Blockchain Thoughts & DeFi Economics

Photo by Pierre Borthiry on Unsplash

Blockchain Thoughts and DeFi Economics

Carlos Mercado

This book is a compilation of my thoughts and opinions on the economics and premises of decentralized finance. Nothing in this book should be confused for financial advice, I am not a financial planner. I will detail my own investments for disclosure where relevant and refer to 3rd party sites and articles for informational purposes only.

This book is for everyone who loves learning for learning's sake.

I hope you connect with me on LinkedIn and let me know what you think!

Carlos R. Mercado
Data Scientist | Economist | Blockchain Enthusiast
LinkedIn: linked.com/in/crmercado

Prologue

Hey, I'm Carlos. I wrote this because I've been studying the growing decentralized finance[1] market. Obviously, "everyone is a genius in a bull market"[2], but because of my experience as a freight broker (arbitrage[3]) and data scientist using open source[4] tools every day I really believe we have something here. There's something to the idea that software with fair, public, and auditable rules can give the regular person a fair chance to make money by investing in other regular people. That is the central premise of DeFi.

To put it more bluntly. If multibillion dollar companies are trusting their products to be built with public, audited, and open source programming tools (e.g., Python and R), is it so crazy to believe they'd put their money into public, audited, and open source financial protocols?

I don't think it's that crazy. At time of writing, MicroStrategy has literally billions of dollars in just Bitcoin[5] – the industry namesake.

I think a lot of regular people are missing out and (just like an IPO!) they'll be invited to the party late after the rich have gotten theirs.

---

[1] Covered later in better detail. But for now, Decentralized Finance ("DeFi") is the idea that money not spent on goods and services (i.e., "saved" money) can be invested (so it grows) without using a bank, brokerage, or other *centralized* business.

[2] Bull market means there is an optimism of "everything is going up!" (bull runs forward), while *Bear* market means there's a pessimism of "everything is slowing down!" (bears stand up). Dot com bubble, 2005-2007 housing bubble, and the 2009 – 2019 impossibly low-interest rate bubble – are "Bull markets". It's not just about being *in a recession* or not, it's about the general *feelings* about the economy (and yes this is real – google Consumer Confidence Index).

[3] Make money by being "in between" sales. Person A is selling X for $4 dollars, Person B wants X and has $5 dollars. You buy X from A, sell it to B, and make $1 in arbitrage. This is technically how Foreign Exchange (ForEx) works too, except that market is what economists call *rivalrous*- for someone to win, someone has to lose. Whereas stocks and (as you'll learn) cryptographic assets are not rivalrous. The market can simply, grow for everyone involved!

[4] In programming today, Open Source means computer programs available for free online. These programs are *literally better in almost every way* than paid programming tools because they have entire communities coming together to both volunteer their time in improving them and sharing their problems for others to solve- constantly making the tool better. You'll understand in this book that centralized finance is under the same risk today.

[5] They have over 70,000 Bitcoin as of Dec 21, 2020.

Section I: Foundations

This section covers foundational elements of Finance and assumes only elementary math and a willingness to Google anything I don't explain in the footnotes.

What is Finance?

There's this really cool site called WordNet[6] that uses a bunch of fancy Artificial Intelligence and Natural Language Processing (i.e., throw math at words) to identify all possible definitions of a word in common usage.

Here's what it returns for a search of Finance:

WordNet Search - 3.1
- WordNet home page - Glossary - Help

Word to search for: finance [Search WordNet]

Display Options: (Select option to change) [Change]

Key: "S:" = Show Synset (semantic) relations, "W:" = Show Word (lexical) relations

Display options for sense: (gloss) "an example sentence"

Noun

- S: (n) **finance** (the commercial activity of providing funds and capital)
- S: (n) **finance** (the branch of economics that studies the management of money and other assets)
- S: (n) **finance** (the management of money and credit and banking and investments)

Verb

- S: (v) **finance** (obtain or provide money for) *"Can we finance the addition to our home?"*
- S: (v) **finance** (sell or provide on credit)

Don't worry about the fancy references to semantic whatever, just appreciate that this word has both verb and noun meanings.

Finance is *commercial*[7] activity that involves the management of *money*[8] including lending it to others.

---

[6] Princeton University "About WordNet." WordNet. Princeton University. 2010.

[7] Goal is to make money.

[8] Object accepted as payment – and some other definitions we'll get to later.

Let's start from the beginning.

(1) People make money, typically at their jobs[9], and they can either spend it or not spend it (i.e., save it).

Typically, people get money from their job as a *flow*, that is, they get a certain amount at a defined time interval. This is as opposed to a *stock* which instead has a static value. Note: I did **not** say a stock has a static *dollar* value; just that it has a static value. That value might be 1 billionth (1/,000,000,000) of Google[10].

(2) When people want to save money, they have options:

- Hide it under their mattress – and risk loss to *inflation*[11].
- Lend it to their friends and family - possibly with interest.
- Convert their money to another asset – possibly as an *investment*[10].

(3) What's the difference between interest and an investment?

An interest *internalizes* trust and is thus *illiquid*[12]. You lent the money to your friend and you probably didn't write up a contract. Even if you did get them to sign an IOU paying 20% extra as interest- people who don't know them won't trust they're good for it and wouldn't buy that IOU. This loan is *not* an investment.

An investment *externalizes* trust and is thus *liquid*[13]. There's a contract and if the terms aren't met, you can use the government's power to enforce the contract. This means people will generally trust a stock of Apple will entitle them to some function of Apple's profit,[14] even though they don't actually know anyone who runs the business.

---

[9] If you *work* for money it is called labor. If you own something that makes money, it is called *capital*. You may have heard the phrase *capital markets*.

[10] Worth ~$502 on January 4th, 2016 and ~$1,221 on January 4th, 2021

[11] Things have static values. An apple is worth an apple, A stock of Apple is worth a stock of Apple. But things change in **price**. Typically, an apple and a stock of Apple both go up in price over time. When an investment goes up, people are happy, but when the cost of food goes up, they're mad. Inflation is when things go up in price and you're mad about it (food, healthcare, education, toys, haircuts). Investment is when things go up in price and you're happy about it (your stamp collection, your baseball cards, your 401k).

[12] Hard or even impossible to convert into a different asset (nobody wants your friend's bar napkin signed IOU).

[13] Possible or even easy to convert into a different asset (you can buy/sell stocks near instantly nowadays).

[14] Liquidity is a spectrum. Nice watches, gold jewelry, etc. can be readily sold at pawn shops or flea market. That makes them more liquid than a house (takes months to sell) or a beanie baby (very small market for it).

(4) How do people *defend* against inflation and *seek out* investment opportunities?

A. People defend against inflation by buying assets (things) that go up in price too.

If I only eat hamburgers and the price of hamburgers is going up 2% a year, I would *love* to buy hamburgers while they're cheap and eat them later when the price goes up but hamburgers spoil. So instead, I have to store money until I want a hamburger later. *Money* is an object that is countable[15], accepted in exchange for goods (hamburgers)[16], and doesn't spoil[17] (as fast as hamburgers).

But inflation *spoils* my money, just like bacteria spoils my hamburgers.

So even if I keep my money in a Ziploc bag under my mattress (or in a bank paying almost 0% interest) I am always losing potential future hamburgers as the price of burgers goes up and I get mad. But I can hack this problem by *buying things that go up in price equal to or faster than hamburgers*[18].

B. People seek out investment opportunities by understanding markets.

In any market (beanie babies, baseball cards, gold, stocks) there are interplays of supply and demand. Generally, there will be a somewhat fixed and known supply. Then demand for that supply is a function of:

- Direct rewards for holding the supply. For stocks this is called *dividends*[19].
- Overall activity (and optimism!) in the market – more participants mean more potential buyers and sellers which means better liquidity which makes the "market" price easier to find.[20]

If you think something is going to go up, you can buy it low and sell it high. If you think something is going down, you can bet against it[21]. If you notice that different markets have different prices for the same thing – you can do arbitrage.

---

[15] Fancy word: Unit of account.
[16] Fancy word: Medium of exchange.
[17] Fancy word: Store of value. <- The Mark Cuban article I cite later is a good read on this.
[18] Even if McDonalds won't accept my gold for burgers; as long as I can trade gold for money in the future, gold becomes an *investment* that allows me to maintain (or even exceed) my number of desired burgers in the future.
[19] Dividends are a *flow* of payments as an entitlement from owning a piece of a company. In stock theory, the "true" stock price is the net present value of its future dividends. Don't worry if you don't know what NPV is.
[20] Fancy word: Price discovery – does **not** always mean things go up.
[21] Check out the GameStop saga for some interesting reading on *shorts*.

What is Blockchain?

When you make certain investments, let's say a house for example, there is a paper trail (almost always *literally paper*[22]). The ownership of land, assessment of property taxes, and the value of the building on the land are all tracked by city, county, state, and federal authorities that ensure they are providing services (water, electricity, police protection) to and taxing (property, sales, usage fees) the properties in their jurisdictions.

Generally speaking, this information is publicly available. I could go out right now and identify the owner of my neighbor's house, the last sold date, the last sold price, the estimated property tax, and other information on that home. That's a **good** thing because it improves information symmetry[23]. It's useful to me to understand my home's value and to the government to assess changes in my property tax (has my neighborhood become way more popular?).

The problem is the *literally paper* part. Blockchain is a cryptographic methodology that manages a database (called a chain) comprised of blocks (sets of information) while connecting the blocks back to back in such a way that the *metadata* of the blocks are cryptographically tied together.

Imagine a housing market. There's homes and they have owners. The paper system treats all the homes individually- the sale of a home becomes new paper added to the pile. The blockchain system can treat each home as a block (of data) and each sale of a home becomes a new block added to the chain that details previous owner, sale price, new owner, new property tax assessment, etc. The interesting thing about blockchain is that the system is immutable. In a paper system, if the sale price has an error, you just go to that home's file, fix it and alert the bank and the property tax office. In a blockchain, fixing that error requires a new block (detailing that a previous block is incorrect). This means you

---

[22] Papers get lost, mis-filed, damaged, experience typos, etc. It's painfully archaic and distributed ledgers (the "fancy" I'm not a bitcoin crazy, I'm a real businessperson word for blockchain) can solve this problem.

[23] In markets, when buyers (or sellers) know more than the sellers (or buyers) it is called information ***a****symmetry*. This is a big deal and is highly regulated by governments- think Lemon laws for used cars or Insider Trading laws for stocks. In fact, I would consider the regulation of information asymmetry in markets to be a **foundational purpose** of government itself. But we'll get to that later.

automatically have version control[24]. There is (almost) never[25] an instance where you can go back and change previous transactions because **blocks are cryptographically linked**.

Ok, so read the footnote on version control and then let me explain the cryptographically linked part.

House A Owned by: Sade hash: 023dfsdkf044	House A Sold to: Bill hash: F(023dfsdkf044) => 0xdsfk30r343

Sade owns House A. She decides to sell it Bill. The chain gets a new block, and that block gets a special ID number called a hash. The interesting part is that the ID is a **function** of the previous IDs. Sade's hash 023dfsdkf044 gets combined with some of Bill's data (the date of sale, the price, the owner's name, etc.) and a new hash is outputted: 0xdsfk30r343. If Bill sells that house ***or*** if another house sells (let's say in the County if it's a County level chain being tracked) that new block will be a function of Bill's hash because his block is most recent on the chain.

The idea here is that instead of houses being individual files of paper dispersed across a bunch of banker and government office desks. The *relevant market* becomes a blockchain and all transactions are permanently recorded *on chain*.

Now here is the biggest big brain part of the whole technology.

---

[24] Version control simply means that you have the full history of something, including changes. So, for a word document that can mean I have every title, every heading, and every paragraph that I have ever had at some save point. (Let's say I hit the save button every day). Then if I erase something or work on the document for a few weeks and wish I could go back and get an old paragraph I deleted (maybe 2 weeks ago) – *I can* – I simply look at the version history and find that paragraph from 14 saves ago and copy/paste it to the current version.

[25] There's some crazy stuff around 51% attacks, forking a protocol to repair damages, and other things you might want to be aware of at a high level. But the truth is *the chain is secure* – it's concentration of the *power to control* the chain that is risky, and you'll hear a lot about certain protocols "having backdoors" or "admin keys" that defeat the whole point of, well you know, *decentralized.* I'll cover this lightly later but it's out of scope of this novella to give you FUD (fear, uncertainty, doubt) before you're even decided on whether you're interested in this technology. Suffice to say, there are *already* blockchains that are decentralized enough to not have these problems and you can definitely find opportunities to engage with cryptographic assets at a variety of risk tolerance levels and I encourage you to define your risk tolerance and stick to it! Like you would with any set of stocks or properties, etc. But be prepared, low risk can mean low reward especially in the early days of this technology (and maybe more important: high reward should assume high risk!).

House A Owned by: Bill hash: 0xdsfk30r343	House B Sold to: Andre hash: F(0xdsfk30r343) => 5994fr3kd034

Because block hashes are **functions** of the previous block hash, an effort to change a past block requires the successful forgery of **all blocks after it** in such a way that the hash IDs perfectly line up.

To change Andre's block would require changing Bill's block, which would require changing Sade's block. But because Bill's hash is a **function** of Sade's hash you have to perfectly alter the data such that Sade's block spits out the same exact hash for Bill.

This is a nearly impossible cryptographic problem[26]. We have a system that doesn't have fraud, meaning it is *trustless*. You don't have to trust anyone that Sade was the owner before Bill. It's on the block, all the information is public, it wasn't changed because it can't be changed.

This does not solve all problems of course:

1) Incorrect data put into the block stays there until updated on a new block.

2) People can try to change the *entire chain,* which is trivially easy compared to solving some of the hardest cryptographic algorithms available today.

Now, if you read my "(almost) never" footnote above you might be wondering about that (2) caveat. Well, this is where our blockchain gets both more complicated and more secure. The blockchain isn't recorded on a single computer. That would be *centralized*.

[26] Try it out for yourself. Click this link and type any sentence into the SHA-256 algorithm. Record the sentence and the hash. Then try to make a new sentence with the same exact hash. If you find a pair, it's called *a collision* – and while extremely rare, weaker algorithms have been found to have collisions. But a single collision doesn't actually "defeat" the algorithm at all, it's just 1 weak point. And finding even a single collision in some algorithms are estimated to take thousands of years of our best computers trying 24/7. To defraud our tiny example chain would require finding 2 collisions (1 for Sade -> Bill, 1 for Bill -> Andre). Many blockchains have millions of blocks.

The blockchain is duplicated across all participating computers[27]. The rules on how a computer chooses to participate vary, for now, just know that participating in a blockchain cost you something (computing power, electricity)[28] but gives you rewards. Not everyone has to participate to gain from crypto assets- just like not everyone has to form a company to buy a stock. But it's a real way to earn money and it is relatively the lower risk since it's trading honest (computer) work for honest (digital) pay[29].

For an update to the blockchain to be accepted, there must be *consensus* among the participating computers. This can be as simple as:

Computer 1: "hey my calculation says the Bill's hash should be 0xdsfk30r343, given the following Sade parameters do you also get this hash?"

Computer 2 – 99: "Yep, confirming that the parameters you gave lead to that hash and that those parameters are correct given my instance of the blockchain".

Computer 100: "No way man, my chain is totally different".

Here, Computer 100 could have fraudulently changed their entire chain. But because the system is *decentralized* Computers 2-99 have no reason to support Computer 100 because Computer 1's chain matches their chain history and successfully moves the process forward by having solved the current block problem. If the owner of Computer 100 also owned Computer 49 – 99; then we might have a problem…

---

[27] Yes, this is a lot of database storage; but it's a massive security boost and with smart contracts, which we'll get to later, it's an entirely new way to think about shared computing.

[28] There are other methods other than proof of work; a popular one is proof of stake. You can google these later.

