Bitcoin Basics

sudo-anon*

September 2024†

Thesis statement

"The current monetary system does not work for a significant portion of people, maybe the majority in some parts of the world[1], and bitcoin may be a less bad solution - but it will be a generational journey to find out."

1 Who is this for?

There is a well known cognitive bias called the Dunning–Kruger effect[2] that, in practical terms, I see as saying that your ignorance of a subject gets in the way of asking intelligent questions and learning more about it. Just to give a round number to this I use the rule of thumb that most people can probably get to the point of asking intelligent questions after 100 hours of high quality study of a given topic[3]. This document can be used to start you on your 100 hour journey to get yourself to the point of being able to ask intelligent questions about bitcoin, and, most importantly, about how to bring about a world that is better for having bitcoin in it. Alternatively, it can be seen as a set of interconnected "Quick Guides to Bitcoin" viewing it from different angles that can be read individually by someone interested in a specific aspect of bitcoin.

*This name chosen is a not particularly clever or unique pun based on the Linux command "sudo", that allows you to elevate your privileges to run any command, and the word "Pseudonymous", which is not doing something under your own name. This is written under a pseudonym, not to hide who I am but rather because it shouldn't matter.

†Minor edit to fix broken hyperlinks December 2024 and a few small typos fixed February 2025.

[1]For example, the figure given by human rights activist Alex Gladstein in 2021 is that 1.2 billion people were living with double or triple digit yearly inflation, mostly in countries with developing economies. Many of these are currencies that are in the process of failing. Currency failure can be seen by people in other countries as something that happens to other people "over there" so it must be something wrong with "their system" that needs a local solution. In contrast, my opinion is that there are systemic issues with the current monetary system but they are affecting some people and countries more than others. Essentially, I think that all fiat currencies are on the road to failure, it's just some aren't noticed as it takes a long time when compared to a human lifespan. For example, hardly anyone who uses the New Zealand dollar seems to be concerned that it has experienced around 1000% inflation over approximately half a lifetime (based on CPI data from Stats NZ, a New Zealand government department).

[2]See Wikipedia article "Dunning–Kruger effect".

[3]This 100 hours is just 1% of the rule of thumb that it takes 10,000 hours to become an expert in a subject. There is no particular rationale for this exact number but it seems to be about right.

This document starts with Section 2 that includes a small number of links to high quality resources to bitcoin related topics. Section 3 then introduces some fundamental parts of bitcoin that are unlikely to change to give a core knowledge to build upon. This section can be skipped if you are just mildly interested in bitcoin. In this case though, it is probably more important to read Section 4 about some of the common misunderstandings of bitcoin. There is also Section 5 that includes a definition of what it means in my opinion for bitcoin to "succeed". As one of my main concerns is the way in which bitcoin will scale, there is also a short section, Section 6, on the history of scaling bitcoin and some possible problems on the horizon. Finally, Section 7 has a couple of links for keeping up to date with innovations in bitcoin.

You will see that there is extensive use of footnotes. Some have links to further resources but some are just digressions. These do not need to be read by the casual reader. This document is available as both pdf and html versions[4]. If you do not want to be distracted by the footnotes, the html version may be easier for you to read, but the pdf looks nicer and can be easily saved so you can refer to it later.

2 Resources for research

This is a short list of resources that are a good place to start your journey. Some of the following sections refer to these so you may want to read the rest of this document before deciding where you want to start.

- "Bitcoin Explained in the Bitcoin Basics Workshop" is a single two hour talk[5] by Andreas Antonopoulos[6] on YouTube that quickly covers most of the details of how bitcoin works. From the slides available for the talk, it looks like they ran out of time and there was supposed to be an additional 5 minutes or so on the basics of hashing and proof of work mining. To cover this you could watch the second half of another YouTube video, from 3Blue1Brown, called "But how does bitcoin actually work?" that goes into a lot of detail about this. This second video contains a lot more detail than most people need, but, between the two, this is likely most of the details people need to know to have context to start understanding discussions about any proposed changes to the way that bitcoin fundamentally works.

[4] Available at http://nofrillstech.net/guests/sudo-anon/BitcoinBasics.pdf and http://nofrillstech.net/guests/sudo-anon/BitcoinBasics.html respectively.

[5] The context of the talk is that it was given in 2019 and was designed to cover what was needed for the Certified Bitcoin Professional exam. I have not taken the exam, nor do I endorse it. But I do think that it is interesting that according to the webpage, the first hurdle you have to overcome in order to take the exam is that "You must pay for the exam in a cryptocurrency such as bitcoin."

[6] Another good resource are the "off the cuff" talks he did at various conferences that were summarised and put into short chapters for The Internet of Money series of books, available for purchase from his website: Volume 1, Volume 2, and Volume 3. (With a free login, you can "check out" Volume 1 and Volume 2 from the Internet Archive). The videos of these talks are available free on his YouTube channel in these 3 playlists: Collection of Videos from "The Internet of Money Volume 1" Book, The Internet of Money Volume 2, and The Internet of Money Volume 3. There is also the "Best of" playlist. Note that he has stepped back from going to conferences and giving talks since the pandemic so most of these videos are from prior to 2020.

- The "Beginners Guide to Bitcoin" is a series of 17 podcast interviews put together by Peter McCormack in early 2020 covering a large number of topics including: what money is, the prehistory of bitcoin, the history of failure of the "altcoins" that tried to make a "better bitcoin", the basics of how bitcoin works, and how the lightning network layered on top of bitcoin works. The interviews can be listened to individually but in some cases the concepts explained in an earlier interview are referred back to and built upon in later interviews so you would get the best out of it if you listened to them in order. In most cases, the people being interviewed have a large number of articles or talks online, some of which may be linked from the individual interview. You can use these links for further details or opinions and perspectives on different subjects if you are interested in what they have to say.

- The Reddit /r/Bitcoin Newcomers FAQ contains some basic information you should get familiar with and a large number of links to further resources for research as well as different hardware and software products that are respected. These lists should be curated and kept up to date.

- Broken Money by Lyn Alden is a book that came out in late 2023 and is a primer on how the current monetary system came to be, how it is broken, and how the future may pan out[7][8]. The former parts give a good summary of the current monetary system while the latter part includes a good introduction and summary of bitcoin. One of the most interesting points is how our concepts of money evolved once we had systems that could transfer information faster than physical goods, starting with the telegraph, and the natural incentives that lead to our current ideas of money. A lot of content is described and briefly summarised with a lot of references so that, if you are interested, you can easily do further research into a topic.

- A very large number of resources have been gathered together under different bitcoin adjacent topics by Jameson Lopp on his website. Most of these are just webpages with a lot of links on them. Without further information it is hard to figure out what is there so I would suggest you systematically go through the Getting Started section but after that just pick a topic that interests you and click half a dozen links at random and just see where that takes you.

[7] A half hour YouTube video titled "How Money & Banking Work (& why they're broken today)" is also available that introduces and summarises some of the ideas in the book. Additionally, a large amount of good information is included in the long form essays published at https://www.lynalden.com/ with one of the central ideas of the book being well described in the article titled "The Speed of Transactions vs the Speed of Settlements".

[8] This book is the only resource on the list that is not available for free so I would like to offer a couple of alternatives that you can start with. While not specifically about bitcoin, there are a couple of books I would recommend as looking at money from a more historical perspective. Hopefully these will allow you to start to have a broader overview of what money has been in the past so you might be able to think that it may change in the future. One of these is "Debt - The First 5000 Years" by David Graeber, available from the Internet Archive. The other book I would recommend is "The Ascent of Money" by Niall Ferguson. While the book itself is not available for free, it was adapted into a 6 part video series presented by the author and is available on his YouTube channel with the playlist called "The Ascent of Money".

- The Learn Me a Bitcoin website is the website I would have written if I had all the time in the world to do so but this comes with the caveat that I like getting into the details of how computer protocols work. You can start with the beginner's section and then follow some of the references to the more technical sections if you want. The basics cover some of the terminology and software you need to know in the current environment if you are going to use the software to interact with the bitcoin network. The technical sections go into a lot more detail about the low level bitcoin protocol itself and are likely of interest to only a small section of people who like to get into the specifics of different computer protocols. The underlying protocol is important to know the basics of, and is something I have an interest in understanding, but in a lot of ways is the least important part of bitcoin when it comes to asking the big questions about the future shape of a world with bitcoin in it.

- I would also suggest that people read the original white-paper that described the original concept of bitcoin after reading a few of the other resources. You do however need to be aware that a few things have changed from the original vision. There are many places to find this and it is only a few pages long but I would suggest the copy that comes as an appendix to the Mastering Bitcoin book[9] that is available on Github as it also comes with a small errata section that highlights some of the things that were found to be wrong or where the terminology has changed as the technology developed etc. At the time of writing these were Appendix A and Appendix B respectively. Most people should be able to easily understand around half of it and after some reading around the subject can probably grasp a good two thirds of it. Feel free to just skim it initially and then come back to it later and see if you can understand more of it. Again though, understanding the minor details of where bitcoin came from are normally not needed to have an interesting discussion about where bitcoin is heading.

