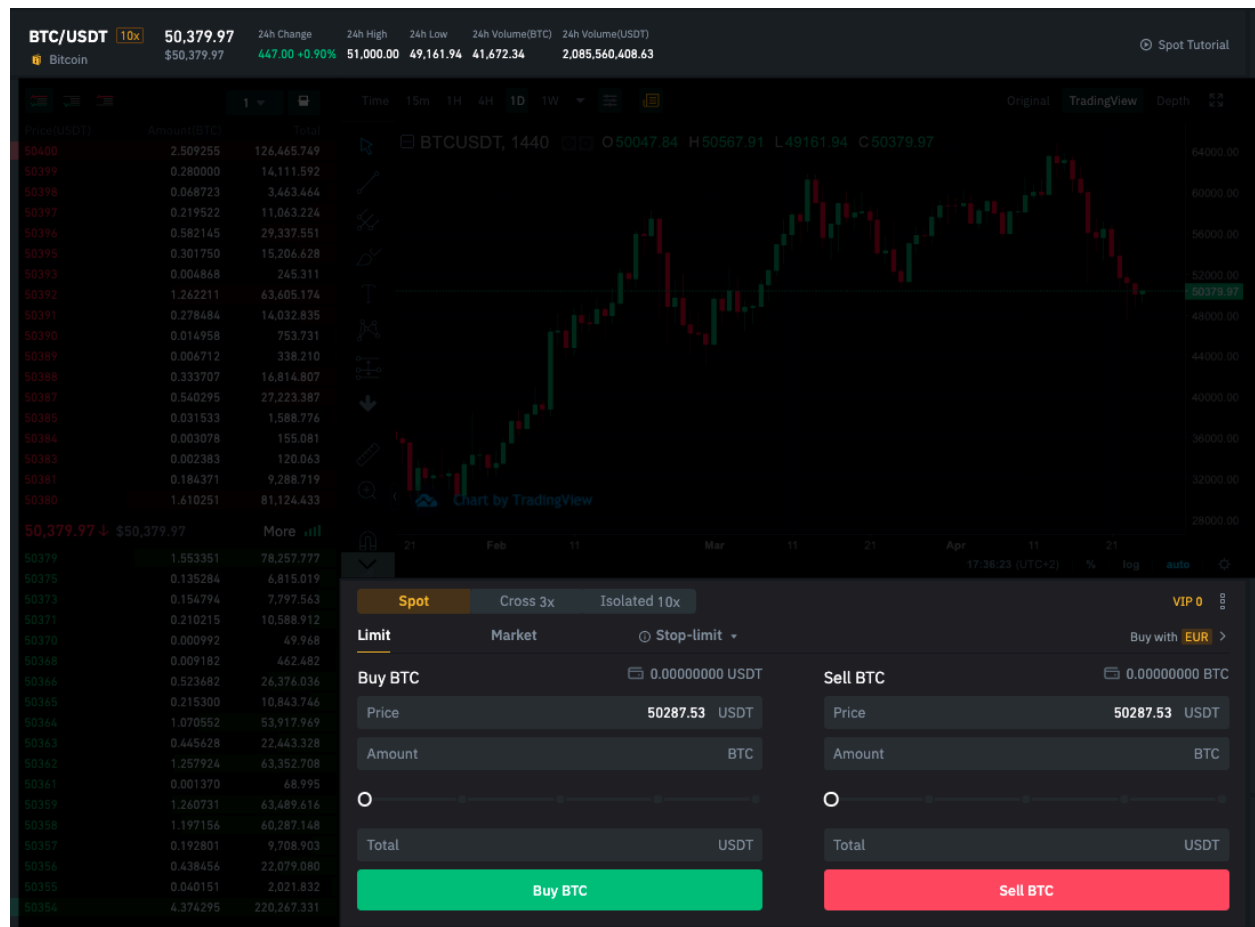


Each candlestick shows you how the price changed during a day. If the price is higher at the end of the day (close) than at the start (open), it'll be green. If the price is dropping, then the candlestick is red.

The “wicks” at each end show you the highest and lowest points the price reached during the day.



Finally, there are two order forms under the price chart:



This is where you can place your orders, either to buy or sell BTC. So you could say “I want to buy BTC and I’m willing to pay \$50287”. When you press “Buy BTC” your order will be added to the order book and it will stay there until someone is willing to sell for that price.

Stablecoins

Maybe you noticed in the previous example that the price was given in USDT instead of USD. That T stands for [Tether](#). Tether is a “stablecoin” that is pegged to the US Dollar. That means it always has exactly the same value as a dollar, but it’s a digital token so you can interact with it in the crypto ecosystem. There are many stablecoins: Binance has their own one called BUSD, and there’s [DAI](#) for people in the Ethereum ecosystem.

Decentralised Finance (DeFi)

Centralised exchanges have some shortcomings. Centralisation is a single point of failure: e.g. in 2014, the [biggest exchange got hacked](#) and 740,000 BTC was stolen from customers. The exchange also works as a gatekeeper, deciding which coins can be traded, and charging a fee for each transaction. They're also regulated by governments, e.g. you may have to prove your identity before transacting with them (this is due to anti-laundering regulations that require financial entities KYC = Know Your Customer).

So there have been many experiments with decentralised exchanges. People want to transact anonymously, without gatekeepers or regulation. Since about a year ago, the most popular approach to decentralised exchange is called a **"liquidity pool"**.

Unlike a traditional centralised exchange, a liquidity pool doesn't have an order book, you don't need to wait for a buyer and seller to meet and agree on a price. Instead, the price is determined by [a mathematical formula](#).