[29] In Bitcoin you participate by becoming a *miner* – this means you contribute computing power to solve the cryptography needed to add blocks to the blockchain (i.e., calculating Bill's hash given his and Sade's block info). In exchange for paying the computing cost to add to the blockchain, you are rewarded with (a chance to get) Bitcoin! I say a chance to get, because technically it's a competition, people with better computers will solve the cryptography first, more often, but you can still win occasionally. The marginal cost of earning a bitcoin rises over time based on the actual codified rules of the Bitcoin protocol. You can read the famous Bitcoin white paper if you're interested in details but suffice to say, it can cost several thousand dollars to mine 1 bitcoin, but it's worth it when the price is $30,000+ (at time of writing).

Why are people crazy over Bitcoin?

Context. It's the late 2000s. The financial industry has effectively collapsed in the average person's mind (some "buy the dip" and make fortunes later). A Japanese man, Satoshi Nakamoto, releases a white paper explaining how cryptographic hashing of transaction timestamps solve the double-spend problem in digital payments **without** reliance on a trusted 3rd party.

This is where you click the link in the Bitcoin footnote, read the 1 paragraph abstract, and say, "alright sounds fancy but explain it to me like I'm 12".

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

If I have $100 and want to buy something on the internet, I can use an online service like PayPal to interface with my bank to take and hold my money. This trusted intermediary tells the seller they have my money, and the seller sends me my purchase. Then the seller gets paid.

Without PayPal in the middle as the *trusted* 3rd Party I could buy 10 things for $100 each, give the same bank info to each seller, and then get my 10 things before the individuals had sorted out with the bank who actually deserves what. This transaction delay (it takes time to transfer money and update accounts) allows me to *double-spend* (here, 10x spend) the same amount of money and defraud people.

Bitcoin's public blockchain uses cryptographic algorithms to link together blocks of information, while resisting fraud, through *proof of work* and *decentralization* of participating computing power. If the system is sufficiently decentralized such that 1 coordinated group does not control 51% of the system– we *no longer have to trust any one individual or designated 3rd party* to transfer money to each other. You can't double spend because everyone knows exactly how much you have, how much you had, and how much you will have upon completion of the next block of transactions.

Attempts to double-spend fail because it's trivial to add up how much you had, have, get, and spend; you simply do transactions grouped together on blocks and any blocks that don't pass these rudimentary tests don't get added. The transactions don't occur and people don't ship what you tried to buy.

If we accept the premise that this transaction network has value, it's pretty quick to realize why Bitcoin is the new gold. People mine bitcoin by participating in the cryptography, they convert their rewards into other assets (e.g., money), and people willingly convert their assets into bitcoin because it has a full digital history proving their ownership and the market for it is robust.

There's a lot of haters and their #1 argument is, "how is this different then beanie babies" – which is a **great** argument. Bitcoin doesn't *do* anything besides record its creation, its ownership, and its transfers perfectly[30]. The market values these properties and thus values bitcoin[31].

[30] Technically it can do more than just this but not well enough for it to be widespread the way smart contracts on Ethereum (covered later) have become widespread.

[31] Check out this great article my Mark Cuban, billionaire investor that you may recognize from the show Shark Tank and owner of the Dallas Mavericks basketball team, i.e., someone who knows what they're talking about when it comes to investments.

The weaker hater arguments tend to rely on perfect solution fallacies – the idea that because something *has a flaw* it cannot *have value*. This is of course preposterous when you recognize the argument. Here's a few:

- It's not real, I can't touch it, it's worthless.
    - There are some really interesting frameworks for understanding value. Some from the historic economic literature include labor theory of value and cost theory of value. Generally, in modern economics, we consider things to have value based on the market for their use. People use Bitcoin and are willing to pay for it, thus it has value just like a mint condition baseball card has value to people who want to own it and look at it. The argument we're just collecting digital Ponzi stamps is a solid one worth considering by any potential owner of Bitcoin. It's about the belief in the fundamental technology, not the belief in some token given as a reward for participating.
- If the internet goes away this is worthless!
    - The chain exists on the participating computers not in some internet void, their inability to talk to each other is a massive problem, but presumably people will try and get the internet back. If the internet disappeared forever, bitcoin would not be the most pressing problem. I'd mark this as a *denying the antecedent*[32] fallacy or possibly even a *modal*[33] fallacy. As blockchains can exist within defined enterprises, bitcoin's problems don't really say anything about the future of blockchain as a technology and you could fork bitcoin on a local access network (LAN) in minutes at anytime and just continue on a non-internet connected sub-chain.
- If electricity disappears this is worthless!
    - Bro, please, be reasonable. Our whole lives rely on electricity LOL.

---

[32] Denying Antecedent: *if A, then B; not A, therefore not B*. If Internet, then Bitcoin value, no internet, then no Bitcoin value. This is neither fundamentally nor mechanically true, although it is troublesome.

[33] Modal Fallacy - Because Bitcoin arose from the internet and the internet doesn't naturally create bitcoin, no internet means no bitcoin. You could have bitcoin using LAN or even just as a methodology written on paper if you had a custom hashing algorithm. It's about the technology and methodology, not the specific implementation.

Why decentralization?

Alright so now you get that decentralized, consensus / proof based cryptography makes the record-keeping secure. You lightly agree that people value this secure method of recording transactions and thus there is some value here (maybe in your opinion not $30,000+ but you can see how people would pay non-zero dollars for it). Let me throw some reminders of our privilege into the mix so you can really understand the global scope of this technology.

I live in the US. Probably the country with the most robust financial systems in the world- the dollar is the global reserve currency[34], all the big companies that do multinational currency exchange and financial transfers have bases here. Why would I of all people care about this stuff? My bank account is FDIC insured, my 401k is in the most trusted variety of stocks, inflation is relatively low[35]. What gives?

The vast majority of the world's population does not live in this situation. Their governments can freeze their bank accounts[36], limit their ability to engage in capital markets[37], inflate their currency which erodes their real wages[38], and just overall put them in a really bad financial situation.

The global decentralization of finance means that individuals will be able to engage in *commercial* activity **directly** with other individuals **without trusted 3rd parties** (e.g., banks that follow the rules imposed by the relevant governments of the jurisdictions they do business in). This is a huge deal. Obviously, it has its pros and cons.

Cons: Easier and more anonymous funding of terrorism, human trafficking, drugs, and other really terrible things.

---

[34] At time of writing.

[35] The astute reader will note the author has not indicated a very strong belief in this one.

[36] At time of writing, Nigeria has forbidden banks from engaging in the crypto market, including working with any exchanges and freezing accounts that engage in the activity. India has made similar efforts.

[37] Argentina has consistently suffered currency control issues over the past 50+ years. They heavily limit the ability of citizens to purchase the more secure US Dollar.

[38] Real wages are "what can I actually buy with my labor". In 2000 an hour of work at McDonalds got you 2 Big Mac Meals. Now it only gets you 1. Recall the definition of inflation, "when price goes up and you're mad" vs investment "when price goes up and you're happy".

Pros: Easier and more efficient funding of new small businesses, more freedom for individuals in their economic choices[39], more competition can reduce prices or improve quality of goods and services.

The blockchain technology itself, entirely separate from the finance benefits, also offers a complete overhaul for record-keeping in complex multi-agent systems where trusted 3rd parties don't feasibly exist. Think healthcare[40] or supply chain management[41].

When you get into the scale of thousands of suppliers intersecting millions of unique products there is no singular entity that is tracking the supply chain of both its own supply and the supply chain of its suppliers. Major enterprises including governmental agencies are exploring blockchain as a solution to these problems.

I want to focus this on the finance implications foremost. But nobody should take away from this tiny book that finance is the only relevant use of this technology. It's probably the opposite. Do only banks use relational database management systems (RDMS)? Of course not. It's an off the shelf service available from numerous competing vendors and in use by nearly every business that collects data. Blockchain will both open up new technology opportunities and replace some current technologies that are not suited for complex multi-agent, trustless, record-keeping and information (or asset) transfers.

---

[39] This is where we quickly get into moral and philosophical debates. I'll try to avoid them, but I do want to leave the reader with a tough one. Should a North Korean person, who had no choice in their location of birth, starve simply because their government is sanctioned for nuclear efforts that they have no power to stop? One prominent developer will likely go to jail over their efforts to enable these people to participate in decentralized finance and thus circumvent sanctions. I'm not in a position to comment on whether the sanctions are rational or are actually working in terms of reducing nuclear proliferation. But the economic literature finds that sanctions injure the everyday population – which *in a functioning governmental system* should lead to changes in government policy. Without a functioning governmental system, I am unsure how sanctions, crypto, and DeFi should go together, but I will watch carefully as countries independently navigate this future.

[40] Electronic health records where the same individual may have records at several disconnected hospitals. This is a nightmare for patients who have learned to expect that their purchase histories and web information should follow them easily just website cookies. Our healthcare system has some catching up to do on people's expectations of technology!

[41] If you're skeptical about any of this because you just frankly, plainly, don't care about finance at all, skim this site on IBM enterprise blockchain for tracking food from farm to retail with Walmart.

What is the future?

I mentioned earlier What is Finance? that people find investment opportunities through understanding markets. Here's the quote again,

If you think something is going to go up, you can buy it low and sell it high. If you think something is going down, you can bet against it. If you notice that different markets have different prices for the same thing – you can do arbitrage.

It gets a lot more complicated than just that. There are derivatives (side bets that a stock will go up or down, without actually buying the stock), indexing (buying groups of stocks such that the overall index grows with less volatility than any individual stock in the group), high-frequency trading (owning a stock for just 1 second or even just a fraction of that). The vocabulary words are endless: short, squeeze, delta, gamma, put, call, option, hedge, etc.

What I want to impress upon you though is- other similarly complex technologies were entirely centralized like finance[42]. If you wanted to analyze data with really good statistical methods, you shelled out $10,000s in licenses for SAS. If you wanted to a way to click around on a computer instead of typing 10101001001 you had to pay for an operating system and programs. Today operating systems like Unix, programming languages like R and Python, and entirely free computer programs like Gimp (picture editing), OBS (video recording), Android (phone operating system), QGIS (geospatial analysis software), and tons of other tech in a wide range of industries is available totally free supported by donations, volunteers, and in some cases even corporations sponsoring volunteers.[43]

So, suffice to say, open source is upending industries and growing immensely. But how does this relate to the future of finance / financial technology?

Remember when I said Bitcoin doesn't *do* anything. Well, Ethereum[44] *does*.

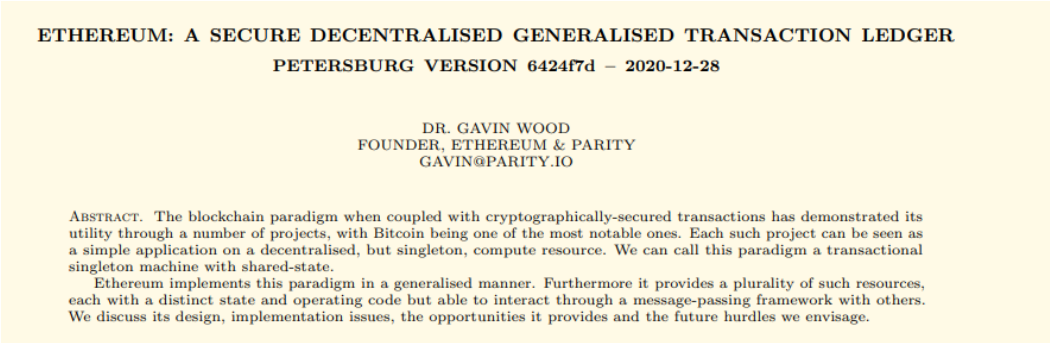
---

[42] This is a slight, but purposeful inaccuracy. Much like finance existed prior to banks, the history of software starts with a very wide open era of open to the public software. It took a few decades for the commercialization and centralization of software to grow into what it is today, much like it took centuries for the Medici Bank to formalize an entirely new way of tracking money – debits and credits in a double-entry ledger.

[43] The list of open available software is mind-boggling in its range of domains.

[44] For more, check out Ethereum including the Yellow Paper and the openly available book: Mastering Ethereum.

Ethereum is a different blockchain than bitcoin but it similarly uses blocks and tokens and cryptography, etc. But Ethereum has a unique innovation. Dr. Gavin Wood, founder of Ethereum details that Bitcoin is a decentralized application running on a single compute resource, perfectly tracking its own state and history. Ethereum seeks to be the generalized version of this- running any amount of computer resources all recording their own states and histories and sharing such information under defined conditions.



ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER

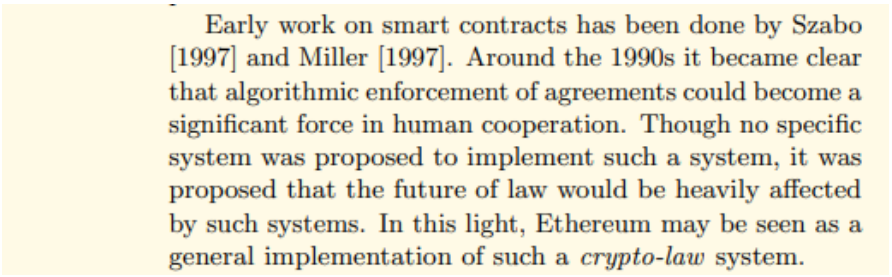
PETERSBURG VERSION 6424f7d – 2020-12-28

DR. GAVIN WOOD
FOUNDER, ETHEREUM & PARITY
GAVIN@PARITY.IO

ABSTRACT. The blockchain paradigm when coupled with cryptographically-secured transactions has demonstrated its utility through a number of projects, with Bitcoin being one of the most notable ones. Each such project can be seen as a simple application on a decentralised, but singleton, compute resource. We can call this paradigm a transactional singleton machine with shared-state.

Ethereum implements this paradigm in a generalised manner. Furthermore it provides a plurality of such resources, each with a distinct state and operating code but able to interact through a message-passing framework with others. We discuss its design, implementation issues, the opportunities it provides and the future hurdles we envisage.

This infrastructure sets up Ethereum Virtual Machines to allow *code* to run based on the state of the blockchain. This self-executing code enables *smart contracts*[45], the "algorithmic enforcement of agreements".



Early work on smart contracts has been done by Szabo [1997] and Miller [1997]. Around the 1990s it became clear that algorithmic enforcement of agreements could become a significant force in human cooperation. Though no specific system was proposed to implement such a system, it was proposed that the future of law would be heavily affected by such systems. In this light, Ethereum may be seen as a general implementation of such a *crypto-law* system.

Over twenty years ago when this technology was first being thought about, they referred to it as a type of cryptographic *legal system.* Serving the function of government, we discussed in What is Finance?:

There's a contract and if the terms aren't met, you can use the government's power to enforce the contract.

[45] The Wikipedia for Smart Contracts is super cool, but technologically, you can safely think about it as a more complex vending machine but in the cloud.

So, we've identified 3 foundational elements of government so far: regulating information asymmetry to keep markets fair (lemon laws), creating money to keep markets liquid (medium of exchange), and getting involved in contracts to keep markets functional (externalized trust).

Putting it all together. This new technology maintains public, immutable records (no information asymmetry), generates assets through the efforts of participants (creating money), and at least one technology has self-executing code that can enforce contracts (transactions can cause actions that are enforced algorithmically like *crypto-law* – externalizing trust).

It sounds like the future is going to have automated government.

This is useful both publicly in finance and privately in enterprise blockchains that can have automatic actions depending on defined triggers. Given the Ethereum programming language Solidity you could be on the ground floor of this movement and get a job of the future!

