6.824 Bitcoin FAQ

Q: I don't understand why the blockchain is so important. Isn't the requirement for the owner's signature on each transaction enough to prevent bitcoins from being stolen?

A: The signature is not enough, because it doesn't prevent the owner from spending money twice: signing two transactions that transfer the same bitcoin to different recipients. The blockchain acts as a publishing system to try to ensure that once a bitcoin has been spent once, lots of participants will know, and will be able to reject a second spend.

Q: Why does Bitcoin need to define a new currency? Wouldn't it be more convenient to use an existing currency like dollars?

A: The new currency (Bitcoins) allows the system to reward miners with freshly created money; this would be harder with dollars because it's illegal for ordinary people to create fresh dollars. And using dollars would require a separate settlement system: if I used the blockchain to record a payment to someone, I still need to send the recipient dollars via a bank transfer or physical cash.

Q: Why is the purpose of proof-of-work?

A: It makes it hard for an attacker to convince the system to switch to a blockchain fork in which a coin is spent in a different way than in the main fork. You can view proof-of-work as making a random choice over the participating CPUs of who gets to choose which fork to extend. If the attacker controls only a few CPUs, the attacker won't be able to work hard enough to extend a new malicious fork fast enough to overtake the main blockchain.

Q: Could a Bitcoin-like system use something less wasteful than proof-of-work?

A: Proof-of-work is hard to fake or simulate, a nice property in a totally open system like Bitcoin where you cannot trust anyone to follow rules. There are some alternate schemes; search the web for proof-of-stake or look at Algorand and Byzcoin, for example. In a smallish closed system, in which the participants are known though not entirely trusted, Byzantine agreement protocols could be used, as in Hyperledger.

Q: Can Alice spend the same coin twice by sending "pay Bob" and "pay Charlie" to different subsets of miners?

A: Suppose Alice does that. One of the two subsets of miners is likely to find the nonce for a new block first. Let's assume the first block to be found is B50 and it contains "pay Bob". This block will be flooded to all miners, so the miners working on "pay Charlie" will switch to mining a successor block to B50. These miners validate transactions they place in blocks, so they will notice that the "pay Charlie" coin was spent in B50, and they will ignore the "pay Charlie" transaction. Thus, in this scenario, double-spend won't work.

There's a small chance that two miners find blocks at the same time, perhaps B50' containing "pay Bob" and B50'' containing "pay Charlie". At this point there's a fork in the block chain. These two blocks will be flooded to all the nodes. Each node will start mining a successor to one of them (the first it hears). Again the most likely outcome is that a single miner will finish significantly before any other miner, and flood the successor, and most peers will switch to that winning fork. The chance of repeatedly having two miners simultaneously find

blocks gets very small as the forks get longer. So eventually all the peers will switch to the same fork, and in that fork there will be only one spend of the coin.

The possibility of accidentally having a short-lived fork is the reason that careful clients wait until there are a few successor blocks before believing a transaction.

Q: It takes an average of 10 minutes for a Bitcoin block to be validated. Does this mean that the parties involved aren't sure if the transaction really happened until 10 minutes later?

A: Yes. The 10 minutes is awkward. But it's not always a problem. For example, suppose you buy a toaster oven with Bitcoin from a web site. The web site can check that the transaction is known by a few servers, though not yet in a block, and show you a "purchase completed" page. Before shipping it to you, they should check that the transaction is in a block. For low-value in-person transactions, such as buying a cup of coffee, it's probably enough for the seller to ask a few peers to check that the bitcoins haven't already been spent (i.e. it's reasonably safe to not bother waiting for the transaction to appear in the blockchain at all). For a large in-person purchase (e.g., a car), it is important to wait for sufficiently long to be assured that the block will stay in the block chain before handing over the goods.

Q: What can be done to speed up transactions on the blockchain?

A: I think the constraint here is that 10 minutes needs to be much larger (i.e. >= 10x) than the time to broadcast a newly found block to all peers. The point of that is to minimize the chances of two peers finding new blocks at about the same time, before hearing about the other peer's block. Two new blocks at the same time is a fork; forks are bad since they cause disagreement about which transactions are real, and they waste miners' time. Since blocks can be pretty big (up to a megabyte), and peers could have slow Internet links, and the diameter of the peer network might be large, it could easily take a minute to flood a new block. If one could reduce the flooding time, then the 10 minutes could also be reduced.

Q: The entire blockchain needs to be downloaded before a node can participate in the network. Won't that take an impractically long time as the blockchain grows?