- One of the ways bitcoin has scaled the number of transactions it can handle is with the creation of the Lightning Network, a set of protocols that run on top of bitcoin. For most people, all you need to know can be summarised in a few info-graphics from https://www.bitcoindesigned.com: One with the big ideas, called "Why build the Lightning Network?", and, if you are interested, a set of three step by step guides showing the back and forth that happens in the background between participating computers when transactions take place on the Lightning network: "Understanding the Lightning Network - Part 1", "Understanding the Lightning Network - Part 2", and "Understanding the Lightning Network - Part 3"[10].

[9] This book itself is a good resource for those interested in the underlying bitcoin network protocol but it is primarily written for programmers and only the first couple of chapters are really for the "normal" person.

[10] If you want to start a deeper dive into how the protocols themselves work, a good place to start is a long article that attempts to summarise the technical Mastering the Lightning Network book. Mastering the Lightning Network is a companion to the Mastering Bitcoin book and aimed at the same sort of developer audience and so not really something I would recommend for the general audience. But, it is a very good resource if you are a developer wanting to understand the suite of protocols. It also includes as an appendix, a review of bitcoin fundamentals, which is a summary of a good part of the Mastering Bitcoin book. This

- Once you have a basic understanding of a topic and want to research it further, you may want to start with the bitcoin wiki, https://en.bitcoin.it/wiki/Main_Page, or you can search for terms, authors, or topics using a bitcoin specific search engine, https://bitcoinsearch.xyz/

3 Introduction to bitcoin

Understanding bitcoin is complicated by the fact that the very word "bitcoin" is used to mean many things. Some ways that it can be used are:

- a name for an alternate digital currency. This document as a whole is about laying the groundwork for trying to understand the consequences of having a world with this currency in it.
- a synonym meaning 100,000,000 units of that currency. The base unit is now called "Satoshis" or "sats" after Satoshi Nakamoto, the pseudonymous creator of the initial white-paper and software implementation[11]. To avoid confusion, all units are denominated in sats in this document, followed by the bitcoin amount if appropriate.
- the computer protocol language and rules for computers to check what it is valid to do with this currency. This is the way the word bitcoin is primarily used in the following detailed section of this document, "The basics of bitcoin transactions and blocks". This can be made more clear by instead calling it something like "bitcoin transaction validation".
- the computer protocol language and rules for these computers to communicate with each other about such transactions. These can be described as the "bitcoin protocol".
- the subset of protocol language and rules that are in common with the majority of the computers (as these things slowly change over time). This can be called the "bitcoin consensus rule set".
- computers and the computer protocol language and rules for these computers to communicate with each other. These can collectively be called the "bitcoin network".

What problem is bitcoin solving?

The concept of bitcoin is relatively simple to understand when you think about the problem it is trying to solve and how it does it.

appendix would therefore be a good place to start to see if you are the sort of person who would like this pair of books.

[11] While the base unit of the bitcoin network is the satoshi, there are already thoughts about how this could be subdivided if needed. For example, the lightning network, built on top of the bitcoin protocol for deferred settlement of micro- to mid-range payments, already has the capability to transfer and charge fees in "milli-satoshi" units. Comments in one implementation, initially written in 2017, say "MilliSatoshi are the native unit of the Lightning Network. A milli-satoshi is simply 1/1000th of a satoshi. There are 1000 milli-satoshis in a single satoshi. Within the network, all HTLC payments are denominated in milli-satoshis. As milli-satoshis aren't deliverable on the native blockchain, before settling to broadcasting, the values are rounded down to the nearest satoshi."

Question: How can people scattered around the world come to agreement on who has money, how much, and the order in which it is transferred between parties without having to trust a central authority?

Answer: Everyone runs their own software to check the rules they think are important and share out the transactions they think are valid and just drop those they think aren't. This goes even further than not trusting a central authority, it means we don't have to trust any particular entity, we have an adversarial approach and assume that anyone could be lying to us - this leads naturally to the conclusion that more bitcoin nodes is better than fewer i.e. decentralisation is part of the way we achieve security.

The complexities come with the subtle interactions of implementation details; for example, a bitcoin node can't really assert the trustworthiness of anything that is not a bitcoin transaction. Therefore the rules we follow must include how new satoshi units of bitcoin come into existence as a special kind of transaction.

The basics of bitcoin transactions and blocks

Note that you do not actually need to know the details in this section to "use bitcoin" or make a bitcoin transactions. The software you use to do so will hide most, if not all, of these details. These details are design decisions that were implemented in the initial bitcoin software, publicly released in January 2009, if not also described in the white-paper, released October 31st 2008. They have consequences that have shaped the evolution of bitcoin in the past, and are likely to do so into the future, so are good to know about if you want to explore interesting "what if..." scenarios about bitcoin's future.

Bitcoin transactions

A bitcoin transaction consists of a list of inputs and a list of outputs. Each of the outputs is assigned a number of satoshi units in value and can have conditions that need to be met to spend it. These conditions can be quite complicated and use a constrained computer language, called bitcoin script, to describe them[12]. These transactions are shared between bitcoin nodes and each checks it's own list of validity rules that they care about. The inputs for a transaction are the outputs of other transactions and may include any additional information needed in order to meet any conditions limiting them being spent. In order for things to be kept simple, each input is wholly consumed in the transaction and if the total of the inputs is more than the sum of the specified values of the outputs then the remainder is used as a transaction fee. If the total of the inputs is less than the total of the outputs it is not considered a valid transaction.

[12]The bitcoin script computer language is explicitly designed to be Turing incomplete, with no loops or recursion and a maximum length of the script. The main reason for this is so that for any transaction it is known that it will halt and give a result of whether or not the conditions are met after a specific maximum number of calculations. Even given that, there were theoretical concerns where a "pathological" transaction could have been constructed that would have taken orders of magnitudes of time longer than the typical transaction to validate and caused significant slowdowns in the bitcoin network. This was called the Quadratic Sighash Problem and is described in a fjahr.com blog post titled "How SegWit solved the quadratic sighash problem". This is in the context of it being one of the the things the SegWit soft fork solved during "The Fork Wars", see the section in this document "The Fork Wars - increasing transaction throughput".

Bitcoin addresses

Because the outputs of one transaction are used as inputs in another, a way was needed to address previous transactions but the way this is done in the actual transactions is not easy for people to use. Quickly an abstraction of "addresses" was created based on the standard spending conditions that were put on transactions. It encoded them in such a way as to include a prefix[13] and checksum. The prefix can be used by people to easily differentiate one address format from another (with the checksum helping to detect and fix typos).

Not all transactions are standardised enough that they fit into this bitcoin addressing scheme but all can be referred to by a hash of the transaction to give them a relatively unique transaction id for the purposes of sharing them between bitcoin nodes so they can quickly identify which transactions they already have and which they have not seen before. A hashing algorithm is a one way computational process to produce the same output for a particular input each time it is run. In this context, one important point is that the hash is a fixed size and will be generally smaller than the size of the whole transaction.

Blocks

Transactions shared between bitcoin nodes like this, once they pass validity checks, are still initially considered "unconfirmed". For the transactions to be confirmed they first have to be gathered together at intervals and put into a data structure called a "block" which has a some additional details in a "block header" and a special transaction that is the first in the block called the coinbase transaction[14]. Bitcoin nodes also share information about which blocks they know about and validate all new blocks they are told about before passing them on to other bitcoin nodes.

The coinbase transaction has one "dummy" input in a specific format and has one or more outputs as normal and is not spendable for 100 blocks. The maximum value of the outputs of this coinbase transaction are the sum of the transaction fees for the other transactions in the block and a calculated value called the "block subsidy".

Block subsidy

This block subsidy is how new bitcoin come into existence and was initially 5,000,000,000 satoshi (or 50 bitcoin) but is split into epochs when it is cut in half (and rounded down to the nearest satoshi)[15] every 210,000 blocks. The block subsidy will eventually be zero after the 33rd such halving. Note that each bitcoin node keeps track of the current block subsidy itself and will simply reject a block with a subsidy it considers too large. The eventual maximum

[13] For a list of prefixes, see this Bitcoin wiki article "List of address prefixes"

[14] This is not be confused with the large cryptocurrency exchange Coinbase that presumably named themselves after this transaction

[15] An interesting consequence of the exact number chosen for the initial block subsidy is that the number of bitcoin in the block subsidy corresponds to the percentage of bitcoin still to be "created" at the end of that block subsidy epoch i.e. 50% of the bitcoin were still to be created at the end of the first epoch, 25% at the end of the second, 12.5% at the end of the third, 6.25% at the end of the fourth. The fifth epoch, which began on the 20th April 2024, therefore began with 93.5% of all the bitcoin that will ever exist.

supply can be easily added up and is a little under 2.1 quadrillion satoshi, or 21 million bitcoin[16].

Difficulty target

Bitcoin blocks can be put together by any computer on the bitcoin network running the appropriate software. Such a subset of bitcoin nodes are called "miners" due to the emphasis in the early epochs on bitcoin creation over fees collection with the block subsidy in the coinbase transaction going to the one who mined the block. In order to make it a "lottery", and so not have any particular miner be preferred over any other, the block header contains a section that the miner can change and then run a hashing algorithm on the candidate block. The output of the hashing algorithm is just a list of ones and zeros that in this case is interpreted as a number. The number must be lower than a specific "difficulty target" number.