Instead of matching specific sellers to specific buyers, a pool contains a pair of coins, let's say ETH and HOT for example. If I have some ETH and I want to trade it for HOT, I can go to find an ETH-HOT pool and make the swap. These are both ERC-20 tokens, so I can find a pool on [Uniswap](#):

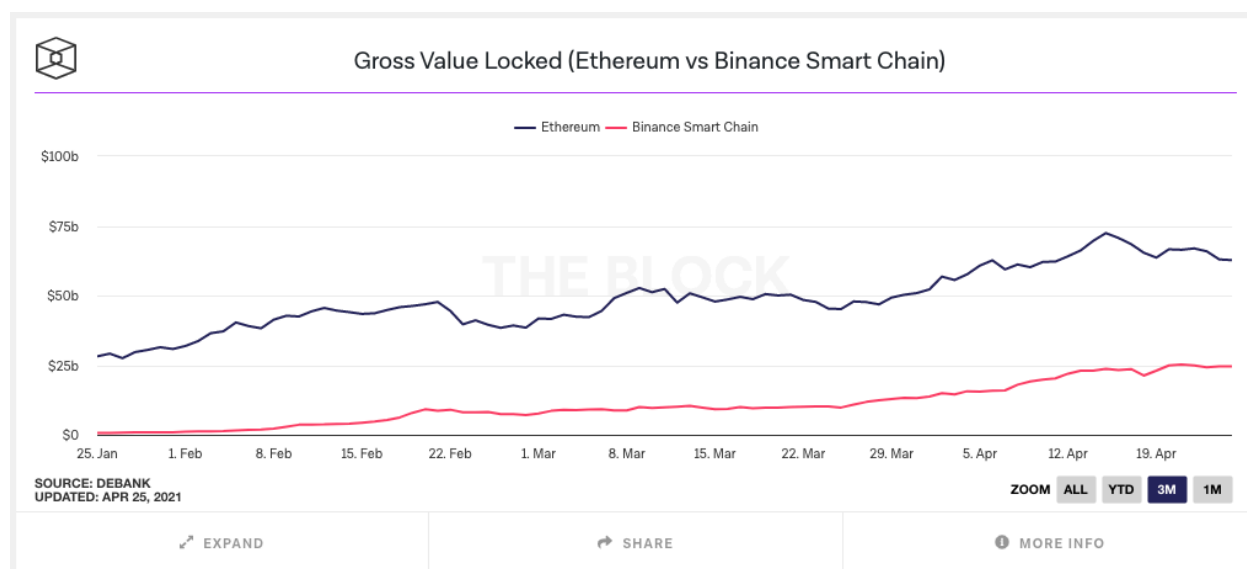


This pool currently has 75 million HOT tokens and 406 ETH tokens “staked” or “locked up”. If I had 500 ETH that I wanted to exchange, I couldn’t do it here, because there is not enough liquidity in the pool. So where does liquidity come from?

Other people who already own HOT and ETH are incentivised to add their tokens to the pool. If you own 1 ETH and 186,651 HOT, you could add those two coins to the pool and be rewarded with LP (liquidity pool) tokens. Whenever someone like me comes along to swap my ETH into HOT, you will get a fraction of the transaction fee.

So now you can be the bank: if you have some assets you can lend them out and earn “interest”, and apparently nobody can stop you.

There’s currently more than \$50B locked up in Ethereum liquidity pools, and \$25B in Binance Smart Chain pools, which only launched a couple of months ago ([source](#)).



Because of this rapid explosion of interest, and the extremely low barrier to entry, there are new DeFi platforms popping up every few days. For example, soon after Uniswap became popular, someone duplicated their code, dropped the fees by 20% and called it [SushiSwap](#). So how does a new DeFi provider find new customers? By offering ~~magic beans~~ incentives of course. They’re all competing to reward you with better profits, high rates of return and tokens of their own.

For example, right now on [Pancake Swap](#), if you contribute to the SUTER-BNB pool, they’re currently offering 1% returns **per day**. If you went back to the pool every day and reinvested your profits, you can expect about 48X returns after a year (assuming the rate stays constant, which is unlikely).

Yield Farming

There are so many opportunities to earn rewards for providing liquidity to DeFi apps, it could be a full time job just trying to keep up with the best deals. This job is called “yield farming”, and it used to be back-breaking labour back in the old days of 2020. Now we have automated tools that go out and search for the best deals for you, moving your coins around from one place to the next to earn the greatest rewards. For example you can give your money to [Yearn](#) and it will automatically shift it around between [dYdX](#), [AAVE](#), and [Compound](#) and find the best deals. If you had joined in the early days, you would have also received YFI tokens, which are [now worth 1000X](#) what they were in June 2020.

[This video](#) is a good intro to DeFi and Yield Farming.

If you have read through this far, maybe you have a similar feeling to me: this seems kind of absurd. Layers and layers of financial abstractions -- it starts to sound like the “collateralized debt obligations” and “credit default swaps” that triggered the Global Financial Crisis in 2008. These returns are “too good to be true”, so I’m expecting a massive crash sometime in the next few months.

However, if you can look behind all the hype, speculation, and gambling, I do believe there is some fundamental value being created underneath it all.

Introduction to crypto investing

If you want to gamble in the crypto space, here’s [my intro to investing](#).

Other things to write about

- Oracles
- NFTs
- Memecoins
- Projects that are not about money
 - IPFS
 - SSB / Planetary
 - Holochain
 - Mattereum
 - DisCO

(to be continued... [join my newsletter](#) if you want to be notified when I finished and publish)