A: It's true that it takes a while for a new node to get all the transactions. But once a given server has done this work, it can save the block chain, and doesn't need to fetch it again. It only needs to know about new blocks, which is not a huge burden. On the other hand most ordinary users of Bitcoin don't run full Bitcoin nodes; instead they trust a few full nodes to answer questions about whether coins have already been spent.

Q: Is it feasible for an attacker to gain a majority of the computing power among peers? What are the implications for bitcoin if this happens?

A: It may be feasible; some people think that big cooperative groups of miners have been close to a majority at times: http://www.coindesk.com/51-attacks-real-threat-bitcoin/

If >50% of compute power is controlled by a single entity, they can double-spend bitcoins: transfer a coin to one payee, and then generate a new fork from before that transaction in which the transaction doesn't exist. Bitcoin's security would be broken if this happened.

Q: From some news stories, I have heard that a large number of bitcoin miners are controlled by a small number of companies.

A: True. See here: https://blockchain.info/pools. It looks like three mining pools together hold >51% of the compute power today, and two come to 40%.

Q: Are there any ways for Bitcoin mining to do useful work, beyond simply brute-force calculating SHA-256 hashes?

A: Maybe -- here are two attempts to do what you suggest:
https://www.cs.umd.edu/~elaine/docs/permacoin.pdf
http://primecoin.io/

Q: There is hardware specifically designed to mine Bitcoin. How does this type of hardware differ from the type of hardware in a laptop?

A: Mining hardware has a lot of transistors dedicated to computing SHA256 quickly, but is not particularly fast for other operations. Ordinary server and laptop CPUs can do many things (e.g. floating point division) reasonably quickly, but don't have so much hardware dedicated to SHA256 specifically. Some Intel CPUs do have instructions specifically for SHA256; however, they aren't competitive with specialized Bitcoin hardware that massively parallelizes the hashing using lots of dedicated transistors.

Q: The paper estimates that the disk space required to store the block chain will by 4.2 megabytes per year. That seems very low!

A: The 4.2 MB/year is for just the block headers, and is still the actual rate of growth. The current 60+GB is for full blocks.

Q: Would the advent of quantum computing break the bitcoin system?

A: Here's a plausible-looking article:
http://www.bitcoinnotbombs.com/bitcoin-vs-the-nsas-quantum-computer/
Quantum computers might be able to forge bitcoin's digital signatures (ECDSA). That is, once you send out a transaction with your public key in it, someone with a quantum computer could probably sign a different transaction for your money, and there's a reasonable chance that the bitcoin system would see the attacker's transaction before your transaction.

Q: Bitcoin uses the hash of the transaction record to identify the transaction, so it can be named in future transactions. Is this guaranteed to lead to unique IDs?

A: The hashes are technically not guaranteed to be unique. But in practice the hash function (SHA-256) is believed to produce different outputs for different inputs with fantastically high probability.

Q: It sounds like anyone can create new Bitcoins. Why is that OK? Won't it lead to forgery or inflation?

A: Only the person who first computes a proper nonce for the current last block in the chain gets the 12.5-bitcoin reward for "mining" it. It takes a huge amount of computation to do this. If you buy a computer and have it spend all its time attempting to mine bitcoin blocks, you will not make enough bitcoins to pay for the computer.

Q: The paper mentions that some amount of fraud is admissible; where does this fraud come from?

A: This part of the paper is about problems with the current way of paying for things, e.g. credit cards. Fraud occurs when you buy something on the Internet, but the seller keeps the money and doesn't send you the item. Or if a merchant remembers your credit card number,

and buys things with it without your permission. Or if someone buys something with a credit card, but never pays the credit card bill.

Q: Has there been fraudulent use of Bitcoin?

A: Yes. I think most of the problems have been at web sites that act as wallets to store peoples' bitcoin private keys. Such web sites, since they have access to the private keys, can transfer their customers' money to anyone. So someone who works at (or breaks into) such a web site can steal the customers' Bitcoins.

Q: Satoshi's paper mentions that each transaction has its own transaction fees that are given to whoever mined the block. Why would a miner not simply try to mine blocks with transactions with the highest transaction fees?

A: Miners do favor transactions with higher fees. You can read about typical approaches here:
https://en.bitcoin.it/wiki/Transaction_fees
And here's a graph (the red line) of how long your transaction waits as a function of how high a fee you offer:
https://bitcoinfees.github.io/misc/profile/

Q: Why would a miner bother including transactions that yield no fee?