More radical though, is the idea that people could *create enterprises* that are governed algorithmically. Imagine 100 average people wanting to pool together money to form a business[46]. Those people could pool in different amounts of starting capital and then get weighted votes based on how much they put in. They could then agree on a governance system (e.g., weighted democracy or a type of republic) that would enable them to make decisions for the business as a group – with perfect recordkeeping of all votes.[47]

These are starting to form today and are known as *Decentralized Autonomous Organizations* (DAOs). This is the natural decentralization of what one may call *centralized* autonomous organizations[48]. Where an enterprise is still hierarchical and centralized, but the business units are loosely coupled. This is how a lot of modern tech companies are structured and, almost like a premonition, we're seeing states become more open to technology companies forming their own local governments[49].

---

[46] Something financial like a hedge fund may be the easiest to think about but it could be any business.
[47] This starts to get really interesting when you think about things like cloud kitchens and how business decisions can be made with more stakeholders and give those stakeholders more liquidity.
[48] I absolutely love this article on Zhang Ruimin's (CEO of Haier) opinion on bureaucracy.
[49] Anyone trying to live in Facebook, Nevada?

Section II: Thoughts

Section II applies the foundations set beforehand to discuss the why, how, what of all this stuff. I should note, that to stay within my page limit goal, I've had to skip a lot of important mechanics of actually investing in the space. So, let me do a brief run through of *stuff I trust you can handle with Section I, the footnotes, and Google:*

- Remember Sade selling her house to Bill? Well, there might be multiple Bills. In reality, "Sade" and "Bill" would be crypto wallet[50] addresses that uniquely identify each of them. Wallets can receive from any other wallet, so always double check who you're sending stuff to[51].
- That fancy options, hedge, short, put, call, finance derivative stuff now exists in DeFi. Something I glossed over in the Ethereum section is that *smart contracts* by being self-executing code written in Solidity (effectively a tweaked JavaScript) enable *decentralized applications*[52]. You can use Ethereum virtual machines to run applications using other people's computing power as long as the application has mechanisms to collect and pay *ether*, the "gasoline" of the Ethereum network, that is used to pay people for their computing power.
- I've said *work* and *miners* throughout this; please review the footnotes and feel free to look into other *proofs* such as *proof of stake* which will be increasingly in the crypto news as Ethereum attempts to pivot from proof of work to proof of stake enabling them to do faster transactions and handle larger applications.

---

[50] A wallet stores public and private keys enabling someone to sign off on blockchain updates (transactions). Typically, you request a wallet, you get a set of pass-words (12 is typical) – **anyone who knows those words is effectively YOU in the blockchain.** Those words hash to your private key which is how a wallet proves itself and signs off on transactions. Because this system is ***decentralized*** nobody can save you if you lose those 12 words. There are of course numerous services out there to remember those words and give them to you upon some password or identification. But then you're just centralizing again lol.

[51] Much like website addresses and the domain name service- Ethereum wallets can have Ethereum name service.

[52] Literally an application in any sense of the word, but instead of running on Amazon Web Services, it runs off the blockchain. If you feel I've been overhyping you – definitely read up on Cryptokitties a decentralized cat collection game that showed the difficulties of scaling decentralized computing on public blockchains. Amazon just spins up new servers on demand and charges you at the end of the month; but these blockchains are limited by their participants, the computing power provided, and the *gas* (ether for Ethereum, but there are other blockchains!) paid by the person to use the app.

Finance is Freedom

Think about retirement. See yourself as retired. Are you old? How old? 65+? Why did you make your vision of your retired self like that?

While it is true most of the world for most of history worked until they died or couldn't work / relied on family. It doesn't have to be that way for those of us privileged enough to live in place with functioning economic mobility[53].

And even if you *want to work* until you can't - whether it be for the sense of identity, protestant work ethic, or otherwise- it's financially prudent to live below your means and save for a rainy day.

For me, I see retirement as the *final phase of my working life*. Now, we culturally associate that with *not working*. But I argue we should reframe it as *having separated work from survival*. When you must work to survive, frictional unemployment[54] is risky. You tank[55] bad bosses, bad pay, no growth, no hope and possibly even harassment and abuse.

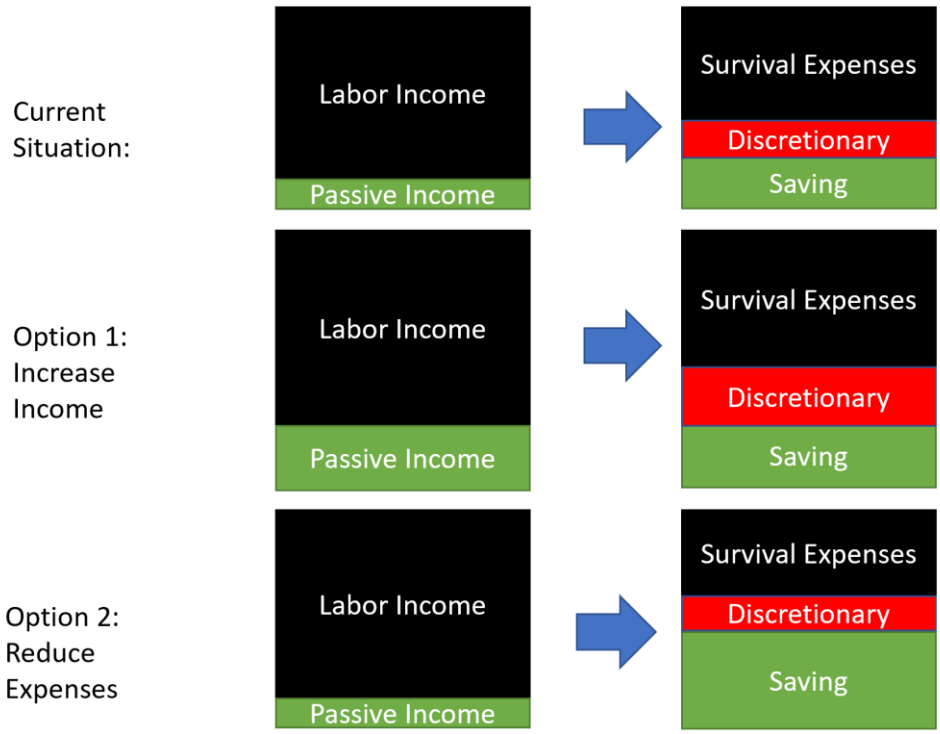
When you reach financial independence[56], you can freely enter and exit the labor market at will. There is of course a spectrum to this stuff:

Level 1: Paycheck to Paycheck	Level 2: Have emergency fund	Level 3: Financially secure	Level 4: Financially independent
One emergency and you're destitute, changing jobs is too risky (even if it pays more).	Could withstand some emergencies, might even be able to change jobs and miss a few paychecks for the right opportunity.	Can withstand most emergencies, change jobs at will, or even be unemployed for a 1+ years with minimal fear.	Can withstand most emergencies, freely enter/exit the job market, possibly never work again and live exclusively off passive income.

[53] For the economics inclined, there are actual numerous types of economic mobilities.
[54] For the economics inclined, there are numerous types of unemployment.
[55] Slang for endure. I use this word constantly because I played too much RuneScape as a kid.
[56] I cannot recommend this enough, the FI and FI/RE communities on Reddit literally change lives every day. Although be aware the selection bias is crazy. Don't beat yourself up for not being a 200k/year software dev in CA at 23. There's a lot of that stuff. Just focus on the fundamentals, safe withdrawal rate, living below your means, etc. I believe in you!

I argue that everyone's goal should be to become financially independent as much as possible and as soon as possible *regardless* of their desires or perceptions of the dignity of labor[57].

To keep it simple, here's a few small flowcharts.



I'm going to assume you, reader, are at level 2. You have an emergency fund, you could survive several months, but maybe not an entire year without work, you are generally feeling solid but know you can do better. Why else would you be here?

Financial independence is possible for you. It is as simple as making the green *Passive Income* box as large as your black *Survival Expenses* box – and hopefully the red Discretionary[58] spending box too.

---

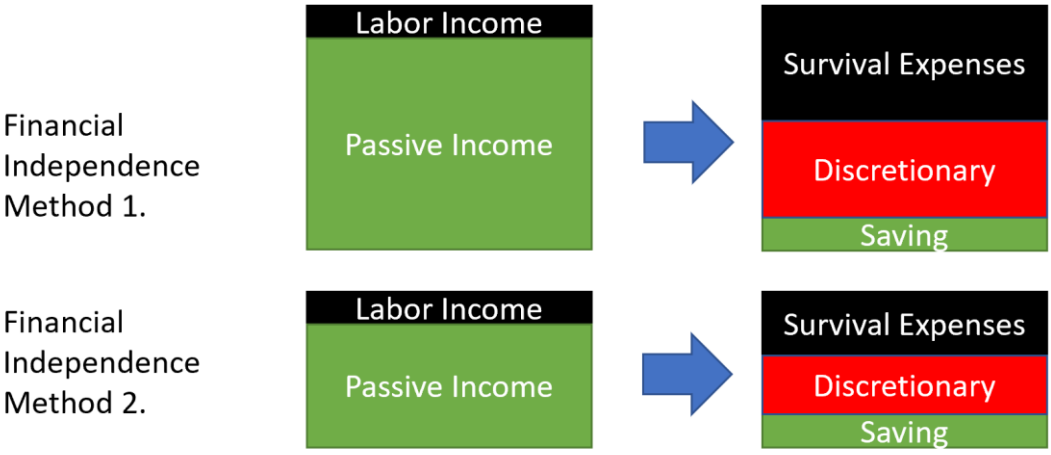
[57] This is a cross-cultural phrase. Typically means that "all work deserves respect" in that every job – janitor to CEO - contributes to society and all labor is labor and thus the laborers deserve respect too. My point here though is to push back on a surprisingly pervasive and toxic idea that humans are *innately* violent or dangerous and that too much leisure is harmful for society. I do not advocate for gluttony and sloth; I simply think we should be as free of laborers as we can. So, to that I say, let there be dignity in rest!

[58] Discretionary spending means *optional* spending; typically used in the context of government appropriations but for you, just think of it as getting Starbucks when you could have made coffee at home. It's not survival spending.

There are two ways to do that. (1) Make more money and thus save more[59]. (2) Reduce your expenses and thus save more[60].

This is where people get primed and ready to attack. They say, "There is no way I am going to live off PB&Js[61] for 10 years just to retire a little earlier. I'm not a pauper[62], I want to live now! You can die any day you know!". Or they say, "Not everyone can be a software developer making 6 figures[63]! This is so privileged to even think you can do something like this!".

Please. Take a breath. This is a math problem that you **can** solve.



Identify your acceptable life number. Can you be happy on $30,000 / year long-term (this is not your desired *income* – this is just consumption: black *Survival Expenses* plus red *Discretionary*). Assuming you're taking this money relatively low-tax or tax-free, assuming you don't need to *save* anything from it, possibly even assuming your home is paid off by the time you decide to start your independence (paying off debt is a form of saving by the way) and/or that your healthcare is covered. Pick your number in current year dollars.

---

[59] Beware lifestyle creep.
[60] I am ***not*** saying "stop eating avocado toast and buy a house". Below a certain income, there's nothing to cut.
[61] Peanut Butter and Jelly sandwiches. A fatty and nutrient dense meal dating back over 120 years in the US. Colloquially considered a staple food of the American working class, i.e., associated with poverty. I think they're great though. It's weird how much we associate with different social classes. See: Dignity of Labor above.
[62] A rude word for being poor or using charity / government assistance. Colloquially, a cheap person.
[63] At time of writing, I am **not** making 6 figures. I am literally a completely average and regular person who just likes googling and reading. I really believe this is possible for people like us. That's why I wrote this.

Multiply that number by 25[64]. I think in certain expensive places 30,000 would be too low, but let's say you retire out to a rural or smaller city where $30k is a good life. Your number would be $750,000.

I can already feel half of you going, "Dang that isn't that bad, I don't even need to be a millionaire to be financially independent on a $30K lifestyle?" and the other half yelling, "How in the hell am I supposed to come up with ¾th of a million dollars!".

Look, I already gave you the secret sauce. Earn more or spend less, they both work. The difference is in what your target lifestyle is. You can always target a smaller number if you are willing to work anyway. If all I can convince you is that you can go from Level 2 "Have Emergency Fund" to Level 3 "Financially Secure" and get out of abusive workplaces and be more confident in your relationship with money, I'll consider this a success.

Let me dive into that multiply by 25. It comes from the idea[65] that on thousands of simulations of the stock market across every possible combination of start dates and end dates; in roughly 95%+ of the simulations, you could start with a pool of money (say, $750,000) and take out 4% each year ($30,000) for expenses and survive 30+ years. 30 years is a pretty solid amount of time to not have to work at all. If you're willing to supplement even *a fraction* of that 4% by working, you can lower the withdrawal rate or even lower the total pool of money you are targeting.

If you're feeling like this is just impossible and will never work for you, please check out the subreddits I've linked. There are some really great personal stories of people in tough situations using these methods to take control of their finances. There is even a phrase – *BaristaFI* for building up to financial security and continuing to work jobs that aren't exactly known to pay well.

---

[64] This is a rough heuristic detailed more extensively in the financial independence literature. Check out that previously noted subreddit for more.

[65] I say idea, but the formal study is called the Trinity Study. It's from 1998 but it has since been revisited post 2008 global recession. There's a lot of nuance I'm skimming over around how to smooth your withdrawals, react to the market in how you withdraw, and how to account for inflation adjusted returns in your withdrawal choices. You can worry about all that later when you're actually set up with a plan to become independent from survival. For now, accept the simplified version and realize that if you can be happy with less and/or make a little more you can put yourself in a situation such that your relationship with finance can be *freeing* instead of binding.

What to Expect when You're Investing

Accept the premise that you trade labor for income. You consume some amount of it, and you save the rest. That savings forms a *portfolio*[66]*.*

Your portfolio has *allocation.* That just means the spread of investments in your portfolio. Here is a portfolio I do **not** recommend for 2 reasons: liquidity and correlation.

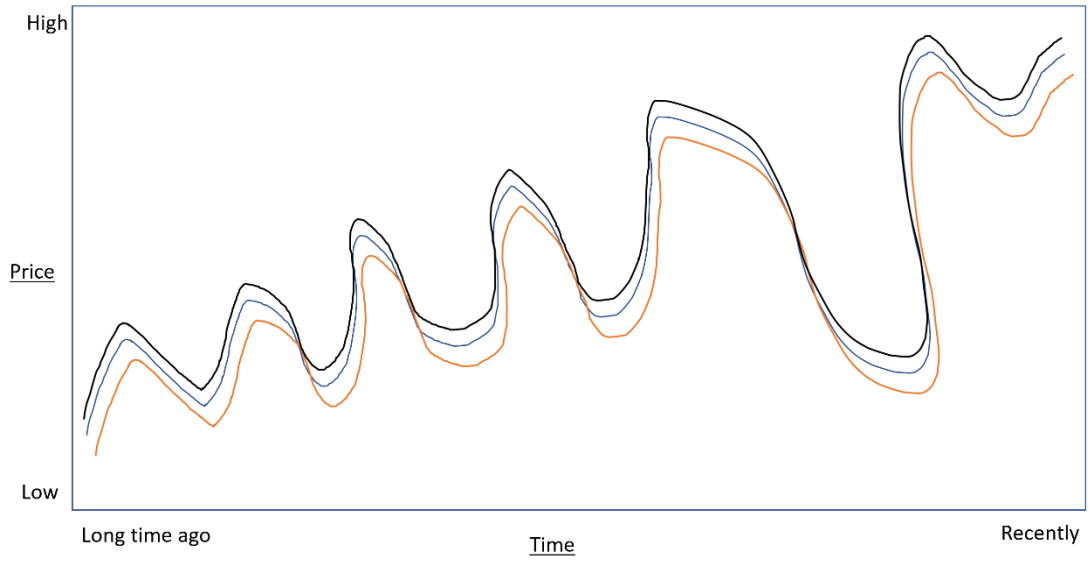
Beanie Babies	20%
Baseball Cards	20%
Rare Stamps	40%
Treasury Bonds	10%
401k	10%

The percentage is how much of your investments is allocated to each group. If I have $1,000 in investments and $400 of that is the estimated value of my rare stamps. That means at least 40% of my portfolio is *illiquid*[67]. In an emergency, I would have trouble selling my stamps (or baseball cards or beanie babies) for their full market price meaning I may sell them for less than they're worth in order to get money quickly (this gives the buyer an *arbitrage*[68] opportunity). Think a pawn shop[69].