There is no known way to know beforehand what the output will be from a given input. Therefore, to try and get a block with a hash value that is lower than the difficulty target, there is no better way known than to just set the miner adjustable values randomly, run the hash calculation, and see if the number it gives is lower than the target number i.e. a simple "guess and check" strategy. This is called "Proof of Work" as it takes real world energy to do these calculations.

Blockchain

Each candidate block header must also contain the hash of the previous block it is building on top of. This links the blocks together in what has come to be a called a "blockchain". The importance of this is that if an entry in a previous block is changed, this will change the value of the hash of that block and break the chain and it's link to future blocks. It will also likely make the block invalid as the calculated hash is no longer under the difficulty target. So, to create a valid previous block, the "guess and check" step will have to be rerun and then when the new valid block hash has been produced, it will need to be used to replace the old one in the next block to relink the chain. This next block will then have a different hash and the process will have to be continued up to the chaintip. The more buried the original change, the more work that would have to be done to recreate a valid chain of blocks.

For a given difficulty target, others can give an estimate for the level of work put in for the block. Remembering that the whole point is to have a process to come to agreement on which transactions are valid, and in what order they occurred, then we can just say that the chain with the most accumulated work is the one we consider the correct one. If there are multiple competing chains with the same amount of work, we keep them all until we hear about a next block built on top of one of them. We then discard the other chain and it's orphaned blocks after taking any valid transactions and incorporating them back into our pool of valid transactions to share out. Depending on the time to propagate

[16] Note that the theoretical maximum is 2,099,999,997,690,000 satoshi but the coinbase transaction does not have to have outputs that add up to the maximum allowable amount and it has already happened, likely accidentally, a couple of times that less than the maximum block subsidy was assigned to a coinbase output in a valid block so the actual maximum supply will end up being a little less than this.

information around the network, the difficulty target, and the total number of competing miner computations, we will be less certain about the permanence of transactions in newer blocks but more certain about transactions in older blocks. We can follow the history of transactions from the first "genesis block" that comes as part of our node software all the way to the current chain tip. At every step of the way we can make sure we agree that every transaction and every block is valid according to the rules we have implemented on our node.

Difficulty Adjustment

The final piece of the puzzle is that the difficulty target is not a specific number but instead is calculated independently by each bitcoin node, including miners, and is recalculated every 2016 blocks based on the time it took to produce blocks in the last difficulty period. As with the block subsidy, each bitcoin node calculates this value independently and will reject a block that has a hash value higher than it's own calculated target, independently of what other bitcoin nodes decide[17].

The calculation adjusts the difficulty target to try and have one valid block produced every 10 minutes on average. So, the difficulty automatically adjusts roughly every 2 weeks, based on the last 2 weeks difficulty, to try and have 2016 blocks created in the next 2 weeks[18]. Extrapolating out this means the block subsidy halving events every 210,000 blocks should take place roughly every 4 years with the block subsidy ending around the year 2140.

Concluding remarks

All the numbers referred to in this section were set in the original software implementation by Satoshi Nakamoto with no stated rationale but it is thought that it is a balance designed to make things practical for a world wide network to bootstrap itself on a human timescale and take real world constraints into account. For example, the fact that the difficulty adjustment is targeting 10 minutes means that it gives enough time for blocks to propagate around the network but not too much chance of having multiple valid blocks at the tip of the block chain. These occasionally happen but are simply solved by just having miners build on top of the first one they see and everyone else just keeping a copy of all valid chain tips they see until there is one that is a clear winner in the sense that it has the most proof of work. This means there are occasional chain reorganisations but they normally only affect the latest couple of blocks so

[17] To allow all nodes to validate blocks, including those blocks that were created before the node was part of the bitcoin network, the difficulty target is included as part of the block header in a compact format meaning that the difficulty target used is actually the calculated difficulty target to 4-6 hexadecimal significant digits.

[18] The highest difficulty target allowed is the one chosen by Satoshi for the first difficulty period at the initial creation of the software but initially blocks were created at less than 2016 every 2 weeks. This meant that the target could not actually be adjusted downwards until the bitcoin network had been running for nearly a year with December 30th 2009 being the first time the difficulty target was adjusted. There is also a know "off-by-one" error in the current code that means it has a small bias toward lowering the difficulty target more than necessary with a theoretical exploit called the Timewarp attack that uses this and an interaction with another time based rule in bitcoin. See the bitcoin stack exchange question "What is time warp attack and how does it work in general?", or the Bitcoin Explained podcast episode 5 "Time-Warp Attacks (And Bitcoin Cash's Difficulty Adjustment Drama)".

there is a rule of thumb that if your transaction is a high value one you should wait for an hour or so (6 blocks) before you consider it final[19].

For more detailed information on some of these topics, see the Learn Me a Bitcoin website sections such as transactions, blocks, mining, and difficulty. For the detail oriented there are also more technical details on digital signatures, the coinbase transaction, and chain reorganisations.

4 What bitcoin is not

There are a number of misconceptions and misunderstandings about bitcoin, and, as the majority of these are about fundamentals, it is good to clear these up as quickly as possible before moving on to the less clear areas. For example, although most news articles that deal with bitcoin have pictures of physical coins, bitcoin is not physical. This is probably at the root of most misconceptions about bitcoin because people describe bitcoin with analogies that relate to the physical world but all analogies break down at some point and if you're not careful, you can take an analogy too far and end up with a flawed understanding without meaning to. So, here is a quick list of common misunderstandings that people have:

- There is actually no concept of individual "coins" at all, just transactions with lists of inputs and outputs. The outputs can have conditions for spending them in other transactions. The inputs are outputs of previous transactions and have attached to them any information needed to spend them. The value associated with an input is totally consumed in the transaction[20].

- Bitcoin is "controlled", not "owned". This seems to be a subtle distinction but is important to understand. You cannot really prove that you were the only person to have known the secret needed to spend bitcoin, just that you were the first person to spend the bitcoin out of all those who knew the secret. If you are supposed to be the only one to control some bitcoin, then you need to understand that you should never share the secrets needed to spend it. This is simplified to the advice that you should never enter your wallet seed phrase into a random website, a random internet connected computer, or any software that you do not trust[21].

[19] Another consequence of the choice of the different numbers are with the ones that combine to make the issuance schedule of new bitcoin. There is an obvious measurement of bitcoin issuance, the annual bitcoin inflation rate. During the fourth halving epoch, starting mid May 2020, this annual inflation rate was less than the standard 2% inflation of government backed currencies that central banks targets in most developed economies. During the fifth epoch, starting at the end of April 2024, the annual bitcoin inflation rate is less than the lower end long-term estimate of 1% for the above ground annual increase in the gold supply. It seems to me these are natural comparisons to make so it may be that the numbers that make up the issuance schedule were chosen, at least in part, to combine so that the epochs in which these comparisons can be made were in a time when Satoshi would likely still be around to see if the project had started to be taken seriously.

[20] If the outputs add up to less than the inputs, any additional value is given to the miner as an implied transaction fee.

[21] The advice can go even further and more paranoid. For example, you should never have your seed phrase on a piece of paper that can be seen by a webcam as it is possible that the webcam could be compromised.

- Bitcoin is not the first attempt at a digital currency to rival government backed ones, it is just the first successful one. Some of the precursors to bitcoin are briefly described in Chapter 20 of Broken Money and are gone into more detail in the Beginners Guide interview "Part 3: Bitcoin's Pre-History and the Cypherpunks with Aaron van Wirdum"[22].

- Bitcoin transactions are not anonymous, only pseudonymous. This is a subtle concept and with bitcoin it is actually reasonably difficult to be anonymous. For a brief introduction, see the Bitcoin Magazine article "Is Bitcoin Anonymous? A Complete Beginner's Guide". For a longer exploration of what it takes to maintain privacy with bitcoin, see the Beginner's Guide interview "Part 12: Bitcoin Privacy & OpSec with Jameson Lopp".

- Bitcoin base layer transaction fees are not based on how much value you are transferring but rather how much data you use with the transaction[23]. The fee you will pay for a typical transaction depends on the total number of bytes the transaction ends up being [24]. Most wallets also contain a fee estimator but you may want to check that against some different views of the "mempool" of waiting transactions[25]

- Bitcoin wallets don't hold bitcoin, they hold the "private keys" that are secrets that allow you to spend bitcoin, along with information about what transaction outputs these belong to. With most wallets, they will have "seed words" that they require you to write down when the wallet is created. These seed words allow you to recreate the private keys with other wallet software so that if you lose access to the wallet but retain the piece of paper with the seed words, you can recreate these secret private keys in another wallet. On the flip side, if you have secured your wallet so only you have access but have given someone else access to the seed words, they can import the seed words into a wallet of their own and spend the bitcoin themselves.

