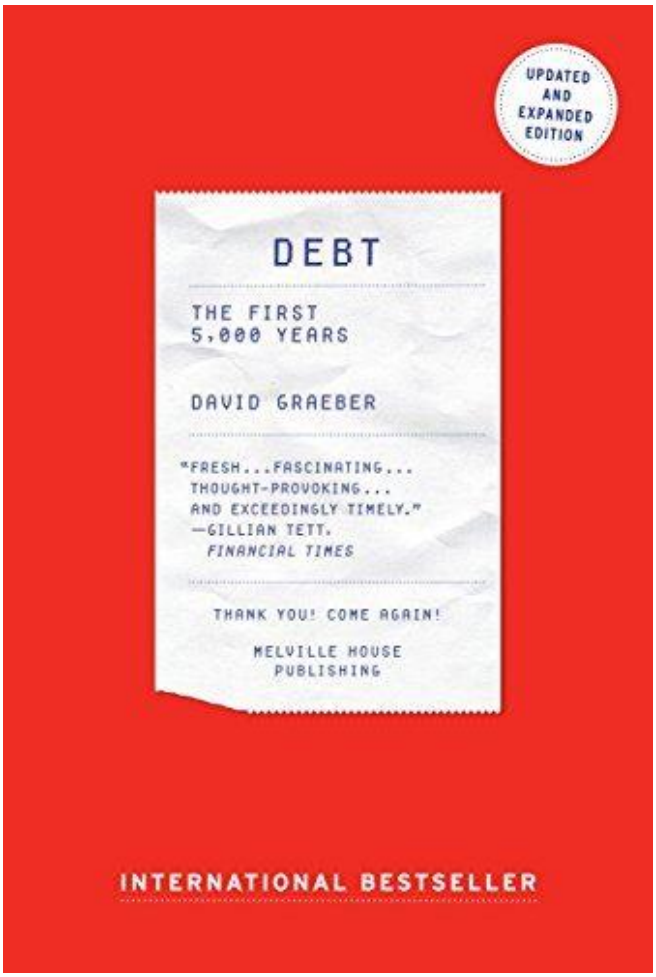
What is a Bitcoin? Everything You Need to Know About Bitcoin

According to dbpedia.org:

> *Bitcoin is a decentralized digital currency based on an open-source, peer-to-peer internet protocol. It was introduced by a pseudonymous developer named Satoshi Nakamoto in 2009. Bitcoins can be exchanged through a computer or smartphone locally or internationally without an intermediate financial institution. In trade, one bitcoin is subdivided into 100 million smaller units called satoshis, defined by eight decimal points.*

No doubt Bitcoin has been the thing of 2017. Many call it the second most important technological advancement of the last century after the internet. Many others instead, label it as the next Tulip Bubble, ready to bust anytime soon.

Whether or not Bitcoin will take over the financial world we don't know. However, Bitcoin made one thing clear; there is an alternative to the traditional financial system we've been used to. Besides, Bitcoin raises another critical point. What the heck is money? For centuries we've believed that money is something that has a real value. In short, based on the old assumption, money, like gold is worth something besides the value we attribute to them. However, this assumption might turn out to be wrong. In other words, money might be just an accounting method. That is the fascinating thesis of the book, Debt: The First 5,000 Years, which I suggest you read if you want to understand what Bitcoin stands for deeply:



In this post, I will show you a few questions a few people dared to ask about Bitcoin, which also explains why that story is so incredible.

Contents [hide]

- The fragility of centralization
- How does the blockchain transaction process work?
- Majority rules
- Privacy is in the master key
- Honest nodes win (in the long-run)
- Related sidebar

Who is Satoshi Nakamoto?

Back in 2008 when Satoshi Nakamoto sent the first email to Hal Finney, his identity was private. He was trying to explain how to get Bitcoin up and running. That is the first email ever between Satoshi Nakatomo and Bitcoin first user, Hal Finney:

> Normally I would keep the symbols in, but they increased the size of the EXE from 6.5MB to 50MB so I just couldn't justify not stripping them. I guess I made the wrong decision, at least for this early version. I'm kind of surprised there was a crash, I've tested heavily and haven't had an outright exception for a while. Come to think of it, there isn't even an exception print at the end of debug.log. I've been testing on XP SP2, maybe SP3 is something.
>
> I've attached bitcoin.exe with symbols. (gcc symbols for gdb, if you're using MSVC I can send you an MSVC build with symbols)
>
> Thanks for your help!

The communication among the people part of the Bitcoin community was private, and many of them didn't meet in person for a few years. Yet none ever met Satoshi Nakamoto. In fact, on April 23rd, 2011, he left anyone baffled with this short and concise message:

> I've moved on to other things. It's in good hands with Gavin and everyone.

