

## DAILY

# Six myths about blockchain and Bitcoin: Debunking the effectiveness of the technology

August 18, 2017

Blockchain: so cool, what a breakthrough — soon almost everything will be based on blockchain technology. If you bought all of that, then I might just disappoint you.

This article will discuss the version of blockchain technology that is used for Bitcoin cryptocurrency. There are other implementations, and they may have eliminated *some* of the disadvantages of the “classic blockchain,” but usually everything is built around the same principles.



## About Bitcoin in general

I consider the Bitcoin technology itself revolutionary. Unfortunately, Bitcoin has been used for criminal activities far too often, and as an information security specialist, I

Alexey Malanov

[12 posts](#)

Malware Expert, Anti-



TECHNOLOGY

BITCOIN

BLOCKCHAIN

BTC

PRIVACY

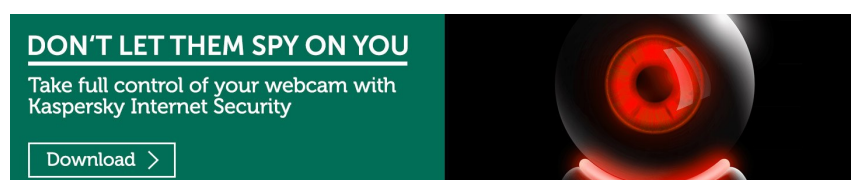
TECHNOLOGY

Share



strongly dislike that practice. Yet, technologically speaking, Bitcoin is an obvious breakthrough.

The Bitcoin protocol components and built-in ideas aren't new; generally, they were all known before 2009, but only the authors of Bitcoin managed to piece them together to make it work back in 2009. Since then, for almost nine years, only one critical vulnerability has been found in its implementation, when one malefactor snagged 92 billion bitcoins. Fixing that required rolling back the entire financial record by 24 hours. Nevertheless, just one vulnerability in nine years is praiseworthy. Hats off to the creators.



The authors of Bitcoin faced the challenge of making it all work with no central system and no one trusting anyone else. The creators rose to the challenge and made electronic money an operational currency. Nevertheless, some of their decisions were devastating in their ineffectiveness.

I am not here to discredit blockchain, a useful technology that has shown many remarkable uses. Despite its disadvantages, it has unique advantages as well. However, in the pursuit of the sensational and revolutionary, many people concentrate on the upsides of the technology, often forgetting to take a sober view of things, thus disregarding all of its downsides. It is for this reason, for the sake of diversity, that I deem it useful to focus on the disadvantages of the technology.





*A book that expresses high hopes for the blockchain. Quotes from this book appear throughout this article*

## Myth #1: The blockchain is a giant, distributed computer

“

*Quote #1: “The blockchain could be an Occam’s razor, the most efficient, direct, and natural means of coordinating all human and machine activity; it is a natural efficiency process.”*

”

If you haven’t looked into the [principles of blockchain operation](#) and you’ve only heard opinions about this technology, then you might be under the impression that blockchain is some sort of distributed computer, performing distributed computations. You might have supposed that nodes across the world gather something bigger bit by bit.

“

*[Blockchain, simplified](#)*

”

That is totally incorrect. In fact, all of the nodes that maintain the blockchain do *exactly the same thing*. Here is what millions of computers do:

1. They verify the same transactions in accordance with the same rules and perform identical operations.
2. They record the same thing into a blockchain (if they were fortunate enough to be allowed to do so).
3. They store the entire history, which is the same for all of them, for all time.

There is no paralleling, no synergy, and no mutual assistance. There is only instant, millionfold duplication. It's the opposite of efficient — and that's important, as we'll see later on.