Second, these investments are *correlated*. When the economy is good, people have money to spend on things like baseball cards and stamps. When the economy is bad[70], people restrict their spending and the market for baseball cards and stamps and beanie babies *probably all fall together*. When things rise and fall together that means they are correlated.

---

[66] Collection of investments.
[67] Review Section I: What is Finance? for more on liquidity.
[68] Something I glossed over earlier. If someone is selling X for $4 and someone else wants X for $5 and I do the buy and sell for $1 in arbitrage profit. It probably doesn't happen instantly. I might have had to take a risk (maybe no future buyer?) or wait awhile to sell (risking inflation). The *liquidity* of markets matters **a lot**.
[69] A business that buys and sells goods from individuals, explicitly to make arbitrage. Often also offer high interest, possibly predatory, loans for people in tough situations. Useful for purchasing second-hand goods though.
[70] Review Prologue, Bull vs Bear market for more on market optimism / pessimism.



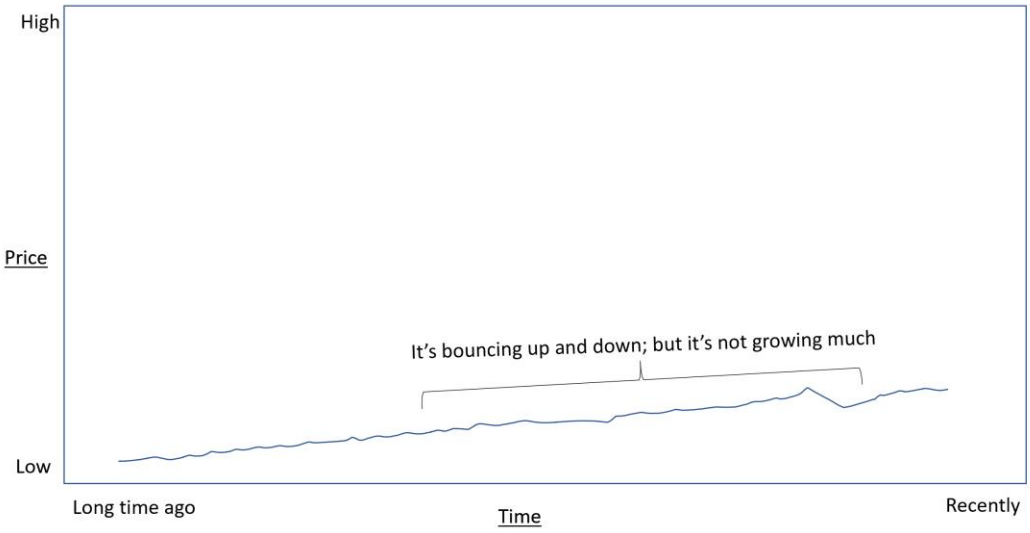
Imagine you're looking at the price history of your investments. Here, 3 lines show that while the price recently (top-right) is higher than the price a long time ago (bottom-left), there was a lot of ups and downs along the way. If the 3 lines were Beanie Babies, Baseball Cards, and Rare Stamps; they would be *incredibly correlated*. They go up and down like crazy and do it together!

This brings us to another vocabulary word: *volatility*[71]. When things go up and down like crazy it is stressful and frankly, markets don't like it. In a liquid market it is easy to know how much something is so there's limited reasons[72] for the price to rise and fall like crazy. But for illiquid markets like baseball cards, the uniqueness of each card and the reality of having to negotiate with the buyer/seller means that the price for a single card can vary greatly (especially when there is information asymmetry, e.g., if I checked the eBay last sold price[73] and you didn't).

[71] There is a special finance calculation as well as the heuristic definition I provide.
[72] This can be geopolitical issues, broader economic problems like a recession, or discovery of something that affects the market. Discovering the moon has easy to mine gold would make the gold markets react (although who knows which direction?).
[73] eBay is an auction site and you'll occasionally get the bored writer who digs around for wild listings to make a clickbait story. At time of writing, I goofed around and found a 1996 Claude the Crab Beanie Baby on sale for $5,000. But a look at the *historical* sales for the same beanie baby show *completed* sales between $5 - $50 dollars.

Here are 3 made up charts illustrating the general idea behind low volatility, medium volatility, and high volatility. In all three charts the investment grows.

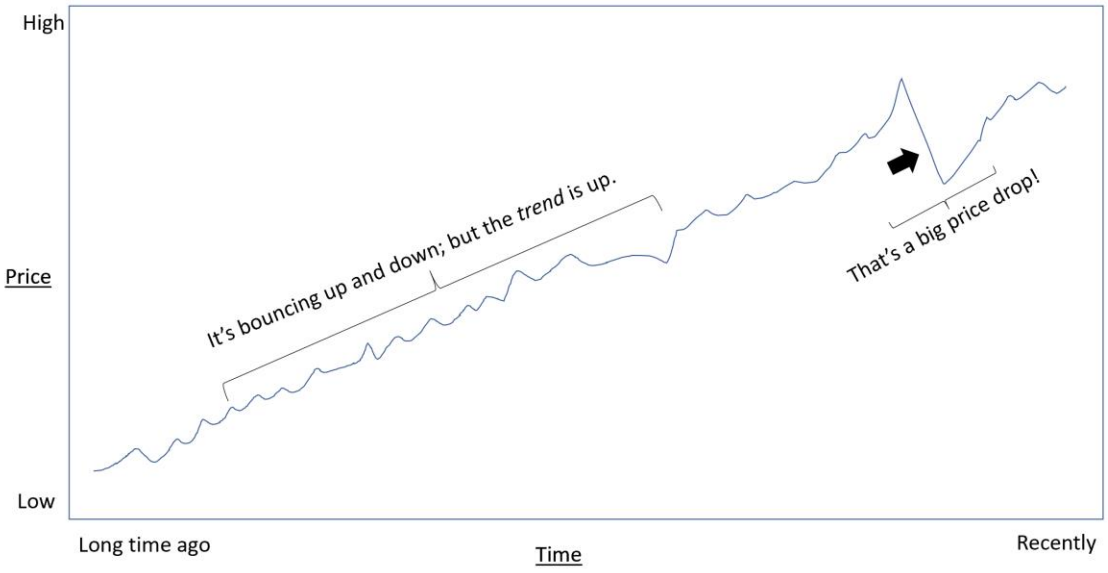
Example: US Treasury Bonds[74]



US Treasury Bonds are some of the lowest risk investments available. They're issued by the US government and are extremely liquid. They entitle the owner to a portion of US tax revenue allocated to pay the interest owed on the national debt. Their low risk tends to limit their ability to reward. Notice how slow the price goes up. It is very common to consider this investment equivalent to *inflation protection* and not necessarily something that will make you rich.

[74] There's actually a lot of types of bonds with yields across different time periods. There are corporate bonds too.

Example: Company Stock[75]



Individual stocks have a wide range of risk[76] but for now let's say we're looking at a well-known, national, historically reliable corporation's stock[77]. Here, the volatility is higher than bonds (the bounces are a bit larger) and the trend is up. This is a bit of circular reasoning, but the general idea is that riskier things *must* have higher rewards to validate being risky[78].

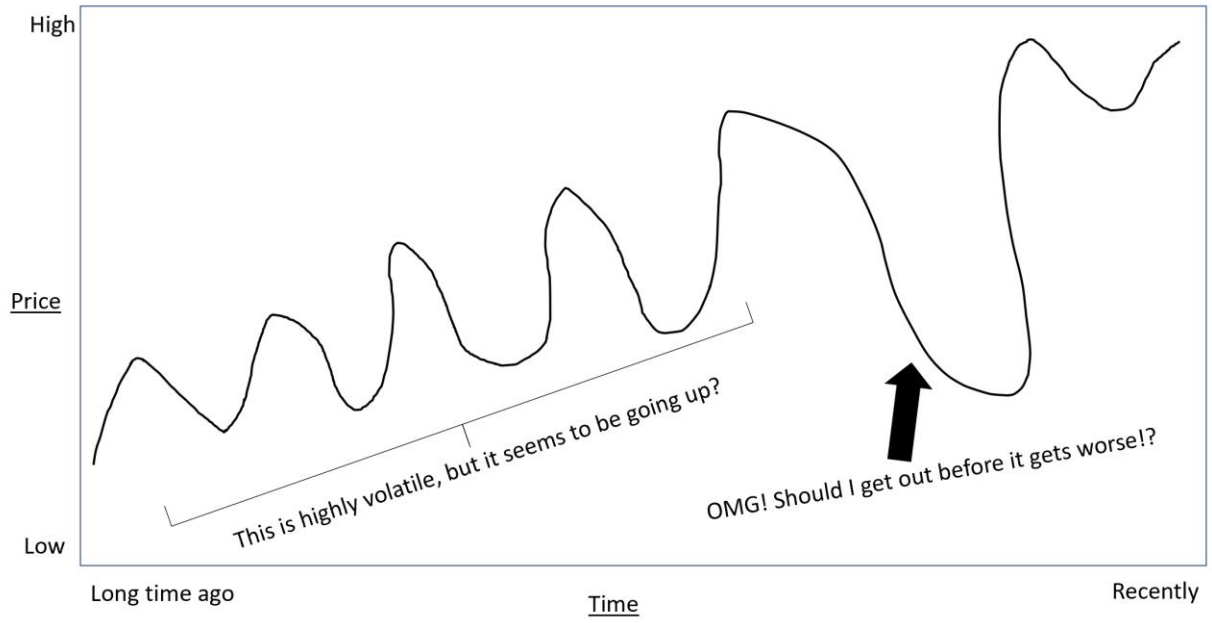
I've also added in a price drop in the top right. It's not unusual for stocks to have break from a pattern. These are called corrections[79] and are not necessarily indicative of a recession. Corporate news like major C-suite hires can cause sudden short term changes as the market reacts to the news.

Stocks make up the vast majority of a traditional portfolio, terms you may have heard of include the DOW[80], the S&P 500[81], and other collections of stocks. The idea being that patterns in these collections can serve as broad economic indicators.

---

[75] Review Section I: What is Finance? for description of stock.
[76] The crazy stuff includes penny stocks – cheap and highly volatile stocks often considered barely above gambling.
[77] There's a word for these types of stocks – blue chip.
[78] Here is a good segue to remind people that *risk* is an entire field of study!
[79] There are some math ways to define correction, but it suffices to say sudden relatively large changes in price indicate that the market has experienced some kind of shock and people are thinking differently about the investment.
[80] Dow Jones Industrial Average – An unweighted collection of 30 large "industrial" company stocks.
[81] The Standard and Poor's 500 Index – A weighted collection of 500 large company stocks.

Example: Crypto Asset[82]



Crypto Assets are not just coins like bitcoins, they are any cryptographically secure and tracked investment[83]. Here though let's imagine it's Bitcoin. It's highly volatile, regularly experiencing 20%+ changes over time. This can be highly unnerving to an investor and should be respected as potentially highly rewarding and potentially very dangerous. It's difficult to pick up trend given the volatility and for anyone who tracks their portfolio carefully, they are going to find themselves in situations where they feel *loss averse*[84] and are at risk of making the worst possible decision in finance:

Buying high and selling low.

When your goal is to make money, you don't want to make decisions that will cause you to lose money. Later I'll detail some high level strategies to help you tolerate volatility and represent your risk profile appropriately.

---

[82] I cannot understate that this ecosystem is massive. At time of writing, the total market capitalization ("market cap" – the price of something times the quantity of it available) of 6,200+ crypto assets tracked on CoinGecko exceeds $1.4 Trillion dollars. That's more than a whole 1% of the global stock market!

[83] An interesting derivative from the finance space using the same technology are NFTs – tokens that are extremely unique. For example, NBA Topshot allows people to own video highlights from NBA games and resell the coolest ones on a perfectly recorded blockchain secondary market. This perfect tracking of a secondary market has major implications for digital art and other copyrightable digital media.

[84] Loss aversion is a significant field of study in economics. The idea being people react stronger to losses than they do to equivalent wins. For example, finding $100 makes your day, but losing $100 might ruin your week.

This is where you may be asking, “Why am I even reading this? I’m not putting my hard earned money into something that can drop 20% overnight”.

Here’s 3 responses to that statement:

(1) That’s totally fine! Risk preferences are very personal and are dependent on numerous factors like people’s upbringings, their ability to rely on family if things get really bad, and the social safety net available in their country.

(2) That makes sense! But be aware that being too risk averse can make your financial independence journey more difficult. Without some risk, you’ll be forced to accrue that $750,000 without barely any help from compound interest[85].

(3) What if instead of worrying about a single investment being volatile, you diversify your portfolio with uncorrelated investments so that high volatility can *cancel out* and you get stable, positive growth?

It is this 3rd argument that inspired this entire tiny book.

[85] The eighth wonder of the world. In short: $100 in bonds that pay 2% a year is: $100 → (100 * 1.02) = $102 after 1 year → (102 * 1.02) = $104.4 after 2 years. While $100 in stocks that pay 10% a year is: $100 → (100 * 1.10) = $110 → (110 * 1.1) = $121. That 8% difference in interest rate adds up fast! After 10 years the 2% growth each year applied to $100 is $121.90 and 10% applied each year totals $259.37. In reality, the 10% probably involves more *risk* which means some years could return negative and others very positive. In practice, we tend to average out the returns across long time periods to get an “expected” returns. Since 1950, the stock market has a return rate of about 11% a year. This is **not** inflation-adjusted. Inflation adjustment simply means returns above inflation. Adjusting the rate of return in the same time period is about 7.7%. In general, when people talk about returns, you should assume they mean inflation-adjusted. Note: these kinds of calculations are very dependent on the start year and it’s easy to cherry pick and twist the date ranges to get the kind of result that boosts a desired narrative.

Think like an Average Person

What's the American Dream? To me, it's fair pay for honest work, a good home in a safe neighborhood, and confidence that if you work hard and get a little lucky you can really set yourself up for a good life. But this doesn't happen in a vacuum. People need functioning markets, with stable money, and fair enforcement of contracts if they're going to be economically mobile. Bribery, corruption, and theft aren't just bad individual experiences- they are an endemic cause of national inability to develop into a respected country. Some of the most interesting work in economics today is the study of Good Governance[86]. The idea that government, or maybe more simply, rules being followed, matters for economic development.

I don't want to belabor the point, but decentralization of finance has the power to be an equalizing force for governance globally[87]. There's a reason autocratic governments are fighting bitcoin adoption viciously. Finance is freedom!

So, what does the average person want from finance and how can decentralized finance be useful for them?

Let's do a quick recap so far.

1. People are always fighting against inflation and investment can help.
2. Financial independence enables people to control their labor fully.
3. Financial independence is unique to each person's long-term spending goals and risk tolerances.
4. Risk tolerance is highly personal but in general low risk is low reward.
5. Governance is a key multiplier (or divider) of risk and good governance makes financial independence much easier.
6. Governance varies globally and decentralized finance can algorithmically perform critical fundamentals of good governance.
7. A bad portfolio is illiquid, highly correlated, and high risk.

---

[86] Did you know Norway has some of the largest oil reserves in the world (#22)? How is it possible that Venezuela with more natural resources is in an economic crisis while Norway consistently ranks among the best democracies? Good Governance is the idea that institutions play a major impact on the effectiveness of individual interactions in an economy. If making a legitimate business requires $100s of dollars in dozens in bribes in a country- how can we be surprised that we see unregulated street merchants as the primary businesspeople in the country?

[87] See Section I: Why Decentralization?