A: I think many don't mine no-fee transactions any more.

Q: How are transaction fees determined/advertised?

A: Have a look here:
https://en.bitcoin.it/wiki/Transaction_fees
It sounds like (by default) wallets look in the block chain at the recent correlation between fee and time until a transaction is included in a mined block, and choose a fee that correlates with relatively quick inclusion. I think the underlying difficulty is that it's hard to know what algorithms the miners use to pick which transactions to include in a block; different miners probably do different things.

Q: What are some techniques for storing my personal bitcoins, in particular the private keys needed to spend my bitcoins? I've heard of people printing out the keys, replicating them on USB, etc. Does a secure online repository exist?

A: Any scheme that keeps the private keys on a computer attached to the Internet is a tempting target for thieves. On the other hand, it's a pain to use your bitcoins if the private keys are on a sheet of paper. So my guess is that careful people store the private keys for small amounts on their computer, but for large balances they store the keys offline.

Q: What other kinds of virtual currency were there before and after Bitcoin (I know the paper mentioned hashcash)? What was different about Bitcoin that led it to have more success than its predecessors?

A: There were many previous proposals for digital cash systems, none with any noticeable success. It's tempting to think that Bitcoin has succeeded because its design is more clever than others: that it has just the right blend of incentives and decentralization and ease of use. But there are too many failed yet apparently well-designed technologies out there for me to believe that.

Q: What happens when more (or fewer) people mine Bitcoin?

A: Bitcoin adjusts the difficulty to match the measured compute power

devoted to mining. So if more and more computers mine, the mining difficulty will get harder, but only hard enough to maintain the inter-block interval at 10 minutes. If lots of people stop mining, the difficulty will decrease. This mechanism won't prevent new blocks from being created, it will just ensure that it takes about 10 minutes to create each one.

Q: Is there any way to make Bitcoin completely anonymous?

A: Have a look here: https://en.wikipedia.org/wiki/Zerocoin

Q: If I lose the private key(s) associated with the bitcoins I own, how can I get my money back?

A: You can't.

Q: What do people buy and sell with bitcoins?

A: There seems to be a fair amount of illegal activity that exploits Bitcoin's relative anonymity (buying illegal drugs, demanding ransom). You can buy some ordinary (legal) stuff on the Internet with Bitcoin too; have a look here:
http://www.coindesk.com/information/what-can-you-buy-with-bitcoins/
It's a bit of a pain, though, so I don't imagine many non-enthusiasts would use bitcoin in preference to a credit card, given the choice.

Q: Why is bitcoin illegal in some countries?

A: Here are some guesses.

Many governments adjust the supply of money in order to achieve certain economic goals, such as low inflation, high employment, and stable exchange rates. Widespread use of bitcoin may make that harder.

Many governments regulate banks (and things that function as banks) in order to prevent problems, e.g. banks going out of business and thereby causing their customers to lose deposits. This has happened to some bitcoin exchanges. Since bitcoin can't easily be regulated, maybe the next best thing is to outlaw it.

Bitcoin seems particularly suited to certain illegal transactions because it is fairly anonymous. Governments regulate big transfers of conventional money (banks must report big transfers) in order to track illegal activity; but you can't easily do this with bitcoin.

Q: Why do bitcoins have any value at all? Why do people accept it as money?

Because other people are willing to sell things in return for bitcoins, and are willing to exchange bitcoins for ordinary currency such as dollars. This is a circular argument, but has worked many times in the past; consider why people view baseball trading cards as having value, or why they think paper money has value.

Q: How is the price of Bitcoin determined?

A: The price of Bitcoin in other currencies (e.g. euros or dollars) is determined by supply and demand. If more people want to buy Bitcoins than sell them, the price will go up. If the opposite, then the price will go down. There is no single price; instead, there is just recent history of what prices people have been willing to buy and sell at on public exchanges. The public exchanges bring buyers and sellers together, and publish the prices they agree to:

  https://bitcoin.org/en/exchanges

Q: Why is the price of bitcoin so volatile?

A: The price is driven partially by people's hopes and fears. When they are optimistic about Bitcoin, or see that the price is rising, they buy so as not to miss out, and thus bid the price up further. When they read negative news stories about Bitcoin or the economy in general, they sell out of fear that the price will drop and cause them to lose money. This kind of speculation happens with many goods; there's nothing special about Bitcoin in this respect. For example:

  https://en.wikipedia.org/wiki/Tulip_mania