## Myth #2: The blockchain is everlasting. Everything that is recorded into a blockchain will remain there forever

“

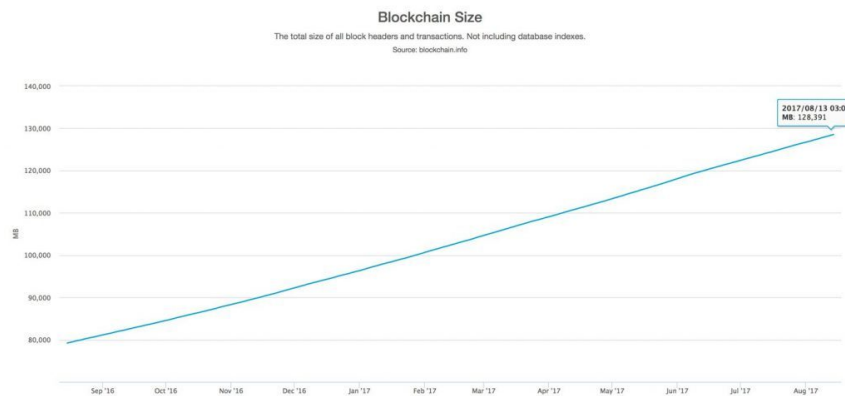
*Quote #2: “With Dapps, DAOs, DACs, and DASs, there could be many interesting new kinds of emergent and complex AI-like behavior.”*

”

So: Every high-grade Bitcoin network client stores the entire transaction history, and this record has already



become as large as 100GB. That's the full capacity of a cheap laptop's or the most advanced smartphone's storage. The more transactions processed on the Bitcoin network, the faster the size grows. And the greatest bulk of it has appeared over the past couple of years.



*The growth of the blockchain.* [Source](#)

Bitcoin's blockchain growth isn't even the fastest — the competitor Ethereum network has accumulated 200GB of history data in the blockchain, within just two years of launch and six months of active use. Hence, the blockchain's life span is limited by a decade under current circumstances. The growth of HDD capacity definitely lags behind.

In addition to the need to store a large chunk of data, the data has to be downloaded as well. Anyone who has ever tried to use a locally stored wallet for cryptocurrency discovered with amazement and dismay that he or she could not make or receive payments until the entire download and verification process was complete — a few days if you were lucky.

You may ask: If it's all the same thing, perhaps we shouldn't store it on every network node? Sure, it would be more efficient. But, first of all, then it wouldn't be a peer-to-peer blockchain but rather a traditional client-server architecture. Second, clients would then have to trust servers. Remember, "not trusting anyone" is one of the foundations of blockchain.



For a long time, Bitcoin users have been divided into enthusiasts, who “suffer,” downloading everything and storing the whole blockchain on their own computer, and common people, who use online wallets, trust the server, and do not care how it all works.

## Myth #3: The blockchain is effective and scalable. Conventional money will soon disappear

“

*Quote #3: “The concept is ‘blockchain technology + in vivo personal connectome’ to encode and make useful in a standardized compressed data format all of a person’s thinking. The data could be captured via intracortical recordings, consumer EEGs, brain/computer interfaces, cognitive nanorobots, and other methodologies. Thus, thinking could be instantiated in a blockchain — and really all of an individual’s subjective experience could eventually be as well, including (possibly) consciousness, especially if it’s more precisely defined. After they’re on the blockchain, the various components could be administered and transacted. For example, this could be done in the case of post-stroke memory restoration.”*

”

If each network node does the same thing, then obviously, the bandwidth of the entire network is the same as the bandwidth of one network node. But do you know exactly



what that is? The Bitcoin network is capable of processing a maximum of seven transactions per second — for the millions of users worldwide.

Aside from that, Bitcoin-blockchain transactions are recorded only once every 10 minutes. To increase payments security, it is standard practice to wait 50 minutes more after each new record appears because the records regularly roll back. Now imagine trying to buy a snack using bitcoins. It's no big deal to stand in line for an hour at the store, right?

If you consider the entire world, that sounds ludicrous even now, when Bitcoin is used by just one in every thousand people on the planet. And given the transaction-processing speed, significantly increasing the number of active users simply isn't possible. For comparison, Visa processes thousands of transactions per second and, if required, can easily increase its bandwidth. After all, classic banking technologies are scalable.

If conventional money disappears, it won't be because of blockchain solutions.

## Myth #4: Miners provide network security

“

”

*Quote #4: "Cloud-based, blockchain-based autonomous business entities running via smart contract could then electronically contract with compliance entities like governments to self-register in any jurisdictions in which they wanted to operate."*



You have certainly heard of miners and giant mining farms built next to power stations. What do they actually do? They burn a lot of electricity for no purpose at all for 10 minutes, “shaking” blocks until they become “beautiful” and thus eligible to be added to a blockchain (you can learn about all of that [in this post](#)). Essentially, it’s done for one purpose: to make sure that rewriting transaction history would require the same amount of time it took to write the original history (given the same overall computing power).