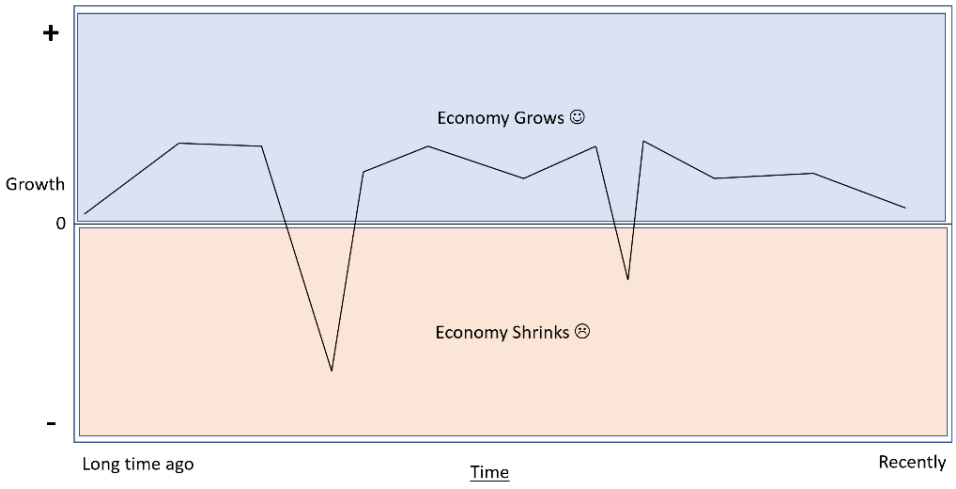
I think we can summarize the average person pretty well now. The average person wants a fair chance to build a good portfolio under good governance. I think the *fair* and *good governance* has been covered pretty well so far. So, let me start winding things down with a *good portfolio*.

1. A good portfolio is *uncorrelated*.
2. A good portfolio is *diverse*.
3. A good portfolio has *low volatility.*
4. A good portfolio *grows*.

Okay, one by one.

Uncorrelated means that we have investments that move in different directions. We saw earlier that a portfolio of mostly beanie babies, baseball cards, and rare stamps is going to be highly correlated. When the economy is good, people buy this kind of stuff, when it's bad they don't. A correlated portfolio will be *cyclical*[88].

See a pattern?



Economies grow and shrink regularly. While the pattern is not exact, in the US the average gap between recessions is roughly 5 years and they last about 1 year[89].

[88] It follows the general economy as opposed to be *countercyclical* – going against the pattern of the general economy. Cyclical portfolios *increase* volatility. You have higher highs and lower lows as the economy cycles.
[89] The history of recessions is interesting, it might not feel true to the early 2020s reader, but mathematically they've been happening less frequently in the US over time.

A portfolio that follows the economic cycle (sometimes called business cycle) will have more volatility as it will grow while the economy grows (possibly *grow too much*) and shrink when the economy shrinks (possibly *shrink too much*).

Think about businesses during a good economic time period. If you own a company and the economy is good, you may take risks and open a new location. You hire extra people to produce more and start paying raises to keep employees (especially highly skilled ones who companies compete for in the labor market).

You don't know the future. You don't know if a major trade deal gets signed that brings foreign competition to your industry[90] or if a faraway war destabilizes the energy sector and prices skyrocket causing massive inflation[91]. It's not only that your new location fails and you let go of the recent hires. Your customers lose their jobs and stop spending money at your first location. Now you're out of business, your employees lost their jobs and the cycle gets worst- businesses all start failing together and the economy shrinks.

Mature governments counter this by enacting *countercyclical* policy. For example, sending people money or cutting taxes during recessions and then raising taxes when things are better again. But this is a highly contentious issue, and you will find economists who believe these government actions are just making it worse.[92]

In the portfolio context, I'm not saying only pick countercyclical investments. I'm saying to pick both! A diverse portfolio will have assets in a wide range of industries and business sizes. Retail, manufacturing, technology, agricultural, health, pharmaceuticals, finance, real estate. There's a lot of options! Some of them cyclical, others countercyclical.

---

[90] Deindustrialization was the widespread reduction in manufacturing capacity in the late 20th century. The amount of people in manufacturing jobs in the US dropped by over 40% from 1979 to 2010.

[91] Oil is the backbone of the global supply chain. Disruptions in oil prices cause everything that involves movement in its creation to skyrocket in cost. For example, ore → processing center → metal → manufacturer → machine part can involve movement of materials across multiple continents.

[92] My personal opinion is it depends on the policy, how it's structured, how automatic it is, and if people know about the policy ahead of time. When governments do things unexpectedly it forces the entire market to react immediately. This can cause volatility. But policies that are automatic can be very stabilizing for markets. For example, unemployment insurance. The markets know about it and can know how to behave when large amounts of people start to claim it as an economy worsens. They know people will still have some money, so they will still have some customers.

A portfolio with low volatility is important. Consider you had $100. If you lose 20% of it. You're now at $80.

To get back to $100 dollars, you need to grow ***25%***.

When you're behind, you have to do even better, just to get where you were. This is the price of volatility.

Lastly, a good portfolio grows. When you blend cyclical and countercyclical, include a diverse set of industries, and aim to reduce volatility you are putting yourself in a good position to grow.[93] Your highs won't be as high, but your lows won't be as low either.

[93] You'll find a lot of literature arguing between 60% stocks / 40% bonds versus 100% stocks versus some other mix, including an older CNBC one claiming they have the magic bitcoin % allocation. The results will be highly dependent on the historical start and end dates chosen and the methods they use to simulate and how they do the investment (lump sum versus periodically), etc. I'm not trying to argue any particular percentage. My goal is checkmark your finance fundamentals and explain what DeFi is, and why I *personally* am investing in it.

High Level Strategies

> *"We need to acknowledge that 1% [bitcoin] allocation isn't going to materially harm a client. It isn't going to prevent them from achieving their financial goals, and won't damage their personal finances".*[94]

You made it this far but let's pretend you threw away everything you've read and you're back to, "why am I going to invest my hard earned money into something that can drop 20% overnight!".

The simple answer is you know the worst case scenario. It could become worthless. But you don't know the best case scenario, it could go up a 10 times over or maybe 100 times. A 1% loss in a portfolio year is bad but not terrible. A 10% gain is good. A 5% gain + a 1000% bitcoin growth[95] is a 15% total gain.

It does sound like gambling though. Let's evaluate what we know about bitcoin (and more importantly, the blockchain industry):

1. It's uncorrelated to any particular stocks or bonds.[96]
2. It's highly volatile with incomprehensible rises and falls.
3. It's an up and coming industry that has potentially global implications in how the developing world does finance.
4. Its technology may revolutionize data collection, storage, and analysis which can boost multi-billion dollar fields like artificial intelligence[97], supply chain logistics, and commercial health.
5. It's highly liquid with a robust (if volatile) trustless market.
6. The newest blockchains have the ability to run decentralized applications and leverage excess global computing power both publicly and within enterprises.

---

[94] Ric Edelman, of Edelman Financial Engines from the CNBC footnote.
[95] If bitcoin were 1% of your portfolio and it grew 10x, this would be roughly a 10% growth in your portfolio.
[96] There's some research implying its countercyclical, but I don't think we've had enough business cycles to say either way. It depends on how the market perceives it. The income effect is when people buy more of it when they have more money (The IRS considers crypto assets to be property). The substitution effect is when people buy less of it when they have more money (maybe they buy nice jewelry instead). With any good, these effects compete, and economists study the aggregate behavior when determining if the good is an inferior good.
[97] I enjoyed the Institute of Electrical and Electronics Engineer (IEEE) review of blockchain and AI intersections.

The framework I personally use- it's like betting on startups[98]. Venture Capital firms spend billions of dollars supporting new technology companies and most of them fail. But even a small percentage of winners that become multi-billion dollar companies can make all the risk worth it numerous times over.

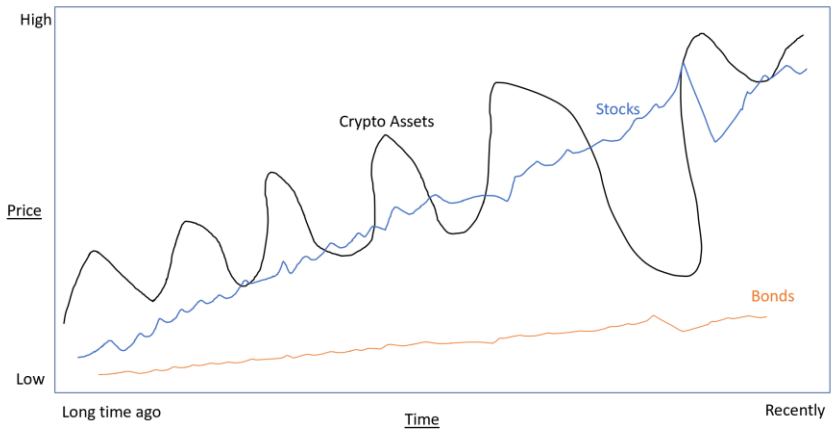
Ok, so let's say you're convinced (it's ok if you're not, I appreciate you reading this far!). You want to allocate some percentage of your income flow into this investment class but you don't know what the options are. Here a few high level strategies and keywords you can google to learn more.

1. Holding On for Dear Life (HODL'ing)

You believe in the crypto asset. You think everyone is going to want a piece of this specific technology / decentralized application (dApp). You feel the market is going to grow and there will be tons of demand. So, you buy it, and you hold it, and you watch it grow. The goal is to buy low and sell high in the *far future*[99].

Recall our 3 previous example charts; here combined.

When combining investments into your portfolio, you would *scale* the investment by the allocation percentages and then add them up.



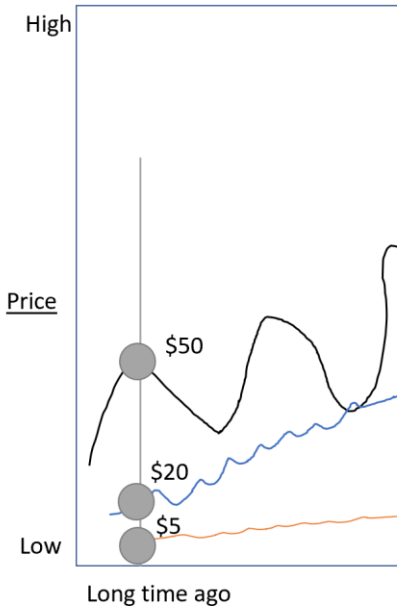
[98] Investopedia has a great article detailing how 90% of startups can fail, but if the 10% that succeed bring 1000%+ returns, it still makes sense for the investor.

[99] Read the subreddits I mentioned earlier. There's a lot of complexity around how to wind down from assets, like your 401k. There are rules around starting age, your tax rates, withdrawal penalties, caps on how much you can add in or take out, etc. Property and Crypto Assets are no different. It should be part of your financial plan.

Imagine it's a long time ago and your portfolio is ***evenly split*** between crypto assets, stocks, and bonds, with unit prices[100] of $50, $20, and $5, respectively. If you have a $300 dollar portfolio; you would have:

- 2 units of crypto (2 x $50 = 100 = 1/3 of $300)
- 5 units of stocks (5 x $20 = 100 = 1/3 of $300)
- 20 units of bonds (20 x $5 = 100 = 1/3 of $300)

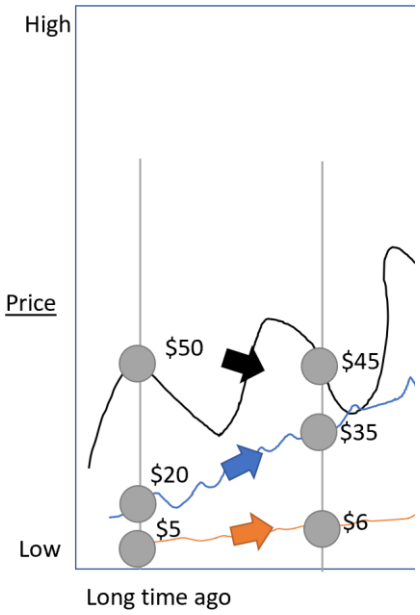
Start of Portfolio.



[100] You might not have whole units of this stuff. It wasn't always possible to buy fractional shares of stocks, some major mobile broker applications still don't make this feature available. The history of only being able to buy whole units, along with human biases around owning whole units and feelings about large numbers leads to some interesting phenomenon like stock splits. Really, a stock split shouldn't do anything at all if fractional shares exist. The market cap doesn't change it's just multiplying the number of stocks for everyone and dividing the price accordingly. But markets are tuned to human psychology and there is a lot of research into the minds of small investors. Again, in a world of fractional shares it may seem silly to worry about the unit price, but if it does truly affect liquidity (or perceptions of it) then it's something you should be aware of.

Some time passes and your portfolio naturally changes and now the chart looks this. The unit prices are now $45, $35, and $6, respectively.

- Your 2 units of crypto are now $90.
- Your 5 units of stock are now $175
- Your 20 units of bonds are now $120.



Your total portfolio has grown to $385; and your allocations are no longer evenly split, they are: 23.4% (90/385), 45.5 % (175/385), and 31.1% (120/385).

A *rebalance*[101] would sell your stocks (45.5% of your portfolio) to buy up crypto and bonds to get back to 1/3 each. Now you might be saying, "well dang I should've just been 100% stocks then!". That is something people argue[102] about, but you get into a bunch of circular conversations about what's cyclical, what isn't, what correlates, can stocks really be diverse if the companies all hold each other's stock anyway[103]. My goal is not to recommend any specific allocation. It's to educate you on a new class of assets that I think can have a global impact.

---

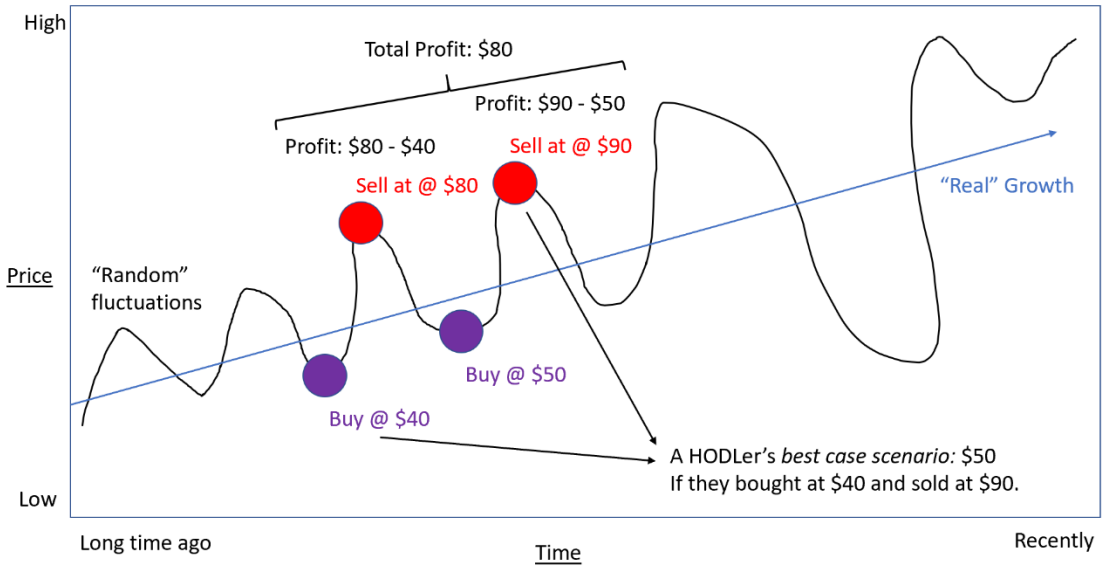
[101] There is a *lot* on rebalancing in portfolio theory (e.g. constant mix). The short of it is, you want to have a target allocation and then based on your understanding of the market rebalance appropriately. I won't get into concave versus convex trading strategy, but some keywords you can look into include CPPI, Sharpe Ratio etc. HODL'ing is essentially the idea that you never rebalance and that it'll all even out in a long enough time horizon.