- Bitcoin is not a "get rich quick scheme". However, this seems to be the way a large number of people come to bitcoin; "come for the profit, stay for the revolution". What seems to happen is that people eventually take to heart

[22] At the time of this interview, there were 5 articles Aaron van Wirdum had written with the title prefix of "The Genesis Files" that are linked at the bottom of Beginner's Guide interview webpage. Since then he has also written a book about this called "The Genesis Book".

[23] This is complicated by the fact that transactions that occur on the Lightning Network built on top of bitcoin generally have fees that are based on how much value you are transferring (and how many nodes you are routing it through). For more information, see the Bitcoin Manual website article "How Fees Work On The Lightning Network".

[24] There are a number of fee estimators that take the total number of bytes into account and check how much the current per byte fee seems to be to give you an estimate of the fee you will need to pay to get your transaction in the next block. This is complicated by different address formats, number of inputs and outputs leading to different numbers of bytes. There is also a "fee discount" for SegWit and Taproot type transactions, see the later sections in this document "The Fork Wars - increasing transaction throughput" and "Taproot - increasing transaction complexity" for some details. A calculator that gives a total number of bytes for 5 different transaction types and contains a technical breakdown of how these are calculated is https://bitcoinops.org/en/tools/calc-size/

[25] For example a quick fee rate estimate is shown on the homepage of https://mempool.space/. Or for graphs of the mempool fee structure over time, https://mempool.space/graphs/mempool or https://jochen-hoenicke.de/queue/#BTC,1w,weight.

the idea that they should not invest in something they don't understand so they try and learn about bitcoin and in so doing end up doing a bit of a "compare and contrast" exercise with their own currency. A good place to start this journey is with the Beginner's Guide interview "Part 7: Bitcoin's Monetary Policy with Dan Held"[26]. If you want to shortcut the process, buy and read "Broken Money" by Lyn Alden, linked to in Section 2[27], and some of the source material it references[28]. A related misconception is that everyone who got into bitcoin early must be very rich. In most cases, the people who are publicly known to have got into bitcoin early have either sold their bitcoin for a lot less than it is worth today or tried something experimental and lost access to a large percentage of their bitcoin.

- Bitcoin is not just one of a large number of other digital currencies aka cryptocurrencies. "There is bitcoin, and there is everything else". In polite company, other digital currencies can be referred to as altcoins. Some of the differences are highlighted in the Beginners Guide with the title "Part 9: Altcoins, A History of Failure with Nic Carter" which goes through some of the different altcoins[29].

- An argument that seems to have been popular over the last few years (approximately 2020-2023) was "bitcoin wastes energy" which was replied to with "bitcoin uses wasted energy". A good place to start with looking into the intricacies of this topic is the Open Access 2023 review paper "Bitcoin's Carbon Footprint Revisited: Proof of Work Mining for Renewable Energy Expansion" and it's 80+ references as well as a couple of pages of links in the supplementary materials. Most estimates for the amount of energy that bitcoin mining uses are generally under 1% of the worlds energy use in a year[30]. Bitcoin mining is always seeking the lowest cost energy use and, in a free market, this energy is generally going to be "stranded energy"[31], or "excess energy" [32]. In neither case is bitcoin mining "competing" for

[26] The "Bitcoin Dad Pod", a podcast that ran for two years from Feb 2022-Feb 2024, is also a good source for educating yourself in this manner. The podcast has been described by some listeners as "come for the bitcoin news, stay for the macroeconomic chitchat". Each episode has some show notes that contain links to the news and reports that are discussed.

[27] Or the alternative free resources mentioned in the footnotes of that section.

[28] By the way, if you think that your currency is backed by gold then you are probably a generation or more out of date. The last major hold outs were the Swiss who came off the gold standard in 1999. The world's national currencies are now "fiat money". Roughly speaking, a currency for a country is backed by the faith of the people in the state's current monetary policy and the view that this will not change drastically in the future, informed by how it has changed in the past. There are some minor differences with which state needs the people's faith tor supranational currencies, like the Euro, currencies used in a country that does not have it's own national currency, like the Cook Islands, government minted but pegged to other currencies, like Tonga, and the currencies accepted in a country as on par with, or better than, the national one, like the US dollar.

[29] For a more in-depth look of a few of the altcoins after 2020, there is the podcast that uses the more impolite label for altcoins, "Shitcoin Insider". This has a small number of episodes that does not have a set production schedule, currently 9 episodes published 2020-2023, hosted by Guy Swann. The podcast summary is "A Bitcoin Maximalist take on the scams, ponzis, & bad ideas in the world of crypto. Doing the dirty work so that you don't have to."

[30] This is literally within the margin of error as most estimates of the world's energy use have an error margin of +/- 1%.

[31] i.e. not able to be used by conventional energy users

[32] Either the excess supply in a variable supply technology like solar or wind, or the additional supply of a constant supply energy source, like nuclear, when there is less than peak demand

the energy with the normal users of the grid. Another energy argument is that bitcoin mining is using excessive amounts of nonrenewable energy. There are no estimates for the breakdown of energy mix that are not controversial for someone as most assumptions can be argued about so the best you can do is pick a methodology you like and see what the trends over multiple years show. The trends seem to currently be towards more renewable energy resources over time[33].

- As a general rule, online cryptocurrency exchanges are not to be trusted. Bitcoin stored on online exchanges are not yours. At best they are an "IOU" until you withdraw the bitcoin to a self-custodial wallet or is in some other way under your control[34]. There is a long history of online cryptocurrency exchanges going out of business and taking what people think of as "their" cryptocurrencies with them. It seems to be a good rule of thumb that the more different cryptocurrencies they offer, the more likely they are to be exposed to hacks, credit runs, or just out and out scams. However, with bitcoin, you do not have to even trust "bitcoin only" exchanges as you have the option to self-custody your bitcoin. You should do this when you have a nontrivial amount on an exchange that you do not want to immediately spend.

5 Bitcoin in the future

A common saying is that "all it takes for bitcoin to succeed, is for it to not die" and this is a true, but not very useful, statement. In the short term, "tick tock, next block" is an easy way to dismiss news articles that people push on to you with irrelevant information that it is not worth the effort to try and debunk. However, for a more in-depth conversation, you need to define your terms and most importantly what it means to you for bitcoin to "succeed" or "fail"[35]. I want to emphasise that this is inherently a subjective value judgement so these terms are quoted. Below is a short exploration of what I personally mean for bitcoin to "succeed" or "fail" as well as links to different arguments for how or why bitcoin might "fail" that you may want to read through while trying to come to your own conclusions about what these terms mean to you.

for it.

[33] The arguments from a few years ago were about whether 1/3 or 1/2 of bitcoin mining came from renewable energy. The arguments these days seem to be whether it is 1/2 or 2/3 so I would think the trends are moving in the correct direction. One set of data that seems to be somewhere in the middle over time is the one graphed by woocharts.com as "Bitcoin Mining: Usage of Sustainable Energy" with data from the Digital Asset Research Institute.

[34] At worst, it is a scam exchange that allows you to put fiat money in and it looks like you can buy and sell crypto currencies but will not allow you to withdraw them to your own wallet (or withdraw fiat money to your bank account).

[35] A number of "bitcoin is going to die" stories focus on the near term volatility of the price of bitcoin on exchanges when it has taken a significant downturn. In the short-term, this is largely irrelevant but some failure scenarios can be stated in terms of negative price trends over the longer term as it is a proxy for the continuing interest and usefulness people feel bitcoin has.

What it means to me for bitcoin to "succeed" or "fail"

There are a number of one line slogans that are used as shorthand for what values people ascribe to bitcoin. The one I most closely identify with in the context of the long term "success" of bitcoin is "the separation of Money and State"[36]. The minimal condition for this to be the case is that bitcoin is seen as a viable alternative to government backed fiat currency in most parts of the world and that it can be used in trade as money on par with the best such fiat currencies. Ranking currencies by how many people hold them, bitcoin will probably be in the top handful of currencies as the network effects of a successful money drop off sharply as less people hold it[37].

Money has three main properties that we need to keep an eye on for bitcoin's acceptance as such: a store of value over time, a commonly accepted medium of exchange across space, and a unit of account that people naturally think of valuing goods and services in[38]. I would argue that these will slowly come to be seen as true of bitcoin in approximately this order and that it is already widely accepted as at least potentially being a store of value by those who have used their local currency to purchase some. Acknowledged properties for money to be a good medium of exchange include that it be portable, durable, divisible, recognizable, fungible, scarce, and hard to counterfeit - all of which it can be argued bitcoin has[39]. This is just not commonly accepted for bitcoin yet. As for it being a "unit of account", even in the long-term, people may only price things in sats for international transactions when different government backed fiat currencies are in use by the buyer and seller. I would still consider this "success" if it is widespread enough.

Along with this is the idea that the current monetary system is broken and would be better if bitcoin were widely adopted. One of the underlying points of Lyn Alden's Broken Money book is that money started to become different when the speed of information transfer started to outpace the speed of physical goods transfer with the invention of the telegraph. Money originally had a

[36] This was likely coined by a flag waving American as a nod to the phrase "separation of Church and State" that is an interpretation of the first amendment to their constitution, and seemingly a phrase popularised by Thomas Jefferson.