The electricity consumed to achieve that is the same as the amount a city with a population of 100,000 people would use. And don’t forget the expensive custom mining equipment, which is almost useless for any purpose other than mining bitcoins.

“

*[Explainer: Bitcoin mining](#)*

”

Blockchain optimists like to say that miners don’t just perform useless operations but maintain the stability and security of the Bitcoin network. This is true, but the problem is that miners are protecting Bitcoin *from other miners*.

If only one-thousandth of the current number of miners existed, and thus one-thousandth of the electric power was consumed, then Bitcoin would be just as good as it is now. It would still produce one block per 10 minutes, process the same number of transactions, and operate at exactly the same speed.

The risk of a [51% attack](#) applies to blockchain solutions as well. If someone controls more than half of the computing power currently being used for mining, then that person can surreptitiously write an alternative financial history. That version then becomes reality. Thus, it becomes





possible to spend the same money more than once. Traditional payment systems are immune to such an attack.

As it turns out, Bitcoin has become a prisoner of its own ideology. "Excessive" miners cannot stop mining; that would dramatically increase the probability of a single person controlling more than half of the remaining computing power. Mining is still lucrative, and the network is still stable. However, if the situation changes (if, for example, the price of electricity increases), the network may come across a huge number of "double spending" incidents.

## Myth #5: The blockchain is decentralized, therefore it is indestructible

“

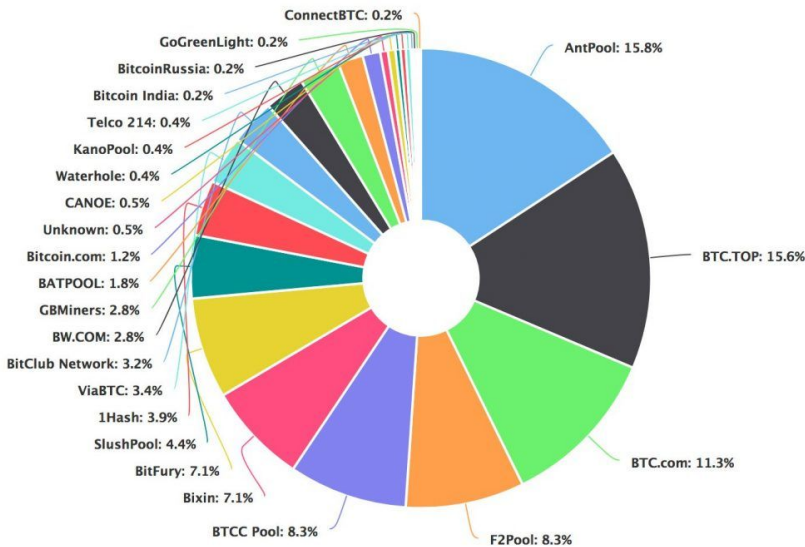
*Quote #5: "To become an organization more formally, a Dapp might adopt more complicated functionality such as a constitution..."*

”

It may seem that if a blockchain is stored on each network node, then special services or authorities can't shut down Bitcoin on a whim, inasmuch as there is no centralized server or something similar — they have no one to go to if they want to shut it all down. That is just an illusion, however.

Actually, all "independent" miners are merged into pools (technically, they're cartels). They have to merge on the assumption that it's better to have a small but stable income than a huge payoff maybe every thousand years (and even that isn't guaranteed if you on your own).

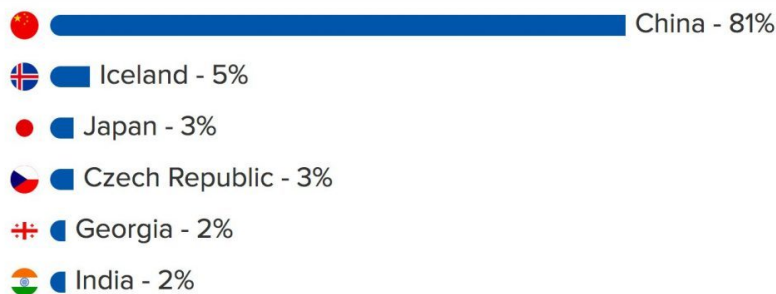




An estimate of computing power distribution among the largest mining pools. [Source](#)

The pie chart above shows approximately 20 of the largest mining pools, but the top 4 control more than 50% of all computing power. Gaining access to just four controlling computers would gain someone the ability to double spend bitcoins. This, as you can imagine, would depreciate bitcoins somewhat, and doing it is actually quite feasible.