[102] See CNBC footnote in Think Like an Average Person.

[103] Are you buying a single company or are you buying a holding company? What's the implication on volatility, correlation, and diversity if control of companies is consolidating?

2. Active Trading

Active Trading is the idea that you buy something when it's *relatively* low and sell when it is *relatively* high (and repeat). When done correctly you generate profit that exceeds the growth of the investment when simply HODLing.



The idea is that an investment has a *real* growth and fluctuations in the real growth are noise[104]. Modeling that noise (and ultimately pulling out *signals*[105]) is often as much studying human psychology as it is financial modeling.

Be careful actively trading, "past performance does not necessarily predict future results"[106]. And there might not be any signal[107].

---

[104] The point is that noise is in uncertain and that the value of the investment might regress to the mean. Some uncertain, but maybe not random, reasons an investment's value can vary include: the market liquidity changing because people are looking at other investments, discussion of government regulation that might affect the industry, and other news, conversations, gossip, rumors, or reports that alter a market's perception of an investment. But perception isn't always reality. A business can survive bad news cycles.

[105] This is often called *technical analysis*. At a foundational level, markets value businesses using metrics like sales, employee turnover, new innovative products, public perception, profit, dividends paid out, major hires, other relevant financial info they are required to submit in periodic public filings, such at the 10-K annual report. Technical analysis layers time series and econometric analysis to identifying patterns in the price and trade data of an asset. The premise: the market *prices in* all relevant information about an asset through constant buying and selling, and this process can be forecasted. Although efficient-market hypothesis has been losing favor.

[106] Securities and Exchange Commissions disclaimer language.

[107] There's some interesting research on stock prices moving like randomly walking down a street.

3. Lending

You're probably thinking of bank right now and you're on the right track. The idea is you deposit your money, the bank lends your (and other depositors) money to someone else and the bank handles getting paid back more than they lent out. Then you and the bank share the profit. It's supposed to be the foundational defense against inflation for the average person. But with interest rates at historic lows[108], the average savings account isn't going to grow like the economy does.

But a lot of the world, and even a noticeable chunk of the United States population is unbanked[109]. They live in a reality where a credit score isn't enough to access money. Instead, they pawn their possessions or deal with underregulated predatory lenders who charge insane interest rates (think borrow $100, pay back $400). This is different from *collateral*[110]. Where you allow the lender to hold onto a different investment of yours in exchange for a lower interest rate (because if you don't pay, they keep the collateral).

In decentralized finance, lending your crypto assets is among the lower risk options for those looking to diversify their portfolio without diving into active trading[111]. Typically, because it is a *trustless* system, collaterals will actually *exceed* the loan amount for safety. But this system isn't foolproof. Any centralized pile of assets can be vulnerable to exploits and hacking – that includes mobile apps that let you buy bitcoin (but don't actually create a wallet for you!).

---

[108] At time of writing, the national average interest rate for a savings account was 0.05%. Inflation is typically estimated between 1-3%; Significantly higher.

[109] While typically defined as the *literal* not having a bank account you should try to think of all the people who are only marginally connected to the banking system. People who live in all cash, who rely on pawn shops or loan sharks to get by, etc. This is the global reach of decentralized finance, where anyone with a cell phone (no matter how intermittently connected to the internet) can access the funds needed to grow.

[110] When you get a loan for a house, not paying puts you at risk of losing the house, but this isn't quite the same as collateral. Collateral is more like telling a bank, "Hey, lend me $10,000 and you can hold the title of my car until I pay it back. I still drive the car, but the car becomes legally yours if I don't pay you back."

[111] This article is a bit old and the Ethereum price is about 8x higher at my time of writing compared to theirs, but it's a good jump off point for those who just needed some help understanding the blockchain and not the finance part. For the investor looking for the absolute simplest way to get exposure to the space, the site linked also reference DeFi Pulse, one of the first major index funds for diversified exposure to crypto assets. As the market formalizes, you'll hear a lot more about indexes and the bleed over from centralized finance to decentralized finance. Some shockingly relevant news that happened during my writing of this, Tesla has submitted their 10-K filing with a note of a $1.5B purchase of Bitcoin (Scroll down to pg. 22). Finance is changing as we speak!

4. Liquidity Pools

I went short on the lending section because it's pretty self-explanatory. Have investment, let someone borrow it, they pay you back more than you borrowed. These final sections and the final chapter – Picking Protocols like an Economist – will be more technical. If you're not already doing so, click the footnotes! I had to make over 100 of them to keep this shortish.

Remember when I said money was a *medium of exchange*[112]*.* Decentralized finance needs mediums of exchange too. You may have gotten pretty far into this book without wondering – how do people trade one crypto asset for another? You may have even just assumed people use US Dollars to do it! Have Bitcoin but want Ethereum? – sell BTC[113] for dollars then buy ETH with dollars. That's how the stock market works after all right?[114] While it's entirely possible to do that[115] you can bypass the dollar entirely by leveraging a *liquidity pool*[116].

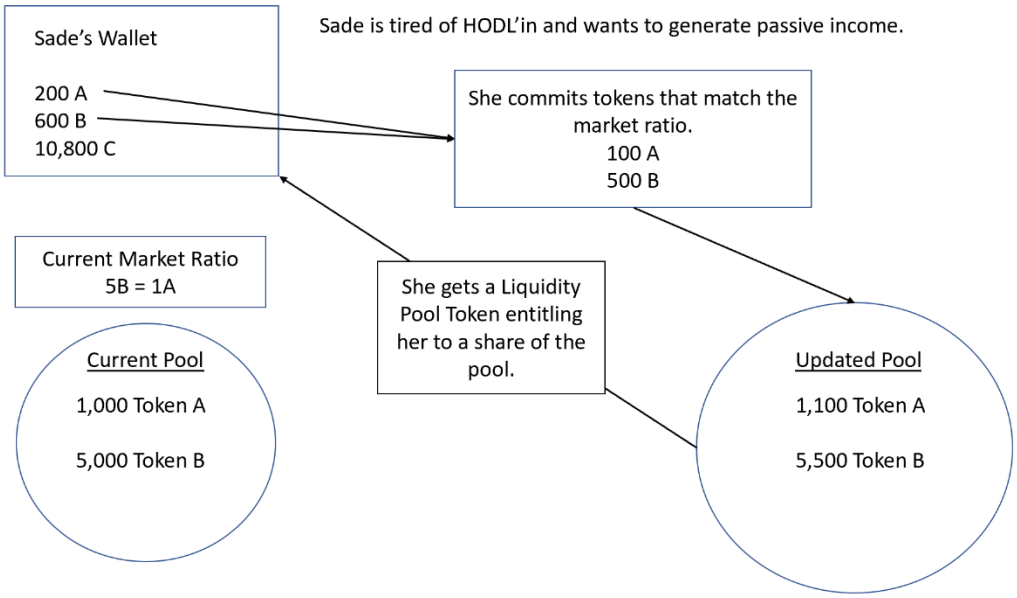
[112] If you have baseball cards but want stamps; you can either find the *perfect* buyer/seller (pay in time) or sell your cards for US dollars and buy stamps with US dollars (pay in arbitrage costs). The dollar is the medium of exchange in this transaction.

[113] Just like stocks have ticker symbols (Google – GOOG), crypto assets also have ticker symbols (Bitcoin – BTC). Except, there is no centralized body enforcing who can use ticker symbols. So *never* trust only a ticker symbol when you buy assets. I'm not saying go to the blockchain and study the hash history- but double checking prices and your expected conversion rate is standard due diligence, and you'll have no one to blame when the future is decentralized!

[114] The stock market is extremely liquid, and this does happen, but it's also possible for entities to trade stock directly, for example in a corporate buyout, stock can make up the difference when there isn't enough cash. Especially if all parties agree the stock is valuable and can rise.

[115] Technically, an intermediary **is** required for BTC ←→ ETH because they are not on the same blockchain.

[116] As mentioned in the above footnote, assets that are not on the same blockchain will be more annoying to trade, I am going to brush over this for now. We'll get to it later.



Imagine Sade has a wallet with 3 tokens in it. She wants to take a bit more risk and contribute to the ecosystem by providing liquidity to a liquidity pool. She contributes 100 A tokens and 500 B tokens to the pool. She now *owns* 1/11th of the pool[117] so she'll be entitled to a nice chunk of the rewards.

When others in decentralized finance are interested in changing their portfolio allocation by shifting their Token A to Token B (or B to A) they pay the following:

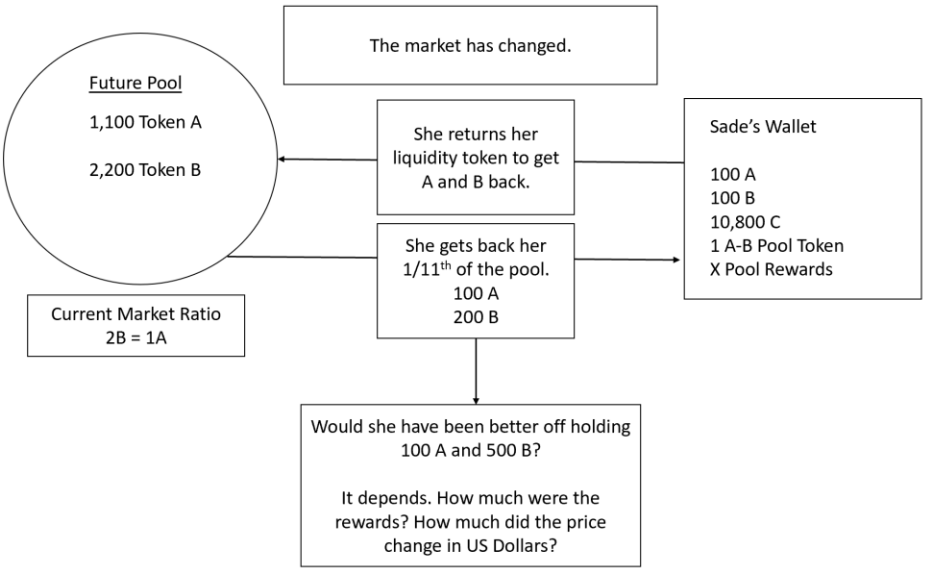
- *Gas* (Ether if the tokens are on the Ethereum blockchain) as the cost of recording a transaction on the blockchain – this goes to the blockchain participants, not the liquidity pool participants.
- Swap fees[118] (as defined by the liquidity pool) that are shared among the participants of the liquidity pool to reward them for providing liquidity, completely separate from the blockchain participants.

[117] I'm not going to cover this in depth, but a pool that is small enough for 1 person to own this much is **not** a pool you want to be in. Trading smaller (defined here by market capitalization) tokens directly will likely require intermediary transactions that dip into multiple larger pools (this increases the gas paid to do a transaction but is significantly safer).

[118] We're very spoiled in the developed world. Checking accounts are often free, savings accounts *pay you* (well, they pay almost nothing but still, an insured business holding your money for you is a valuable service!). In decentralized finance you pay for what you get. Unlike the modern ad-funded internet, you are *not* the product.

This sounds awesome right; you do a service to your fellow investors and you get rewarded fair fees for clear risk. Well, what is your risk? The astute reader will recognize *the risk of giving your coins over to a smart contract* – the "not your wallet, not your crypto" risk.

But in addition to that risk, there is also the risk of *loss*[119].



Token A and Token B have their relative values, which will fluctuate as people put more A into the pool and take B out (if B is more popular). The fees Sade receives are both a reward for providing liquidity and a cover for the loss of value she suffers when the coins in the pool change in their market price at different rates. This can be kind of complex to think about because A and B have market prices in *countless* mediums[120].

---

[119] Often called *impermanent loss* in the field.

[120] Economists love to argue about value. I tend to sympathize with labor theory of value, but there are numerous others. Something I really hope to impart to the reader is that you can and should think about the value of things outside of just US dollars (or your local government fiat currency). Not because of some anarchist anti-authority whatever, but because its value is always *inflating*. It's a really troublesome property of most currencies. That it will lose out to almost anything you want to buy with it *today*. It makes saving more difficult (imagine if stocks *stole* dividends from you but you had to have them because they were the only way to pay taxes). Competitive currencies (i.e., Hayekian money) have the possibility to *deflate* – become more valuable relative to other things. This makes them *difficult to spend*. A complete inversion of people's relationship to consumption.

At a minimum they have their independent values relative to the US Dollar and their relative values to each other. Consider some time has passed and Sade has gotten X Pool Rewards – which are in unit C[121]. The market has changed. It now only costs 2 Token B to get 1 Token A, as opposed to 5 earlier. When Sade returns her pool token to claim her 1/11th of the pool back she'll get 100 Token A and 200 Token B. Now, it's entirely possible both Token A and Token B grew relative to the US Dollar. So how do we evaluate whether Sade is better off?

One way to measure it is to assess if the X Pool reward C is higher in value than 300 B Tokens. The difference between the amount of token she got back (200) and the amount she could have HODL'd (500) as her next best available strategy[122].

That makes sense if HODL would have been her other option. But what if her other option was to sell her Bs for US Dollars and put them into the stock market? The context of her decision is important in extracting *feedback* from the market. When you think about whether you want to engage in decentralized finance try to really think of what options align to your risk preferences and set metrics ahead of time for how you measure whether your decisions were good given the information you had at the time[123].

---

[121] Did that surprise you to hear the reward could be in a 3rd unit? I'm imagining half of you going, "This is a bunch of Ponzi scheme nonsense, why would I agree to get paid interest in a *different* currency then I lent!?" and the other half going – "This is a good kind of chaos."

[122] Opportunity cost is the value of the choice you didn't make. The idea being that you shouldn't value a decision based only on its output (I lent $10 and got back $11); but its output compared to the next best decision you could've made(I lent $10 to Bill and got back $11; but I would have put the $10 in my crypto index and it'd be worth $14 right now). This allows you to *optimize* decisions. The field of decision science is a nice jump from this.

[123] This is called model calibration. When you are developing your *gut* for investing, do all the events you estimated at 20% of occurring, actually end up happening close to 20% of time when aggregated (occurred vs didn't occur)?

5. Mining / Farming

Earlier in What is Blockchain? I mentioned participating computers get rewards.

> *"You see, the blockchain isn't recorded in a single computer. That would be centralized. The blockchain is duplicated across all participating computers. The rules on how a computer chooses to participate vary, for now, just know that participating in a blockchain cost you something (computing power, electricity) but gives you rewards."*

In Bitcoin and Ethereum[124] solving the algorithms needed to secure transactions rewards participants with payment of the crypto asset. Decentralized applications running on top Ethereum leverage Ethereum Virtual Machines to run self-executing code (smart contracts). The self-executing code is able to generate their own assets if they comply with the Ethereum blockchain's ability to store and secure transactions. This is called the ERC-20 technical standard.

For example, in Sade's activity in the liquidity she earned tokens in unit C. Those might have been *brand new* units of C[125], a money supply process completely run by an algorithm. No more wondering about inflation (or deflation) like with the US dollar which uses a discretionary method for creating money- the entire printing process is publicly available, able to be forecast, and able to be invested in.

Because of the widespread growth of the industry, along with numerous DAOs competing to draw investors, numerous higher layer products have come into existence. Yield farming is a contentious one, it automates bouncing between liquidity pools to optimize the units of C (and D, and E, etc.) you get by providing liquidity at peak times. People worry it's a Ponzi Scheme built on top of a Ponzi Scheme[126]. I mean, how many currencies do people really need[127]? We'll see, it's possible that question is as silly as asking how many banks do we need.

---

[124] At the time of writing both blockchains use Proof of Work consensus.
[125] This is *liquidity* mining – in exchange for the fees you bring in by providing liquidity, you get rewarded.
[126] Old investors are paid money from new investors, as opposed to any underlying value generation process their money was actually used for.
[127] Probably more than one, but beyond that it's hard to say.