[37] As the number of people in a network doubles, the number of possible transactions between two people in the network quadruples. Or, if you increase the number of people 10x, the possible transaction pairs increases 100x. You could argue about how much value each potential transaction brings to the network but just the potential of the interaction makes the network more useful.

[38] Another property for money is that it be a "standard of deferred payment" but I would argue that a commonly accepted medium of exchange that is also a widely recognised store of value would likely be a natural fit as a standard of deferred payment so we don't need to really mention it when talking about such relationships between individuals. However, this is generally an activity that involves the legal system when it goes wrong so for this standard to be met would generally mean the legal systems around the world would need to be modified. You could also argue that payment of income taxes are a form of "deferred payment" which would mean there would need to be a whole other set of legal modifications if a government wants to directly collect taxes in bitcoin and fulfil this monetary property in it's widest interpretation.

[39] The fungible nature of sats, i.e. one sat is the same as any other, is the most controversial of these properties given the radically transparent nature of bitcoin blockchain transactions. The possibility exists that unspent outputs may be censored or otherwise treated differently due to the inputs that make them up. Some see this as disqualifying sats from being fungible, at the base layer anyway. It would be best going forward to follow the example of the Lightning Network protocol and have additional privacy options available in layers built on top of bitcoin to make them more fungible at the higher layers at least.

physical form that needed to be increasingly abstracted to be of use in such a world. These abstractions lead to a number of weaknesses, the most obvious being that money increasingly became something that could have units created without effort by those in power without the knowledge or consent of those they governed and so one of the primary properties of what make a good money is destroyed. Bitcoin is money that is designed from the first to be transferred over information channels and has a built in issuance schedule with the important property that this would need the consent of all parties to increase the issuance rate. This does not necessarily make it the best money but (like is said of democracy), it seems to me to be the least bad one we've yet come up with for an internet connected world. For bitcoin to "succeed" it will likely take a significant number of people around the world to come to the conclusion that their government backed currency is flawed and/or that bitcoin is better long-term. One obvious way for bitcoin to "fail" therefore is for governments to actually have good fiscal policy and for their people to believe this will continue into the future. I don't see this as likely [40].

A more subtle point is that I would like to see bitcoin do all this while keeping the important properties that I see that it has currently, what I will call "the spirit of bitcoin" for lack of a better term. These are obviously subjective but most of these properties are a direct consequence of the decentralisation of bitcoin at different levels so continuous pushing back against centralisation pressure will be needed for this definition of "success". Centralisation generally makes things more efficient so, as bitcoin runs into more issues around scaling, there will always be a push to have the solution to a scaling issue be more centralisation in some way. Hence why I see the largest long-term threat to bitcoin as being the ongoing debate about how bitcoin should scale and the compromises made to allow it to do so.

Important properties of bitcoin I value i.e. "the spirit of bitcoin"

There are a number of people in bitcoin that have put out a lot of opinions and content over the years. The one that I would align with more than most is Andreas Antonopoulos[41] who has said that bitcoin is "for the other 6 billion"[42]. By this he means that bitcoin should be for those that are not being served by the current financial and banking systems. This could be people that live in a country with an authoritarian, corrupt, or just incompetent government that is destroying an individual's life savings through policies that lead to high inflation. The people may not have banking infrastructure that serves the individual in the community, implicitly, or even explicitly, excluding certain types of people from participating in the banking system. Whatever the reason, these people

[40] See, for example, the list of 56 known hyperinflation events, mostly in the 20th Century, compiled into a 3 page table on pages 12-14 of the Cato Institute working paper titled "World Hyperinflations", published 2012

[41] A 2024 interview available on YouTube, "Block & Key Podcast Episode 1: Is Blockchain Living Up to the Hype? Featuring Andreas Antonopoulos" seeks to summarises his views. If I wanted people to reach the same conclusions as I have, I would suggest that they start by watching one of his talks on YouTube titled "The stories we tell about money". It was given in 2017 in front of an Indian audience in Mumbai and references the 2016 Indian banknote demonetisation that happened a few months earlier.

[42] See the talk on YouTube from 2019 "Universal Access to Basic Finance"

should be able to use bitcoin as an alternative way to transact value within their community, country, and around the world.

So, the desirable properties for bitcoin that Andreas frequently lists[43] are:

- Open
- Borderless
- Neutral
- Censorship Resistant[44]
- Public[45]
- Immutable[46]
- Auditable
- Transparent

In addition, some other properties I believe it is important to explicitly state:

[43] See the talk on YouTube titled "The Five Pillars of Open Blockchains" where he expands on the first 5 somewhat. In some talks, the last three properties are not mentioned or are described as a natural outflow of one of the first five. This list also has some overlap with the properties listed on the bitcoin wiki as the properties that make bitcoin desirable as a low trust medium of exchange.

[44] Almost by definition, this relies in large part on the decentralised nature of bitcoin as, if there is a central point of control, there is likely a way it can be used as a central point to censor. However, even without a practical way to censor bitcoin, it is likely that there will be a lot of emotive arguments about this. There is the meme "bitcoin is money for enemies" as it does not seem there is a way to protect donations to "good" causes, such as human rights activists in authoritarian regimes, without also allowing "bad" transactions, such as donations to terrorists. For example, the concept of "silent payments" can be used by both where the sender can pay to an address that the receiver can spend from but there is no obvious way to associate it as being "owned" by the receiver. My cynical take, as someone who was around for the first internet "Crypto Wars" of the 1990s, is that, as always, the "Four Horseman of the Infocalypse" will be used in bad faith rhetorical arguments to try and "win" the argument to censor bitcoin by different parties for whom it would be advantageous to do so (see Wikipedia articles of the same names for details). Those who push back and point out that it is impossible to do this will be labelled as bad people. It may be that a number of politicians will score points with such rhetoric but it is unlikely there is a practical way to censor bitcoin in the short term. However, it is something that needs to be protected against in the long term. Any potential changes to the protocol need to be designed to make it more decentralised and censorship resistant, not less.

[45] This is in tension with another property that I consider valuable, privacy, but is covered by having pseudonymous transactions on the base chain as mentioned below. Alternatively, a different kind of privacy can come from using the Lightning Network which does not broadcast individual transactions and only has the settlement transaction with a relatively trusted peer broadcast when the channel is closed.

[46] Technically, no bitcoin transactions are actually immutable, it is just that it would take a large amount of energy to undo a transaction by recreating the block containing it and this amount of energy increases the further back in the blockchain it is, quickly becoming excessively expensive. A calculation can be made that allows you to compare how immutable the blockchain is across time. This is sometimes called the "proof of work equivalent days" and is how long it would take to rewrite the entire blockchain using all of the currently estimated mining hash rate. As at the start of 2024, a calculation in Jameson Lopp's yearly report showed this was around 600 days, down a little from the slightly over 2 years it was at the same time the year before (due to the significant increase in the mining hash rate over that year). An up to date graph tracking this metric since the beginning of bitcoin can be found here: https://bitcoin.sipa.be/powdays-ever.png.

- pseudonymous transactions[47]
- easy to use trust minimised self-custodial solutions available[48]
- flexible transaction types
- fast transaction settlement and finality
- low fee transactions that can be used by the disadvantaged of the world and basically not have the poor be second class citizens in the bitcoin world[49]
- bitcoin nodes can predict with reasonable accuracy the next block that a miner will mine and/or from a block that was mined, be able to deduce the algorithm used to choose the transactions that were put into the block using only their own knowledge of the unconfirmed transactions at that time[50]
- easy to use estate planning and management of generational wealth transfer. This seems to be seen currently as a "nice to have" feature and, to some extent, will depend on the laws of different countries. However, in the long term view, there need to be ways for transferring people's bitcoin on to their heirs that actually work and are relatively easy to implement.[51].

[47] There is currently the ability to have pseudonymous transactions in bitcoin but it is not necessary to do so and it is relatively easy to break this. For example, you can create new output addresses for every transaction but if you spend an output and then create a transaction that has the same output again you link the two transactions together. If one of the payments is linked to you for some reason, the other will be as well. The current generation of wallet software makes it easy to use a new output for every transaction and/or makes it hard to reuse an output for multiple transactions. Hopefully this will continue to be the case and the user interface will evolve to protect the user from making simple mistakes like this and add in additional ways of obscuring the linking of transactions to individual entities.

[48] Ease of use is not something that can easily be evaluated but will likely be something that evolves over time. As new software solutions are created they will likely start by being only for experts but hopefully, if they are to succeed, they will become easier to use for a wider audience over time.

[49] I think this is likely to be the property that causes the most contention and potentially bad compromises as the number of users of the bitcoin system scale. There is an argument that fees on the base chain need to increase as the block subsidy decreases over time and so low value transactions and fees will be pushed to higher levels, such as the Lightning Network, that are built on top of bitcoin. The trade offs needed for these higher level protocols may take years to evaluate. For example, the Lightning Network is only now becoming mature enough that we will be able to evaluate in the next few years if the trust minimised self-custodial solutions available are seen by the community of new users to be "easy to use".