But the threat is even more serious than the above might imply, because the majority of pools, along with their computing powers, are located inside one country, which makes it much easier to capture them and gain control over Bitcoin.



Distribution of mining by country. [Source](#)

## Myth #6: The anonymous and open character of the blockchain is a good thing

“

”

*Quote #6: “Traditional government 1.0 is becoming outdated as a governance model in the blockchain era, especially as we begin to see the possibility to move from paternalistic, one-size-fits-all structures to a more granular personalized form of government.”*

Blockchain is open, and everyone sees everything. Thus, blockchain has no real anonymity. It offers *pseudonymity* instead. Putting aside the significant issues that crooked users have with that, here’s why pseudonymity is bad for honest users. A simple example: I am transferring a few bitcoins to my mother. Here’s what she can learn:

1. How much money I have at any given time.
2. How much I spent and, more important, what I spent it on. She could also find out what I bought, what I gambled on, and what politician I supported “anonymously.”

Alternatively, if I paid back my friend for some lemonade, I would thus let him know everything about my finances. That’s hardly a trifling matter: Would you reveal the financial history of your credit card to everyone you knew? Keep in mind that this would include not only past but also future transactions.

Some disclosure may be tolerable for individuals, but it is deadly for companies. All of their contracting parties,



sales, customers, account amounts, and every other little, petty detail would all become public. Financial transparency is perhaps one of the largest disadvantages of using Bitcoin.

## Conclusion

“

*Quote #7: “The connected world could usefully include blockchain technology as the economic overlay to what is increasingly becoming a seamlessly connected world of multidevice computing that includes wearable computing, Internet-of-Things (IoT) sensors...”*

”

I have listed six major disadvantages of Bitcoin and the blockchain version it uses. You may ask: “Why did I have to learn it from you and not earlier from someone else? Is it possible that no one sees the problems?”

Some people may be blinded, some may simply not understand [how the technology works](#), and others may see and realize everything but feel the system is working for them. It’s worth considering that many of those who have purchased bitcoins begin advertising and advocating them — as in a pyramid scheme. Why disclose that the technologies have disadvantages if you’re counting on the growth of the exchange rate?

Yes, Bitcoin has competitors that tried to solve some of these problems. Although some of those ideas are quite good, they are still based on the blockchain. And yes, there are other, nonmonetary applications for blockchain technology, but the main disadvantages are found in them as well.



So, if someone tells you that the invention of the blockchain can be compared with the invention of the Internet in terms of importance, be skeptical.


<

Taxi Trojans are on the way

Not-a-Virus: What is it?


>

## Read Next




TECHNOLOGY

Problems and risks of cryptocurrencies




THREATS

CryptoShuffler: Trojan stole \$140,000 in Bitcoin



TECHNOLOGY

Why blockchain is not such a bad technology



TECHNOLOGY

Explainer: Bitcoin mining

### Products to Protect You

Our innovative products help to give you the Power to Protect what matters most to you. Discover more about our award-winning security.

### FREE Tools

Our FREE security tools and more can help you check all is as it should be... on your PC, Mac or mobile device.



## About Us

Discover more about who we are... how we work... and why we're so committed to making the online & mobile world safer for everyone.

## Get Your Free Trial

Try Before You Buy. In just a few clicks, you can get a FREE trial of one of our products – so you can put our technologies through their paces.

## Contact Our Team

Helping you stay safe is what we're about – if you need to contact us, get answers to some FAQs or access our technical support team.

## Connect With Us



## Blog List

Securelist

Threatpost

Eugene Personal Blog

---

Copyright © 2017 AO Kaspersky Lab. All Rights Reserved. • [Privacy Policy](#) • [License Agreement](#)

 Global