None heard from him anymore. Until…

On January 2018, thesun.co.uk spread the news that Satoshi Nakamoto is the real name of a Japanese man living in Temple City, California. Of course, that is speculation, and none knows whether he is the same person or it was just a pseudonym used by Bitcoin's creator.

Did you know Satoshi Nakamoto was nominated for the Nobel Price in economics in 2015?

That's right; Satoshi Nakamoto might be the first fictional character to go close to win the **Nobel Memorial Prize in Economic Sciences.**

The Prize was proposed by Bhagwan Chowdhry as explained in this tweet:

Bitcoin is decentralized, what does it all mean?

That means that none controls, neither guarantees for the system. In a traditional financial order, a central authority, like a bank or a government are necessary to make the system work. Instead, with the Bitcoin, the central authority isn't needed, because the whole system relies on a technology called Blockchain.

In short, that is a distributed ledger made of millions of computers, each of which plays a role in ensuring that the ledger's transactions are approved in block (that is why Block-chain). In fact, for each block of operations, a lottery gets to run among a set of machines that have to solve for math problems to approve those transactions. Once the computers in the chain approve the transactions, the block gets recorded in the Blockchain forever. To pass a block of transactions the majority principles applies. If 50% + 1 of computers approve a transaction, while the remaining do not, the majority wins.

What is the Blockchain foundation? That is a function, called SHA256.

What is SHA256?

SHA256 is a particular type of algorithm, a Cryptographic Hash Algorithm. In short, you input value and the algorithm spits out a 256-bit code, which can't be reversed. Therefore, you cannot get the initial input. In this way, none knows who this code belongs to. That is how privacy is insured.

For instance, let's say I input into SHA256 "Gennaro" and I get back the following code:

5b77b0b0984e51447faac5ab0dd46491501d73a8e985d12f2a7159ef3bddd854

Thi code cannot be decrypted back to find out my name. In short, it works only in one-way!

Is Bitcoin really redistributing wealth?

As anything that starts with a visionary attempt to change the world might become just another way to create a cluster of wealth, that might be true for Bitcoin as well. It is true that a few new millionaires came up from Bitcoin. However, of the current, almost two hundred billion dollars market cap of Bitcoin, 40% of that wealth is in the hands of 1000 people.

As reported on Bloomberg:

About 40 percent of bitcoin is held by perhaps 1,000 users; at current prices, each may want to sell about half of his or her holdings, says Aaron Brown, former managing director and head of financial markets research at AQR Capital Management. (Brown is a contributor to the Bloomberg Prophets online column.) What's more, the whales can coordinate their moves or preview them to a select few. Many of the large owners have known one another for years and stuck by bitcoin through the early days when it was derided, and they can potentially band together to tank or prop up the market.

Therefore, rather than creating distributed wealth for millions of people, the Bitcoin so far has created a new financial elite.

What is the Market Cap of Bitcoin?

As of today (January 20th, 2018), the Market Cap for Bitcoin is two hundred billion dollars. The price of Bitcoin is quite volatile. Just in the last few months, it swung back and forth. That is why the Market Cap can change quite fast as well.

How much can a Bitcoin be Worth?

Wences Casares, CEO of *bitcoin* wallet Xapo and member of PayPal's board of directors, was one of the first Silicon Valley investors to believe in the potential of Bitcoin. As reported by the book Digital Gold, Bitcoin could be worth as much as a half million dollars. This computation was based on a simple assumption. Given all the value of gold in the world at around 7 trillion dollars. Like gold needed to be mined, so Bitcoin does. In fact, to create new Bitcoins, computers dedicated to mining, must solve for complex math calculations. The more the mining gets closer to the limit of Bitcoin that can be mined (set at 21 million), the more it gets hard to mine new Bitcoins.

What is going to happen next? In theory, the limit should be kept to guarantee Bitcoin value stays stable. In practice, that limit might be changed as well. Like money back in the 60s was supposed to be tied to the reserve of gold. On August 15, 1971, President Nixon announced the end of the so-called Gold Standard. The US currency, the dollar, was finally free to be printed, without the need to have a correspondent reserve of gold. The Federal Reserve together with the US government became the guarantors of the system.

Could the same happen to Bitcoin?

Who controls the mining of Bitcoins?

Mining requires complex math calculations that can only be handled by machines. The more the mining gets closer to the limit of 21 million Bitcoins available on the market the more it gets hard for those devices to mine new Bitcoins. What that means is that those machines now need to be more and more efficient in solving calculations. It also means that they need way more electricity to be run properly.

Not that surprisingly China controls the mining of Bitcoins. In fact, as reported by Quartz, one of the largest Bitcoin mining facilities is in Mongolia. The electricity bill can be as high as $39,000 on a given day. And those facilities compete for a piece of the pie that according to Quartz is about 7 million dollar on any given day!