6. Use It Like Money

Ok, I've detailed some strategies for generating returns for your investment, whether they be in the same currency or otherwise. But I'd like to end this chapter on a note about the *purpose of blockchain* and how it's not all just about money. It's about supporting initiatives, "voting with your dollar"[128] in some sense.

These currencies exist to support a technology. For example, Basic Attention Token (BAT) is an ERC-20 compliant token designed to build a better system for digital media and online advertising[129]. Advertisers pay websites and content creators for generating views to their advertisements in BAT – and people receive BAT in exchange for opting in to view advertisements on the websites they visit. BAT does not use a mining process to create them, they are "pre-mined". Investment in BAT is investment in the value of the technology and its ability to disrupt the digital ad industry[130].

I'll cover more protocols including some that I will disclose that I am actively invested in. My point is not to tell you what to buy- it is to detail how I look at these protocols through different lenses and how you can use these ideas to make your own portfolio aligned to your own interests and risk profile.

---

[128] The idea that what we choose to spend on our money, is a reflection of how we want the world to be.

[129] BAT seeks to disrupt the $330B+ digital advertising industry with privacy-first data practices.

[130] I use Brave browser, which is integrated with BAT, but I don't actively trade or invest in BAT (at time of writing I've watched like $0.30 worth of ads LOL). I just wanted to remind you that this is a technology with financial implications, not financial instruments with technology implications.

Picking Protocols like an Economist

1. The Mechanics

The vast majority of (American) people's investing comes from simple, employer sponsored index funds. At time of writing, my employer uses Fidelity as their 401k manager which gives me access to targeted date funds[131] and other ETFs. I fully expect that most readers will either hold off on this technology until they get exposure through the standard investing platforms[132] or keep it simple and invest in the big players and maybe a broad fund.

This section is for those who are interested in an economist's viewpoint on how to review these investment opportunities, including some of opportunities I turned down (and how they turned out).

Earlier, I said to generate *feedback* from the market in a way that tunes your *model*[133] (i.e., your "gut" feeling for investing) you need to create benchmarks and metrics ahead of time, so you are gauging your performance effectively.

A simple benchmark that I highly recommend is: how is my crypto assets portfolio doing compared to bitcoin? This is a great benchmark because it's both extremely simple to access and it allows you to identify the *marginal*[134] impacts of your decisions.

---

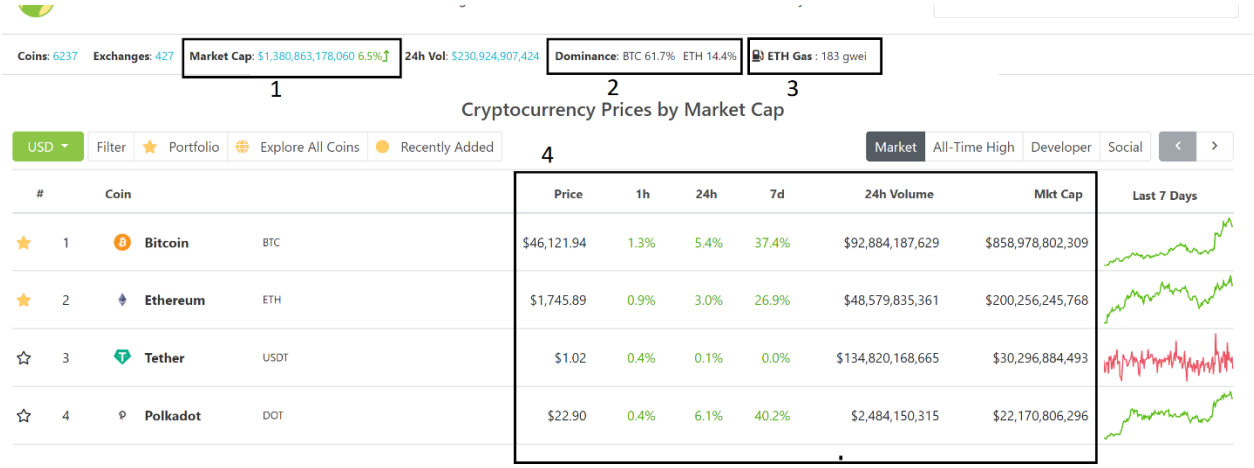
[131] Automated investing based on the patterns of changing risk preferences as people age, e.g., optimize for me retiring in 2050.

[132] MicroStrategy and Tesla have BTC on their books, so buying their shares gives you some indirect exposure to crypto assets. While Grayscale Bitcoin Trust, an over the counter publicly traded trust is valued directly for their bitcoin holdings. Although some find the idea antithetical to the point of bitcoin and argue it's a fundamentally overpriced way to access the asset- it has become the primary mechanism for people to have bitcoin exposure in their 401ks and traditional investment vehicles.

[133] Review Section II: Thoughts – High Level Strategies – 4. Liquidity Pools

[134] If you judge all your assets relative to the US dollar, that's obviously very useful, but it confuses both *exogenous* effects (the entire crypto asset market is down a bit today) and your specific (marginal) decision making (instead of keeping it simple and holding bitcoin, I tried to get fancy and put money in liquidity pools). When there is a bull market, all strategies might be winning against the US dollar (after all, it's an inflationary currency). You should seek to compare your decisions *to the next option you would have made* – if your options were not "liquidity pool or checking account", but instead "liquidity pool versus bitcoin", or even "liquidity pool versus S&P 500"; you would be giving your gut the best feedback by comparing it directly to your 2nd best option. This is a foundational principle of decision science – setting definitions of a good decision ahead of time and only relative to the relevant alternative decisions you would have made.

Let me walk you through CoinGecko[135] the tool that I use to monitor my crypto assets portfolio. You make an account, you click the portfolio button, and you can add your assets and track your transactions, fees paid, and portfolio growth. They also have full profiles of all the coins they track including historical pricing and a free API to access even more detailed information.



Looking at the home screen some key boxes you want to review are:

1. The overall market cap of all the coins they are tracking.

This is the sum total of all the individual market caps for each coin. Where the market cap of any specific coin is the available supply times the price. Typically coin supplies change through the minting (coin creation) process. For example, Bitcoin is estimated to max out at 21 million coins in the year 2140; there are currently a little more than 18 million in circulation[136].

---

[135] CoinGecko is a totally free site for tracking your portfolio, identifying new coins, getting links to coin white papers, websites, and communities (you can interact directly with developers using Telegram, Discord, Twitter, and other social media sites they participate in). It also has (simple) charts allowing you to compare coin growth to Bitcoin or Ethereum. This is important, as the market is still maturing, and the vast majority of coins have *extreme* correlation with Bitcoin. This is another reason to benchmark yourself against Bitcoin since it serves as the leader of the entire market.

[136] It gets harder over time to mine bitcoins which means their marginal cost per coins (in terms of electricity cost for the participating computers) rises over time. If the market stopped valuing bitcoin above its marginal cost, people would stop producing them. There is a lot of conversation and press around whether bitcoin mining is sustainable in terms of energy consumption. Realistically, a lot of bitcoin mining comes from solar and hydroelectric facilities (for the same reason some companies are considering putting their data centers underwater- it saves money in keeping your computers from overheating).

2. Dominance

Bitcoin and Ethereum are the top 2 coins by market cap and it isn't even close.

Quick note: The third place coin, Tether, is a US Dollar backed "stable" coin designed to allow people to easily de-invest and re-invest into crypto assets without doing a full exit and dealing with centralized banks[137]. There are numerous coins seeking to serve as the equivalent of a dollar and it offers an interesting way to access relatively low risk lending and lower risk liquidity pools[138]. In some ways, you could argue these coins shouldn't be tracked as crypto investments if they're pegged directly to US dollars, but for purposes of dominance they are tracked.

The BTC market cap is over 60% of the total crypto market cap, and ETH is about 14%. The market tracks this as *dominance* – how dominating are Bitcoin and Ethereum in the total crypto assets space?

This is important for 2 reasons: First, a market where 60% of the money is in one asset is going to be highly correlated to that one asset. There's an argument to be made that *if everything just follows bitcoin anyway* why be in anything else? Second, the growth of any particular coin in the market can itself happen two ways: the market can grow and thus people buy it with *new money*[139] or the market can change, and people buy *less of another coin* and buy it. This is called income and substitution effects.

---

[137] I haven't done this to you yet- but something you'll hear a lot in the crypto space is DYOR. Do Your Own Research. There is no central authority to hold people's hands as they try to enter the space (although numerous private companies do try, they are known as centralized exchanges). Tether's history itself is contentious and the idea that they are *not actually* backing their coins 1:1 with US dollars is something you should research prior to using them. In fact, you should get into the habit of researching *everything* you invest in- we've been spoiled by corporate backed 401ks and federally insured bank accounts. It's not a natural way to think about investing!

[138] See Section II: Thoughts – High Level Strategies for more. The idea is you can reduce risk of loss by providing liquidity for a single coin plus a stablecoin. Because stable coins are, well, stable, you don't have to worry about the relative price movements of the two coins you provide liquidity for.

[139] US Dollars or other non-crypto asset. New, meaning that the value was previously not in the crypto market.

When people get money, how do the markets for hamburgers and steak react? Realistically some people when they have more money buy more hamburgers (income effect) and some buy more steak (income effect). But in addition, some people might become so rich that they *begin to see hamburgers as inferior* and shift their hamburger money to steaks (substitution effect). It is entirely possible for the substitution effect to be larger than the income effect and thus the hamburger market shrinks as people get richer[140].

The point being the crypto market is currently highly correlated with the dominant assets. This might not be true in the future as the technology develops, the market matures, and it begins to differentiate among similar investments[141]. If you accept this premise, then eventually as smaller technologies that, you know, actually *do* something[142] grow they'll have to grow from both new money entering the space (income effect) and money being shifted away from the dominant assets (substitution effect).

[140] The classic economics example is SPAM; I mean just look at a google search for spam inferior good.
[141] In the early 1990s, did the average investor really differentiate between Circuit City, RadioShack, and Best Buy stocks? Maybe a little bit, but it can take years for the market to accurately assess differences between similar investments and ultimately choose a winner.
[142] See: Is it Solving a Problem?

3. Gas

Gas is the transaction cost in the Ethereum blockchain[143]. A simple smart contract uses less computational resources than an intense one. For a participant to be incentivized to put your transaction on the blockchain, you pay them gas – which for visual ease is in a unit called gwei (10^{-9} ETH). You can technically set your own price and limit for how much you are willing to pay (at max) for a transaction and be refunded the difference between your maximum and the actual amount used, but this can be overwhelming for a beginner. But it's an important concept for you to understand because, **if you underpay you lose it all**. If you send a complex transaction and not enough money to pay the computational resources needed to run it, the participant will fail to complete the transaction, it will not be added to the blockchain and your gas will have been spent trying and failing[144].

[143] There are numerous competitor blockchains that have adopted smart contracts and designed their proofs to be lower intensity, while arguing they are equally secure, thus enabling much smaller transaction costs. Generally, these can be Ethereum compatible which is known as a Layer 2 solution or be an entirely separate blockchain competing directly with Ethereum's use case. The issue with this is that Ethereum's first mover advantage is so large, many developers are not bringing their applications to other blockchains. There are also some technologies looking to serve as *bridges* between blockchains to provide cross-chain liquidity, thus improving the overall ecosystem's interoperability.

[144] This is a massive ongoing conversation. High transaction prices are themselves proof that the system is incredibly popular, but it also alters the calculus needed to invest. Can you validate only putting $100 into an investment when the transaction cost if $20+ *each way.* You would need an ROI of 40% just to break even. Centralized exchanges typically have *significantly* lower (i.e., near $0.00) transaction fees compared to decentralized exchanges on the Ethereum blockchain; but the price you pay is in privacy, control, and arbitrage. They can (and often do) charge you more per coin than the prevailing market rate and there's nothing you can do about it and rarely any evidence that they did this (different markets can have different prices for the same good!).

4. The Financials

Some coins cost 10s of thousands of dollars, while others are a *fraction* of a penny. Because you don't have to buy full units of a coin the price isn't that good of a signal. Supply differences[145] can cause two otherwise equivalent investments to have a magnitude of order difference in prices[146]. So, it's common to look at market cap instead of price. A coin with $10M in market capitalization is small but has opportunity to grow. But the market for that coin could be illiquid and highly volatile. The smart contract code could be exploitable. High risk, high reward.[147]

Focusing on market capitalization makes it easier to compare $10 coins with 1M supply to $1 coins with 10M supply. But this method isn't foolproof. People have psychological biases to owning whole numbers of an asset. A large number of low cost items is not necessarily a growth opportunity[148].

The action of a market is typically measured by its *volume*. This is the amount of buying and selling that occurs in some time period (typically the previous 24 hours)[149]. It is common to review the ratio between trading volume and market capitalization as a measure of *action* in a market, but there are numerous financial methods for assessing markets that I can't fully cover here[150].

---

[145] Both with the total supply and the amount the supply changes each day. Note: supply does not have to only increase, there are actually protocols that involve *reducing* supply especially if they are targeting a specific price. This is often called a *rebasing* token. It's a bit beyond the scope of this book, but I will include 1 example later.

[146] You can own 10 $100 coins, or you can own 100 $10 coins. If they have the same market capitalization it doesn't change your investment allocation in dollars. Also, because fractional units are so common, they have even less reason to be considered functionally different.

[147] One strategy known as, *aping*, is a play on the famous "monkey picking stocks" trope. Whereas the monkey picks stocks randomly (as evidence that expert curation of stocks is basically irrelevant), aping splits a portfolio into numerous small (hopefully uncorrelated) high-risk investments hoping just a single one skyrockets like Bitcoin did.

[148] At the time of writing DOGE coin has bounced from under a penny to nearly $0.10 and back down to about $0.07. There are numerous twitter campaigns challenging users to buy the coin until the price hits $1 which would be a 1,000% (colloquially called a "10x") return on investment for those who bought at $0.10. It's definitely been interesting to see DOGE rise from obscurity to a top 20 coin by market cap effectively overnight; but hitting a $1 would require the coin become the 3rd most popular coin by market capitalization – which will be tremendously difficult given the, frankly, more *functional* competition up there. But who knows, brand matters to markets.

[149] Note: Crypto assets are a 24/7/365 market. Between the US/Latin America, EU/Africa, and Asia time zones this shouldn't be too surprising.

[150] If a market has a capitalization of $10M but the trading volume in the past 24 hours is $20M, it implies that a single coin has multiple buys and sells of the same token in the same day. This does not directly mean the capitalization will grow, but it is a good sign of liquidity and it is marker I personally use to assess markets.

2. Platforms not Products

This is a contentious[151] venture capital phrase with the premise that products have too much competition and it's better to be the foundation on which a market of products compete. So instead of managing housing development (one of many uses for land)- you invest in land that developers want and will compete for in the future. Or instead of becoming a vacation rentals company, you invest in Airbnb where independent rental "companies" (including individual homeowners) compete for short term tenants.

Some blockchain technologies that might be considered platforms include:

- Ethereum[152] – the blockchain that serves as the foundation for decentralized applications that are ERC-20 compliant. Investing in its token Ether, is like investing in oil when you believe the usage of gasoline is going to grow.
- Uniswap[153] – the major liquidity pool exchange, allowing users to create their own liquidity pools to earn fees. Investing in its token UNI is like investing in banks- the business behind businesses doing business.
- ChainLink[154] – a completely decentralized data communication network. It allows smart contracts to access information that isn't stored on the blockchain, for example, a smart contract that triggers based on the price of a particular US stock or an insurable event like a flight cancellation, would pay LINK to access APIs maintained by market assessed operators that make certain data available in blockchain readable formats. Investing in its token LINK is like investing in business journalism that keeps information flowing to markets.

These technologies are different than say a yield farm that rewards participants with tokens that provide voting rights governing the algorithm used to generate yield; or bitcoin which rewards users for recording transactions.