[50] This particular point is pushing back against things like the "transaction accelerators" that some of the large mining pools have started advertising where the user can give the miner additional compensation outside of the bitcoin network to include their transaction when they mine a block. This is only really practical when there are a small number of large mining pools so if the mining becomes more decentralised, and/or the miners in the pool create their own block templates, it should not be an issue. However, the fact that it has arisen as presumably an economically valid thing to do implies that bitcoin mining is "not decentralised enough". The ability of other nodes to predict what the next block should be based on their view of the unconfirmed transactions at least allows the ability to have a warning system that this sort of thing is being done, albeit with a few false positives as there is no single view on the totality of unconfirmed transactions. One such attempt is https://miningpool.observer/ with occasional analysis in long blog posts such as those here: https://b10c.me/observations/.

[51] At the present state of immaturity there is no obvious advice that is applicable in all circumstances and in most cases there is tension between having self-custody of your bitcoin

Nuanced reason for bitcoin to "fail"

One argument that has more nuance than a lot of people think is "bitcoin is digital and needs computers and the internet to run. What about when there is no internet or the electricity grid fails?". For bitcoin to fail as a "store of value over time" due to lack of electricity or internet, you're basically talking about an apocalypse scenario and all fiat currencies are worthless at that point anyway. A lot of replies to this argument stop there but, more generously, you could say this would refer to bitcoin being used as a "medium of exchange" in a more narrow sense in a particular time and place where there is patchy internet/power or a local problem that takes away internet access. One difference with bitcoin base layer transactions and transactions on the Lightning Network is that the Lightning Network needs both parties to be online at the time of the transaction. Therefore the option of paying via the Lightning Network is not possible in this scenario. As a comparison with a common electronic payment method in use in the developed world, this would also be an issue with paying using EFTPOS, unless it went to an offline mode called "Electronic Offline Voucher" (EOV) mode. Paying via a standard bitcoin transaction would work in a similar, but potentially more reliable way, to this EOV mode.[52]. If the vendor had their own bitcoin node, that "offline" bitcoin node would still be able to reject an invalid transaction based on it's view of the bitcoin blockchain up until the point in time it went offline.

However, remember the problem we are trying to solve: deciding who owns what, based on an ordering of transactions in an adversarial environment. What if the customer can't be trusted? They may have modified their mobile wallet software to attempt "double spends". In this case, they can buy goods with multiple "offline" vendors by spending the same bitcoin multiple times. Once everyone reconnects to the internet, because the transactions are "valid" in the sense that they do in fact meet the conditions to spend the bitcoin, all the transactions will be broadcast, one will be put into a block and accepted as valid but the others will not. However, if the vendors had internet access in this scenario, the first vendor would broadcast the transaction, and a few seconds later the other vendors would know about it. If the customer tried to spend the same bitcoin with them they would be able to detect this and reject the transaction.

This is potentially better than current EFTPOS systems rolled out for fiat currencies in developed economies in emergency situations but that does not mean it is a good solution. As such it is not viable to use for such transactions in parts of the world where internet access is not common. Building more reliable, fault tolerant, and wider reaching internet and electricity infrastructure is going to need to happen before bitcoin can be successful in a number of places in the

and providing for your heirs to take possession of it. I would suggest that you start by looking into some variant of multi-signature solution, do not let the perfect be the enemy of the good, do not over complicate matters, and provide instructions to your heirs as to how to gain access to your bitcoin after your passing. For some ideas, have a listen to Episode 77 of the Bitcoin Dad podcast "Bitcoin - TNG with Anthony Park".

[52]There is nothing inherent in a bitcoin transaction that means it must be transmitted between customer and vendor via the internet and, people being people, there have been bitcoin transactions passed via carrier pigeon, just to say that it had been done. Any way of transmitting information can be used to pass a bitcoin transaction between customer and vendor. In the scenario where both the customer and vendor were face to face this could be done via QR codes for example.

world where this is currently lacking[53].

Other arguments for why bitcoin will "fail"

- A long list of (mostly bad) arguments and short responses is available at https://safehodl.github.io/failure/.
- A short list of good arguments is given in Chapter 26 of Broken Money as risks to be aware of and keep track of with reasons why the author is not too worried about them at the time the book was written:
  - RISK 1: MARKET DILUTION
  - RISK 2: CRITICAL SOFTWARE BUGS
  - RISK 3: GOVERNMENT BANS
  - RISK 4: COMPUTATIONAL THREATS
- In the early days of bitcoin, the same problems were bought up again and again and so a set of dice were made to be a "tongue in cheek" way of disparaging people thinking they were being original in making them. "Part 15: Bitcoin FUD with Nic Carter" in the Beginners Guide series is an interview with the creator of these dice revisiting these arguments. In around half the cases they basically say that there is some relevance to the argument.
- My own number one issue is the same problem that was bought up the very first time bitcoin was introduced to the world: "bitcoin won't scale". At different points in time there have been different problems with scaling that have been solved through various means and with various trade offs. They have never been solved until they became a problem and there is no guarantee that this will continue to happen or that the trade offs will be ones that keep the "spirit of bitcoin" as I perceive it. I don't think this is a large risk over the course of a few years but over the course of decades it may be that compromises made to allow more people to do a larger variety of transactions with bitcoin will lead to something that falls short of what I see as the potential of bitcoin.

6 Additional information about bitcoin scaling

Originally, the software for running the bitcoin network was written by one person, Satoshi, and presumably only run by them as well. When it was made

[53]Obviously physical cash is the current solution to this problem but it is slowly being displaced by electronic representations where it can be in countries with good infrastructure e.g. where EFTPOS can be rolled out. If you live in such a country, there are probably less banknotes representing your money than you think. There are a number of different measurements of money supply , see linked Wikipedia article, that can vary slightly between countries, and different countries report different ones, but the standard M0 is generally physical banknotes with the M1, M2, and M3 definitions becoming more abstract and including more things, but all are a form of nonphysical money, see the appropriate list on the https://tradingeconomics.com/indicators webpage. Note that the figures on the linked website were collected from official sources all over the internet but they are not necessarily checked by a human as I found an obvious error with a 35x spike in the amount of NZ M0 supply in February 2017, compared to other values for that year.

available to others, they started using it with Hal Finney being the next person known to be running the software[54]. As more people used the software, they found bugs that they wanted to fix, or features they wanted added, and originally sent patches to Satoshi via email. Eventually, multiple people were given access to make changes to the code of this software project. As more people became involved, they started to specialise in what they wanted to do with the software and eventually terminology was created to describe different parts of the software and these pieces of the software were sometimes spun off into their own projects, most of which centralised something initially as it made things easier. The successor to the original Satoshi client, Bitcoin Core, has come to be called the "reference implementation" in recognition of this.

Mining and Wallets - creation of whole new products

One of the first distinct groups to be recognised were people doing mining and the software they needed to do so. It was of benefit to the individuals that they had the best software with which to do the mining and to take the mining code from the Satoshi client and tweak it so it worked faster on their hardware. Eventually the bitcoin mining competition got large enough that it switched from running on general purpose CPUs, to GPUs, and then purpose built ASIC machines. The CPU mining functionality was finally turned off in Bitcoin Core in the 2016 release in recognition of the fact that CPU based mining had not been viable for a long time and this part of the software ecosystem was mature enough and had enough competition that the Bitcoin Core version was not needed. As the number of miners increased, the profits for an individual miner became less regular so mining pools were formed and software to coordinate them was also developed. Initially, as it was easier, the software was developed such that the mining pool coordinator would create the block template and give it to the participants. Lately, a new version has been developed[55] that gives some power back to the miners to pick the block template.

Another piece of the software identified as being useful to have multiple implementations of came to be called "wallets". Originally, the user would have to create and record the public key and private key for every new output they sent bitcoin to so they could later spend it. However, in approximately 2013, there was the growth of standalone wallet software that needed a better way to do this. As the number of software wallet projects grew, there also grew a need for importing and exporting sets of keys between them. A number of standards were proposed and the concept of the hierarchical deterministic (HD) wallet[56] was created where there was effectively infinite sets of public and/or private keys generated from an initial seed, which could be recorded as a set of words[57].

[54] In order to prove that the first public version of the software, and the blockchain based on it, was not created before a certain date, the initial genesis block that is built into the software references a headline from a UK newspaper: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks." The genesis block hash value that is needed to link it to the next block in the chain would have needed to be recalculated if this message was added in later so this proves that no blocks of the bitcoin blockchain could have been created before this date. Hal Finney publicly posted that he was running the bitcoin software on the 11th of January 2009.

[55] It is called Stratum V2. For technical details, see the documentation here:https://stratumprotocol.org/docs/

[56] For technical details, see the Learn Me a Bitcoin webpage on HD Wallets.

[57] The downside to this is that the standard was in flux and so different software defaulted

Note that standalone wallet software, and later hardware wallets, needs to know about the blockchain from a trusted source. A lot of software has the ability to nominate your own bitcoin node but a simpler method is to have the software talk back to a node, or network of nodes, maintained by the people providing the software[58].