How long it takes before a new block of Bitcoins is solved?

There is a time limit for each block of coins to be solved, that is ten minutes. Why?

As reported on a bitcoin.stackexchange.com discussion:

> *Ten minutes was specifically chosen by Satoshi as a tradeoff between first confirmation time and the amount of work wasted due to chain splits. After a block is mined, it takes time for other miners to find out about it, and until then they are actually competing against the new block instead of adding to it. If someone mines another new block based on the old block chain, the network can only accept one of the two, and all the work that went into the other block gets wasted. For example, if it takes miners 1 minute on average to learn about new blocks, and new blocks come every 10 minutes, then the overall network is wasting about 10% of its work. Lengthening the time between blocks reduces this waste.*
>
> *As a thought experiment, what if the Bitcoin network grew to include Mars? From the farthest points in their orbits, it takes about 20 minutes for a signal to travel from Earth to Mars. With only 10 minutes between new blocks, miners on Mars would always be 2 blocks behind the miners on Earth. It would be almost impossible for them to contribute to the block chain. If we wanted collaborate with those kinds of delays, we would need at least a few hours between new blocks.*

In short, to make the Blockchain efficient, ten minutes seemed to be the right timing to allow all the machines in a blockchain align without wasting too much work.

Can you live On Bitcoin for a week?

Is the blockchain allowing the emergence of innovative business models?

The Blockchain is not a unique protocol. There are many out there. What protocol will turn out to be the most successful we don't know yet. However, by looking at the current landscape it is clear that the blockchain is allowing new business models to spring up. Think of the Steem Blockchain and the apps that have born with it!

To understand the Bitcoin and the Blockchain you need to understand the key principles from its White Paper.

A glance at Bitcoin key principles

Bitcoin has been built upon a technology called Blockchain. This technology allows decentralizing transactions or interactions among parties without the need of a middleman and without necessarily relying on trust but math and probability. Since then, new blockchains protocols are in use and have been proved effective so far to offer alternative business models. For instance, the Steem Blockchain allows online publishers to monetize their content. In this article, I want to show you a few key takeaways from Bitcoin White Paper by Satoshi Nakamoto.

Cut off the middleman

> *A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.*

One critical aspect of the blockchain thought by Satoshi Nakamoto is cutting off the middleman.

The proof-of-work as a central concept

> *The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.*

What makes the whole blockchain system thick is the proof-of-work. In fact, to deter service abuse, the protocol requires a computer to performing computational work.

Business with less data

> *Merchants must be wary of their customers, hassling them for more information than they would otherwise need.*
>
> *A certain percentage of fraud is accepted as unavoidable.*

Today businesses like Facebook and Google have built a fortune thanks to the data of their users. However, this business model is asymmetric and lacks transparency. Instead, with the blockchain, a transaction can occur with a few information.

Trust the cryptographer

system based on cryptographic proof instead of trust,

Another compelling aspect of the blockchain is the fact that it relies on math and probability rather than human trust. This is true to a certain extent. In fact, as the network grows the more effective, it should become.

The collective is good

The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Another assumption of the blockchain which is connected to the previous one is that for it to work, honest nodes have to control more CPU power compared to attacker nodes. We will see why this is the case – from the probabilistic standpoint – when the blockchain reaches a critical mass.

The fragility of centralization

The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

Centralization works but it's quite fragile, and it creates a bunch of side effects. For instance, if we think about governments and banks substantial transactions fees, frauds and corruptions are some of those. Also, an asymmetric system, where one authority has power over a large number of people by controlling their data.

The blockchain avoids just that. Of course, as the blockchain is based on a private key that if stolen or lost cannot be either replaced nor generated again third parties that secure private keys have become the norm. This makes Bitcoin less decentralized as it seems.

How does the blockchain transaction process work?

1) New transactions are broadcast to all nodes.

2) Each node collects new transactions into a block.

3) Each node works on finding a difficult proof-of-work for its block.

4) When a node finds a proof-of-work, it broadcasts the block to all nodes.

5) Nodes accept the block only if all transactions in it are valid and not already spent.

6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Majority rules

Nodes always consider the longest chain to be the correct one and will keep working on extending it

The blockchain process for approving transactions is based on the fact that the longest chain is assumed to be the correct one. So if a shorter chain finishes first, the longest chain will still win over the shortest.

Privacy is in the master key

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous.

As the private key is anonymous, so the privacy of the person that holds is kept so. This is a central principle of the blockchain.

Honest nodes win (in the long-run)

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes

will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

and it continues:

Given our assumption that p > q, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

There is a probabilistic reason why honest nodes win against attackers and that is what makes the blockchain thick.