---

[151] Here's a whole article debunking it. The idea being that in *reality* platforms expand from singular highly successful products and don't just occur by themselves, so products with platform evolution potential should be the focus.
[152] Disclaimer: I am invested in ETH.
[153] Disclaimer: I am invested in UNI.
[154] Disclaimer: I am invested in LINK.

3. Is it Solving a Problem?

In the stock market you can invest in banks. Doesn't this seem a little circular? Or is it the simple acknowledgement that if all businesses are going to need banks at some point anyway, you can cut out the middle-man and go direct to them.

I personally don't buy into that idea. I think the businesses you want to invest in are the ones that outgrow banks[155]. To do that, I look for opportunities that disrupt the market.

Just like Basic Attention Token seeks to disrupt the digital ad agency through a privacy-first and direct-payment internet, other crypto assets identify new ways of doing decentralized business.

Bird.Money[156] seeks to differentiate interest rates for (anonymous) wallets that are good borrowers. By studying the blockchain, differences in how borrowers (as identified by their wallet hash ids) interact with lending platforms can be identified as more or less amenable to loans. This type of credit score[157] system directly parallels the function of the major credit bureaus in normal centralized finance and differentiated interest rates that are tied to direct activity and not potentially biased loan applications[158] solves a real problem.

PieDAO[159] seeks to reduce transaction costs by allowing people to pool their requested transactions via smart contracts with up to 97% cost reductions for those willing to wait for their 'pies' to bake in the 'oven'. They also manage several index funds for those looking to get curated access to different blends of the DeFi ecosystem. This performs a similar service to centralized finance exchange traded funds (ETFs) that serve as curated bundles other stocks.

There are thousands of decentralized applications and DAOs looking to disrupt multi-billion dollar industries, it's not all finance. In the next chapter I'll detail some coins I am not invested in (at time of writing), but have considered, as examples of how I assess value.

---

[155] I mean with both Apple Card and nearly $100B of cash on hand you start to wonder how many companies are pretty much banks with a side gig of selling a product.
[156] Disclaimer: I'm invested in BIRD.
[157] In the US, credit scores use publicly available and company provided information to rank people as borrowers.
[158] Mortgage discrimination has a devastating history and persistent effect evident in the wealth gap today.
[159] Disclaimer: I'm invested in PieDAO.

4. A Personal Audit

In this final section, I'd like to look at a few investments I considered but ultimately did not commit to and reflect on how they turned out without me.

Shopping.io[160] is a decentralized application built on Ethereum by a private organization based in Florida, launched in December of 2020. It uses the Ethereum blockchain to secure private transactions with the major online retailers of the day: Amazon, Walmart, and eBay. I first identified their utility token SPI in late January of 2021, trading between $10 – 12. It passed my checks.

It's a platform that unifies the search and purchase of goods across 3 major sites allowing a singular user experience to identify the best price for their real world product while enabling better data privacy by purchasing through their smart contract instead of through the user's account.

It also solves a real problem, allowing users to purchase real goods, online, with over 100 crypto currencies.

It's market capitalization at the time was about $10M across a maximum supply of 1M coins (960,000 of which were circulating). These types of smaller market caps are prime growth opportunities, but they can also fail quickly – not only in that their price could fall tremendously, but that their liquidity could be pulled by enough individuals such that you get stuck with the coin and no one to buy it from you. I rated it as a medium-high risk and medium-reward opportunity. Reading the white paper[161] I liked that they incentivized people to hold their utility token SPI to get discounts for purchases made through the site and entitled them to earnings from their liquidity pool[162]. Large holders also had direct access to the management team for contributing ideas to grow the project.

---

[160] Ticker: SPI – but again, never trust a ticker. Always check the price and token you're buying.

[161] It is common practice for a protocol to launch a white paper detailing their goal, roadmap, and technical details around how they interface with other protocols and secure data. Occasionally you'll find coins that don't have one, it's a red flag in my opinion, but there are some good groups out there who instead of a white paper (which is static) deal directly with their community of buyers through medium articles, newsletters, twitter/discord/telegram, and other methods.

[162] This is a special type of liquidity pool called *staking*. You trade for an organization's coin and then lend it back to them in exchange for a portion of earnings from their smart contract and potentially other rewards. Can be a bit Ponzi-ish when the value generation mechanism isn't explicitly detailed.

I decided against investing because of my overall lack of knowledge on the dropshipping[163] ecosystem of the 3 platforms they are connected to, along with feeling the SPI token was a bit gimmicky. It wasn't strictly necessary for them to have a governance token to be a platform that oversees conversion of crypto currencies for real world products. Amazon could wake up tomorrow and accept BTC[164] and it would weaken their value-add, or Square could partner with a centralized exchange and offer the same capabilities to the thousands of businesses in their network.

I also didn't like the way their paper detailed owning 0.1% of the *entire market* enabled someone to have a 5% discount on goods purchased. It seemed to be a market cap limiting mechanism – if 1,000 people wanted 5% discounts on Amazon – they could give SPI $10,000 each? In higher risk investments, to lend someone that much money would require *very good* returns and I wasn't convinced the liquidity pool fees cover the entrance and exit costs they impose to incentivize long-term staking (10% on entrance and exit!). On top of that, they limit how many orders you could make per month based on how many SPI you held (not necessarily held *in their staking pool*, which makes it a bit safer, but still!).

The free shipping, the innovation, the platform, the real problem-solving were all super interesting, but I couldn't see myself using their service.

Outcome[165]: At time of writing SPI is trading for $50, with a market cap exceeding $48M, with a trading volume of $8.9M (19% TV / MC ratio).

It always hurts to feel like you missed a major opportunity. But ultimately, given the information I had at the time and my hesitancy around SPI being *the* place to buy things with crypto long-term (Amazon, eBay, and Walmart could start accepting crypto directly) I think my decision was reasonable.[166]

---

[163] Dropshipping is the coordination of a purchase and delivery without taking ownership of the product, e.g., having a website that allows businesses to order metal parts and then using a connection to a manufacturer to build that part and mail it directly to the buyer from the manufacturer- without taking ownership in between. It is very popular on Amazon for independent sellers who have good marketing and branding skills, but don't want to oversee the logistics and inventory management of goods.

[164] During the editing process of this book, news broke that Amazon and Mastercard do intend to work with cryptocurrencies directly.

[165] Here is the link to the current market at your time of reading. Was I right? How is it doing relative to BTC?

[166] During the editing process of this book, recent news seems to have impacted SPI, it fell >50%.

ThorChain[167] is a chain-agnostic protocol that uses its core token RUNE as a mechanism for providing liquidity across blockchains. Someone could deposit Bitcoin into a Thor liquidity pool (an asymmetric deposit[168]) which would be mapped to the prevailing exchange rate of BTC and RUNE, and then own a % of a BTC-RUNE liquidity pool. Because of the atomic pair of [any Coin] – RUNE across multiple pools and blockchains, ThorChain is able to create a *continuous* liquidity pool such that any pairing can be exchanged regardless of chain (given that there is liquidity between the two and RUNE).

It's current market cap at time of writing is $1,085M with a 24 hour trading volume of 95M (9% TV/MC). Its price is $4.57 with a circulating supply of 237M coins out of 500M projected maximum supply[169].

ThorChain is a relatively mature protocol, growing consistently over a year+ and ranks in the top 100 coins on CoinGecko[170]. Given its longer history, it's possible to review how it performs relative to the growth of bitcoin (assuming that is my benchmark strategy).

Looking at the market cap of RUNE in BTC (as opposed to US Dollars) shows that it is close to its all-time high[171] relative to BTC.

---

[167] They use a lot of Thor references throughout their pages, you'll quickly see how different crypto assets instill culture to their development process.

[168] Symmetric versus asymmetric deposits are covered more deeply in the thorchain liquidity pool documentation, but imagine Sade submitting only token A to the A/B pool.

[169] Earlier I mentioned there are 18M bitcoin and in 2140 there will be 21M bitcoin, as it will take that long to mine all the coins. I like to think of circulating versus maximum as a kind of roadmap estimate for the asset to reach maturity and try to judge it based on those standards. Will people use when they aren't being given new money to do it or will they go on to the next thing with inflated rewards?

[170] This is not actually that great a signal – there are a lot of contentious and highly volatile coins that have a large market.

[171] All time high (ATH) is a common phrase indicating the price of something has never reached the amount. During editing, Bitcoin reached a new ATH of $50,000. This industry moves quick!

This recent growth is interesting and maybe I'll learn a bit more about how it handles differences of its price on different blockchains (they state they use bots to automatically trade to balance liquidity values in the face of low trade volume) and reassess if I should add this to my portfolio (as opposed to buying more of something else[172]).

A momentum investor[173] might see this chart and quickly decide to spend the gas to replace their recent lowest performers investments with this. While a contrarian investor may think it will regress to the mean relative to bitcoin and instead continue to buy bitcoin.

Outcomes: TBD, I wouldn't be shocked to hear its price double or more ($10+) but I also wouldn't be shocked if it regresses to the mean relative to bitcoin[174].

---

[172] There is always an opportunity cost, don't forget to set mental benchmarks.

[173] This is a real trading strategy. Some studies state its quite performative, but the behavior can become a self-fulfilling prophecy and worsen bubbles.

[174] During editing, Bitcoin went on a major run to $50,000 while THOR has stagnated around $4. The industry moves fast, but THOR is still on my radar as continuous liquidity is a big value-add for blockchain interoperability.

The last coin I wanted to discuss may be the trickiest but, in some ways, the most fun to think about. For me, it's to bitcoin, what bitcoin is to stocks. An uncorrelated and unique (but not always low) volatility investment that diversifies a portfolio.

Ampleforth is a *synthetic commodity*[175] designed to have low correlation with Bitcoin and other assets. It's token AMPL has a special provision in its smart contract allowing it to scale up or down the tokens people hold in their wallets. This is called a *rebase*[176]. When an AMPL strays too far away from $1, for example by $0.25, all wallets containing AMPL will see their amount of AMPL rise when the daily rebase time is reached. Not quite by 25% - that would be too sudden – but by a function of how much it deviates from $1. Then 24 hours later, it forgets the previous rebase and calculates a new percentage to rebase all wallets based on the current price deviation from $1. The process repeats daily with no memory.

When the coin has more mature adoption and its volatility is lower (but still unique!) it can serve as a completely decentralized version of a stablecoin[177].

Because of this unique price mechanism, the way the math works out is that your purchase of AMPL is a static percentage of the *market cap*[178]. This offers the same growth oriented investment mechanism as any other coin, but via a coin that seeks to maintain a peg to US dollars. The more it's used the more your fraction of the total market cap becomes worth.

---

[175] Fancy word for fake-thing.

[176] Some coins are stable by being backed 1 for 1 to a dollar. AMPL attempts to be stable by strategically manipulating the amount of coins that exist directly in people's wallets.

[177] While it still aims to be worth $1, it doesn't rely on storing large amounts of US dollars in a centralized way serve as the reserve; this means AMPL can serve as a reserve currency for other smart contracts that want to have a US Dollar reference value in the future (instead of agreeing to a payment $500 or 500 USDT, they could agree to a payment of 500 AMPL knowing it will be roughly $500 worth of coins).

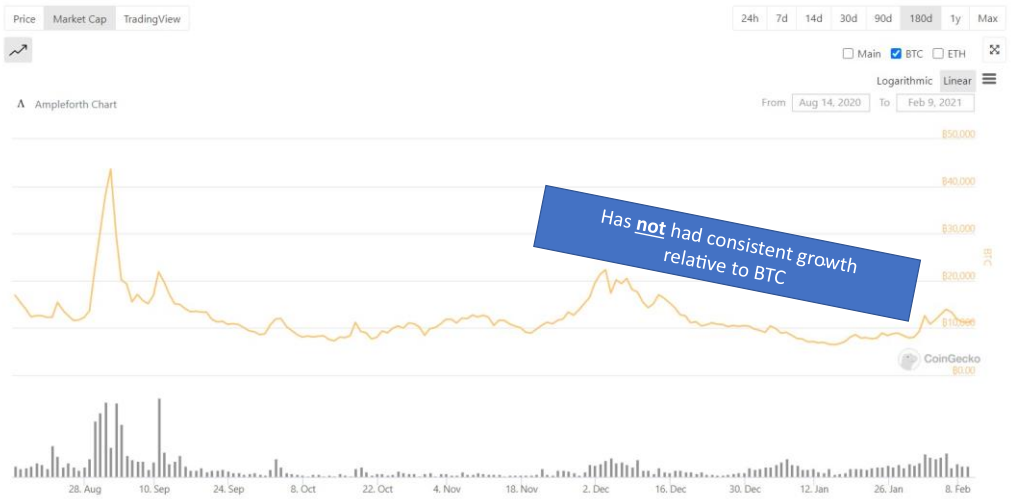
[178] If AMPL's market cap (MC) is $10M and its price is $1, there must be 10M AMPL. If later on it deviates from its price target in the free market and is trading for $1.25 with 10M AMPL in circulation, the market cap will be $12.5M. The price deviation causes the supply to rise (but *not* to 12.5M AMPL immediately) at the rebase time as monitored on the official dashboard. This causes the price to fall (but *not* to $1 immediately). This regularly scheduled arbitrage session enables a new market assessment that *could* exceed $12.5M market cap meaning the price grows more after arbitrage. In the long term even sustained buying from momentum investors has a limit. When prices fall below $1, *negative* rebases occur which reduce the amount of coins in people's wallets (this pressures the price to rise to $1 but not immediately). Over time, the idea is that the fad of positive rebasing (and seeing simplistic "tokens go up") dissipates leading to long term lower volatility and more gradual growth in the market cap as it becomes adopted for its original use.

I was a major fan of AMPL through Summer 2020, seeing its first major bubble burst in late July, having (luckily) decided to exit over too much volatility.

At the time of writing, there are 391M AMPL with a Market Cap of $543M meaning the price is above its target ($1.39 instead of $1). This means that at the next rebase cycle, everyone's wallets will inflate with AMPL, pressuring the trading value of AMPL to fall.

At time of writing $543 would by 1 millionth of the AMPL market cap. If AMPL caught up with the most popular stablecoin USDT, with a market cap of $30B at time of writing; $543 would grow to 1 millionth of the $30B market cap, equaling $30,000. A bit counterintuitive but it manages to solve a problem – decentralizing stable coins – which are a major piece of the decentralized finance ecosystem.

But separate from appreciating the potential and innovation - viewing the market cap of AMPL in BTC (as opposed to in $USD) over the last 180 days you can see it has not seen a sustained pattern of beating Bitcoin (although this comparison is a little less fair given Bitcoin mines new coins and thus people don't get to keep a consistent share of the market cap).



Outcome: I avoided the worst of its Summer 2020 bubble, and it has failed to exceed our benchmark strategy (HODL BTC) over the same time period. But broader adoption of blockchain, reduced volatility in the long-term, and numerous farming options available to AMPL may make this coin worth revisiting if centralized stablecoins fall out of favor.

Epilogue

Thank you for your interest in this growing technology. I just want to end with a note that while *this space is constantly changing* – all the coins I mention could fall out of favor before 2022 and I could look pretty dumb pretty fast- there are some fundamental concepts (and contexts) in global economics and decentralized finance that can validate allocating a portion of your portfolio to these technologies.

As always do your own research and try to balance hype and your own sense of the fundamentals. Or maybe more simply, see if you can get a comfortable amount of exposure through your existing investment methods like your 401k, IRA, or post-tax savings. There's no need to rush, bitcoin has at least 100 years left of mining to do.

I hope this small book was engaging, useful in boiling down some complex topics to their core, and worth sharing with others.

I hope you connect with me on LinkedIn and let me know what you thought!

Carlos R. Mercado
Data Scientist | Economist | Blockchain Enthusiast
LinkedIn: linked.com/in/crmercado