The Fork Wars - increasing transaction throughput

During the time period approximately 2015-2017, there was a "civil war" amongst the bitcoin community that I will call "The Fork Wars"[59]. The original Satoshi client had no explicit block size limit but did have an implicit 32MB one i.e. things would crash if a block that was bigger than 32MB were created and transmitted around the network. Satoshi implemented a 1MB block size limit without much explanation early on but it is generally agreed that this was in

to different derivation paths so you may want to note down the software you use and/or the derivation path along with your seed words so you can restore to a different wallet. One resource for trying to figure this out after the fact is https://walletsrecovery.org/. One benefit to the HD Wallet model is that you can have a "watch only wallet" where it can derive public keys but not the matching private keys so you can monitor your bitcoin without the ability to spend it.

[58] There has also been a concerted effort to refactor the Bitcoin Core code so that the code referring specifically to consensus rules was all in one library which would mean others could take this core code and make additional "node" implementations in a similar way to the way mining and wallets have been spun off. This is currently called the libbitcoinkernel project. For a high level view of where the different parts of the consensus code are within the Bitcoin Core code base, as at the end of 2023, see the list under the Consensus Mechanism section in the BitPublica Bitcoin Mining Newsletter article "Understanding the Bitcoin Source Code". There are other node implementations out there, such as BTCD, that have rewritten everything from scratch but it would have been easier, and there would likely be more, if the core consensus code was in a single place within the reference implementation for them to refer to or build on.

[59] This time period is more commonly called "The Blocksize Wars" but I think this detracts from what the core philosophical differences were. It doesn't help that one of the most recommended books on that time is "The Blocksize War" by Jonathan Bier. It was put up on the Bitmex blog one chapter at a time, between March 22, 2021 and August 8, 2021. However the chapters did not link to each other so here is a full set of links to all 21 chapters: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21. The book itself recognises the complicated issues at play but it unfortunately calls the sides "small blockers" and "big blockers" even though both sides were agreed a block size increase was needed. From the first chapter of the book: "This war over the blocksize would shatter and split the ecosystem over the next two years. As the war progressed, it emerged that the struggle was perhaps more complex than just the maximum size of blocks; the battle went right to the core of Bitcoin's DNA. The contention was essentially about four somewhat interrelated issues:

1. The level of blockspace available in each Bitcoin block – Essentially, whether the eventual state should consist of surplus capacity available in the blocks, or consistently full blocks.
2. How to modify the rules of the Bitcoin protocol – Whether the rules on the validity of Bitcoin blocks should change relatively easily, or whether they should be more robust and only change in exceptional circumstances, with broad support from all interested parties.
3. The significance of the nodes of ordinary users – The extent to which, if any, validating nodes of the ordinary end users had a say in enforcing Bitcoin's protocol rules.
4. Time preferences – Whether Bitcoin was like a tech startup which should prioritise gaining market share in the short term; or if it was a long-term project, a new global money, and one should think decades ahead when making decisions."

part to stop a denial of service attack from a hostile actor[60]. By 2015 it was generally agreed that 1MB blocks were or would soon be full with transactions from the "good" participants of the bitcoin network, even without taking into account any attackers who would want to create spurious transactions for their own ends[61]. The general consensus was that an increase of the block limit to at least 2MB was needed. The question that people had was how to do this. Nominally this was about a block size increase but I consider that it was fundamentally about how bitcoin should be changed. In today's terms, should it be a soft fork or a hard fork? The big problem is that, while these terms existed at the time, some of the subtleties were not so well defined and there was a lot of miscommunication during this time, in part because of this[62].

A hard fork is a change to the bitcoin rules that is not backwardly compatible as it is a loosening of the rules and, when a block following this changed rule is created, if everyone checking the rules is not upgraded, it guarantees there will be a chain split. A block size increase seems to obviously need a hard fork. A soft fork, on the other hand, is a change to the bitcoin rules that is backwardly compatible as it is a tightening of the rules and, when a block with this changed rule is created, a chain split is not guaranteed to happen if not everyone has upgraded. With a hard fork, you have to have a set of people who are "in charge" and coordinating that everyone is upgrading. With a soft fork, you need to have a minimal set of nodes that are checking the new rules to avoid a chain split[63].

In this particular set of circumstances, the hard fork was driven by the businesses who thought they would lose money if the block size was not increased,

[60] One of the interesting things that happened during the period of the "Fork Wars" was that both sides tried to use quotes from Satoshi's public comments to bolster their case in an "appeal to authority". Maybe because of this, in arguments that happened after this, the perceived original vision of what Satoshi wanted was given less credence.

[61] I have not mentioned in the main text the OP_RETURN Wars which were the debates that raged when it was discovered that transactions could be created that could be used to store arbitrary data in the blockchain. A compromise was reached where the code OP_RETURN was used at the start of the bitcoin script condition for spending an output and then up to 80 bytes of data could be added. The transaction output this was attached to was known to not be spendable so could be ignored by a node if they wished. As it was not spendable, the value associated with the output would normally also be set to 0. Data put into the blockchain this way includes the bitcoin white-paper pdf itself and the script used to do so. To see how to extract this, see the answers to the bitcoin stack exchange question "How is the whitepaper decoded from the blockchain (Tx with ~1000x m of n multisig outputs)".

[62] One side would say "everyone should be able to run a node" and the other side would push back with "hardly anyone needs to run a node". These two statements can both be true. The latter however is underpinned with the assumption "everyone is like me" while the former is more inclusive. Given that the argument was generally between people in relatively privileged circumstances, I came down on the side of those that by default did not exclude the underdogs of the world.

[63] There were previous chain splits in bitcoin's history due to accidental hard and soft forks that could be referenced in these discussions, but normally they were not described as such. For example, see the approximately 12 minute digression in the talk "Consensus Algorithms, Blockchain Technology and Bitcoin" by Andreas Antonopoulos starting at around the 54 minute mark. He first describes an accidental hard fork based chain split that happened in March 2013. It required an emergency online meeting of bitcoin node operators in order to coordinate how to fix it. It was severe enough that it is sometimes considered the last time the bitcoin network as a whole was "offline". He then describes an accidental soft fork based chain split that was happening at the time of the talk, in July 2015, due to the BIP66 soft fork upgrade. It did not require any coordination to fix and only caused minor "instability" in the network for a week or so. This meant that in some cases when doing a high value transaction, it would be recommended to wait for 2 hours before considering it final, rather than the more normal 1 hour. It ended up being such a nonevent that it is hard to find many details on it.

and they obviously thought they should be in charge of the upgrade. Initially, there was no soft fork proposal, just a push back that this was a dangerous thing to do. So the hard fork side got by default all those with less conservative views on the block size increase and had people who wanted a one off increase to 2MB, those who wanted a forever doubling of the block size limit on a schedule, and all those in between.

When a soft fork proposal was put together, called Segregated Witness, or "SegWit", it was a complicated but elegant hack[64] that needed to have the miners implement it first[65] in order to not cause a chain split. It also fixed the final obstacle that would allow the Lightning Network to be built on top of bitcoin to take the smallest transactions off the blockchain[66]. The people who started the discussion wanted a 2MB block size limit and SegWit would effectively do it without the need for a hard fork[67]. By this time though there was so much miscommunication and mistrust between the two sides, and the more radical block size increase contingent had dug their heels in about wanting a hard fork, that this was not an acceptable solution.

After a long series of events, the network finally forked in August 2017, doing both a hard fork and a soft fork. The bitcoin network split with a hard fork on August 1st 2017, and the fork using the original rule set was upgraded via the SegWit soft fork on 24 August 2017. The hard fork was given the name Bitcoin Cash and has become an "also ran" in the larger cryptocurrency world[68].

[64] There are a lot of descriptive words used to describe the SegWit proposal but I chose the ones I did because by "hack" I mean it is probably not the way that you would go about designing a protocol from first principles. However, I also call it "elegant" because each design decision solves multiple problems. For a technical overview of some of these design decisions, listen to the first half of the Bitcoin.Review podcast Episode 29 "SegWit, Taproot, Schnoor, Inscriptions & Witness Discount ft. Andrew Poelstra & Adam Gibson", available multiple places, including on Youtube.

[65] One of the possible sources of confusion during this time is that both hard and soft forks needed the miners to implement their ideas before anything could happen.

[66] It took a few years for the Lightning Network to grow after initial software was released for it at the end of the Fork Wars. Initially there were only a few nodes, and then it was difficult to find a path to route payments around the network because the nodes that were available were not connected or did not have the appropriate capacity to do so. It has now got to the point where routing failures are rare and the Lightning Network can reliably route most small to mid size payments. Due to the privacy offered by the nature of the Lightning Network, there is no good way to get an accurate count of how many transactions are conducted over it. However, one of the companies that run some of the largest publicly known Lightning Network nodes, River, produced a report in 2023 that included a lower estimate. The title of the report is "The Lightning Network Grew by 1212% in 2 Years - Why It's Time to Pay Attention" with the executive summary including the statement "we estimate a lower bound of 6.6 million routed Lightning transactions in August 2023."

[67] A SegWit transaction stores the conditions for spending the transaction in a new part of the block that would not be seen by non-SegWit nodes. This means that a node that was not upgraded will see it as an "anyone can spend" transaction. A block full of "typical" SegWit transactions was calculated to have 1MB used in the normal part of the block and another 1MB in the other part of the block for a total of 2MB (although the actual new maximum block size limit was 4MB).

[68] From Chapter 21 of "The Blocksize War": "...in spite of these efforts, the coin never really gained traction compared to Bitcoin. Over the next few years, Bitcoin Cash underperformed Bitcoin with respect to price. Not only that, but Bitcoin Cash even had lower on-chain transaction volume than Bitcoin, when on-chain throughput and a blocksize limit increase was said to be the primary driver behind the coin. Even worse, by March 2018 it emerged that Bitcoin Cash on-chain volume was even lower than SegWit volume on Bitcoin. SegWit had increased on-chain transaction volume faster than Bitcoin Cash...In part due to the difficulties of conducting a hardfork in Bitcoin, the Bitcoin Cash community opted for a different

Taproot - increasing transaction complexity

One type of transaction that bitcoin can do is a multiple signature, or "multi-sig", transaction where a threshold number of private keys must sign a transaction in order to spend the bitcoin. Due to the way this was initially implemented there were a maximum number of 15 signatures and the larger the number of signatures, the larger the transaction. Another waste of space in bitcoin transactions was that if you had multiple sets of conditions that could be fulfilled to spend an output, they all had to be revealed when it was spent, not just the condition that was met. Enhancements to these were proposed under the name of the "Taproot" soft fork. A new signature scheme was created so that no matter how many signatures were used, they took up the same number of bytes, and could be processed faster than the older method[69]. More complicated sets of spending conditions could also be created with a new Tapscript variant of the bitcoin scripting language. Only the single condition that was actually used would need to be revealed with the others being summarised by the appropriate set of hashes. There was also a transaction size limit that was relaxed so that a single transaction could in theory be as large as the new 4MB SegWit block limit[70].

This was a relatively uncontested proposal and implementation, due in part to one of the features of the SegWit upgrade being that it made other large soft forks easy with the use of a version number[71] . There was a soft fork coordination method that had been developed during the Fork Wars called "Speedy Trial" that allowed it to be relatively quickly activated at the end of 2021[72].

---

approach. They conducted a hardfork every six months, in May and November of each year. In November 2018, just over one year since Bitcoin Cash had launched, there were tensions in the Bitcoin Cash community... Exploiting the scheduled hardfork date of November 15, Bitcoin Cash split into two coins... As a result of the split and the resulting uncertainty, the value of Bitcoin Cash compared to Bitcoin continued to decline. Just as the small blockers had expected, some of the large blockers began to slowly see merit in the idea that, in the event of a dispute over the rules, the original rule set is a key schelling point [see the Wikipedia article "Focal point (game theory)"]. If one diverts from this philosophy, the risk is that the coin continues to split into smaller and smaller factions. The large blockers were painfully experiencing this first-hand. "

An alternate version of this time of bitcoin history is told by one of the players who ultimately ended up on the Bitcoin Cash side of things in the book "Hijacking Bitcoin" by Roger Ver.

[69] Depending on how you build the transaction there are different limits on the number of signatures you can have, but they are much larger than the previous limit of 15. The most obvious limit being only 999 signatures can be combined and checked in a "simplistic threshold number of signatures" transaction due to a stack size limit of 1000.

[70] This was done to make it feasible to do automatic formal verification and optimisation of Tapscript scripts but there ended up being an unintended consequence of this. Previously, if someone wanted to store a large amount of data in the blockchain, they would have to do it in a number of transactions and there was no guarantee the transactions would be ordered they way they wanted, unless it was done by a miner themselves. With the transaction size limit removed, it meant that now arbitrary data up to 4MB could be stored in a block just by paying a competitive fee.

[71] The original SegWit soft fork was SegWit version 0. At the time, a transaction output with a SegWit version that was anything other than 0 was deemed to be "anyone can spend" but if it was version 0 a stricter set of rules were checked. Taproot was implemented as SegWit version 1 and the rule amended to anything that had a SegWit version that wasn't 0 or 1 was deemed to be "anyone can spend" but stricter rules were applied to version 0 and 1 .

[72] There were many articles discussing the Taproot soft fork at the time but one of the most comprehensive is the Cointelegraph article "A Beginners Guide to the Taproot Upgrade". For a technical overview, listen to the second half of the Bitcoin.Review podcast episode 29

A future store of value due to scaling to more users, not just scaling transactions

There has recently been a number of "spot ETFs" approved. The ones that made the most news were the 11 approved at once in the US at the start of 2024 but there have been others, both before and after these highly reported ones. Roughly speaking, buying and selling of shares in these Exchange Traded Funds[73] (ETFs) result in a nominated custodian buying and selling bitcoin on your behalf. This allows those for whom the current financial system is already working to have some ability to be exposed to the risks and rewards of the changes in price of bitcoin. This can be seen as a way of scaling bitcoin to more people and exposing them to the idea that bitcoin is a "store of value". However, this is both custodial and not something the "other 6 billion" can do. So, in my value system, it is not one of the more important uses of bitcoin but it is interesting to think about why people would want to invest in these ETFs[74].

You can see the "store of value" monetary property of bitcoin as being a circular reference i.e. people think bitcoin will have value in the future because people think bitcoin has value in the present and that will continue into the future. This is likely how most investing in the ETFs see things. However, I don't think this is the whole story. The value of bitcoin had to start somewhere and it is not so far in the past that we can't have a good guess as to what it was. In my view, the first people to think bitcoin had value, thought it did so based on it's use in a possible future as a medium of exchange that could happen over the internet. This continues and some of the value as a "store of value" property is still based on the perceived "medium of exchange" property of bitcoin. This is, in turn, based on the size of the network of users and the variety of transactions they can potentially engage in.

As more people saw potential use for bitcoin, it gained value due to it having a large enough network of users that it could actually function as a medium of exchange over the internet in some niche markets. As it became used enough that transactions had fees, this functioning as a medium of exchange was restricted, as there was now a lower limit on the value of a transaction that it was viable to do at some points in time. The creation of the Lightning Network and the subsequent migration of very low value transactions on to this network put this problem off for a while, possibly as much as a decade, but it is likely that we have now passed the point where there will be blocks that will regularly have transactions at less than the nominal fee of 1 sat/vbyte level[75]. During this time, the number of users of bitcoin has increased so the network effects have also increased and the price of bitcoin has increased, at least in part, to reflect the increased potential transaction partners.

The Lightning Network requires the participant to have bitcoin on the base chain and they need to make a base chain transaction to enter or exit the Lightning Network. As the price of bitcoin increases in fiat currency terms, and

"SegWit, Taproot, Schnoor, Inscriptions & Witness Discount ft. Andrew Poelstra & Adam Gibson".

[73] See Wikipedia article titled "Exchange-traded fund"

[74] It can be argued that ETFs and the large amount of money that can easily flow through them may potentially be a stabilising influence on the price volatility of bitcoin over the short and medium term which is likely a net good.

[75] According to a long running mempool.space graph, the last time the mempool had cleared of all pending transactions at or above 1 sat/vbyte was at the start of 2023.

the transaction fees increase in bitcoin terms, there will come a time when new people cannot participate in the Lightning Network. In the short term there are compromises that can be made with custodial services. These are not solutions I see as being in the "spirit of bitcoin" that I want to support, and so I see the need for better solutions. In short, there is an obvious need for a new way to scale the number of people who can self-custody their own bitcoin and transact with it in smaller amounts without compromising the best aspects of the current bitcoin network.

If this is not solved, then the "medium of exchange" property of bitcoin is lessened and it becomes a less attractive "store of value" and more likely to stay a niche product. In this case bitcoin will not reach it's ultimate potential as a world wide medium of exchange of value of almost any amount. On the other hand, each successful round of scaling will eventually just lead to another round of scaling being needed as the bitcoin network becomes more useful to more people for more transactions.

As more people are involved with bitcoin, it becomes harder to come to agreement on any changes that are needed. In the short term this means that nothing changes until and unless there is overwhelming agreement. I consider this to be generally a good thing. However, in the long term, this may mean that any changes that are needed are delayed or that the "easy" path is chosen that leads to more centralisation or trade offs that go against what I see as the "spirit of bitcoin". Hence why I think that the major risks to bitcoin over the long term will come from the rounds of arguments, discussions, and decisions needed in order to enable another round of scaling.

7 Resources for keeping up to date with new developments

A large number of sources of bitcoin news start up one year and stop the next. Therefore, these are a couple that have existed for multiple years and so it can be assumed they will continue to exist.

- To keep up with low level technical discussions and changes, without taking up too much time, read the weekly Bitcoin Optech newsletter or listen to the related podcast that discusses the items in the newsletter[76].
- To keep up to date on what is considered relevant on lots of different topics around bitcoin, the "Bitcoin Audible" podcast is good to monitor. It is primarily episodes that are Guy Swann doing an audio reading of an article and then a monologue on it. The podcast notes will also have a link to the original article.

[76] You can access archived versions and sign up to receive new episodes of both from links on the https://bitcoinops.org/en/publications/ webpage