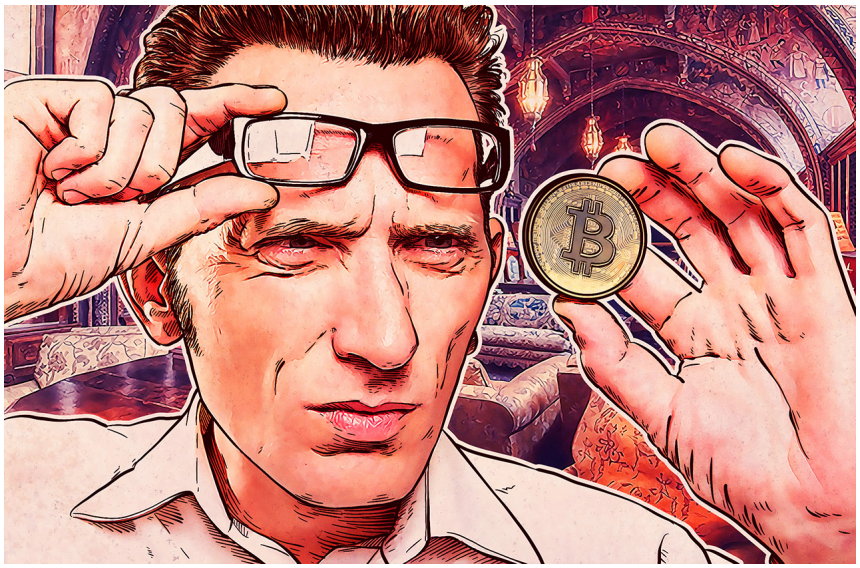
DAILY

Blockchain, simplified

September 8, 2016

Bitcoin, and its fundamental technology **blockchain**, have been popping up in the news plenty over the past few years. However, discussion about them is typically a bit high level — or, OK, gibberish — leaving the average person with the vague impression that something cool is happening with currency, but very little in the way of actual knowledge or understanding.



The technology is indeed elegant, but it is not that difficult to understand. We'll take a shot at explaining in a straightforward way how blockchain works, avoiding geeky jargon as much as possible.

Just two tech concepts...

How digital signatures work

Anyone can generate a *digital name* and *digital signature*. Those aren't like your typed name and handwritten

signature; they are a public key and a private key, respectively. Having these digital assets enables the following scenario:

1. A person can write messages, sign them digitally, and publish online.
2. The world can see that the message is genuine — people can identify the person's digital name thanks to the digital signature.
3. No one can forge a signed message.
4. A person may generate numerous name-and-signature pairs (think of them as stage names) for various purposes.

> *What is All this Business about #Bitcoin? http://t.co/scbRcfPmoX #onlinethreats*
>
> *— Kaspersky Lab (@kaspersky) November 8, 2013*

How hashing works

Let's say I write a message ("Hello") and want to send it to my friend. But I need to make sure it reaches the intended recipient unaltered. How would I do that? The easiest way would be to ask my friend to send the whole message back to me so I can compare the two messages and see if they match. Many people use the same approach when dictating some numbers or spelling e-mail addresses over the phone.

However, the message might reach my friend perfectly but

"break" on its way back, and in that case we would not be able to ensure its integrity. Moreover, the message might be very long. What if the message contains a high-def video? It makes no sense to send back all those gigabytes of data just to verify they were received properly, and that's why another approach is used to ensure message fidelity. It's called *hashing*.

Let's create a numeric representation of "Hello." Here's one way to do that:

Let each letter be associated with a sequential number (i.e., a=1, b=2, z=26), so Hello would read 8 5 12 12 15.

Multiply the numbers to get 86400. That's how we get the simplest hash.

After I have sent a primary message to my friend, I send the hash so that they can check whether the received message matches the intended one.

Now, what if the message was altered on its way, and now it reads "Hallo"? Well, that would change its hash: 8*1*12*12*15=17280. My friend would expect to get 86400, so when they get 17280, the difference would alert us both that something went wrong.

We should note here that the hash itself could be altered or otherwise compromised. It does not serve to protect the integrity of the message (a signature does that); it is used to simplify and speed up the process of integrity checking. Also, in actual use, people do not encode their hashes and send them to their friends as separate messages; their computers handle the entire process in a way that is invisible to the users.

That simple hash method would not catch swapped letters in the message — it was just an example. In the real world, we use much more complex algorithms.

Creating a message with a "cryptographically strong"

matching hash becomes an extremely long process. Take, for example, the popular SHA-1 algorithm (which is not as strong as it was designed to be, but that's another story). A hash for "Hello" would look like this:

f7ff9e8b7bb2e09b70935a5d785e0cc5d9d0abf0

For "Hallo," the hash would look like this:

59d9a6df06b9f610f7db8e036896ed03662d168f

Not much in common, is there? Well, that's how it was meant to be — it's a code.

Enabling virtual money

OK, that's the hard part done. So, what cool things can we do with these technologies?

Imagine there are 30 kids in a classroom, and they would like to use their own play money, which should be entirely virtual (i.e., mere numbers written on paper or stored on the Internet).

To do this, the kids write the values of their initial cash possessions on the chalkboard, and then write down how much money each of them gave to another person. They write down each "transaction" in their genuine handwriting and sign it with a signature, so no one can mess with transactions while everyone is out during the break. This approach works perfectly until a teacher comes and wipes it all off the board, claiming control over the cash flows because he or she has power and, say, wants to prevent children from using the system for buying drugs from each other.

> *#Bitcoin Safety Guide by @Kaspersky Lab*
> *http://t.co/RjwzqAwPXR*

— Kaspersky Lab (@kaspersky) November 23, 2013

As a result of these unfavorable conditions, kids turn to keeping their financial records in notepads. Each of them keeps a notepad under their desk and constantly updates the record with transactions. Of course, they cannot shout about their purchases during class, so they use paper notes (aka the Internet). So, at first sight, this is cryptocurrency in action!

Problems

Bundling transactions into pages

Now there are 30 notes circulating in the classroom; how would one know that each of students copied the contents of all of the paper notes into their notepad? Which paper notes were copied by all of the students and can be disposed of? How would one know if Billy has 50 coins to pay to Johnny and has not paid them to someone else without Johnny's knowledge?

There is a solution to those problems: Children need to exchange not only short notes containing lines of transactions, but entire pages. When someone has accumulated a lot of transactions, they copy accurately all of the lines, calculate the hash for the previous page, copy it on the top of the new page and distribute the new page to all of the students in the class.

On receiving the page, Johnny checks it for consistency: All lines should be written in the same handwriting, the page should contain a new number, and the hash for the previous page should match the hash written on the new page. And one more thing: Each contributor should have

as much money as they want to pay. To ensure that, Johnny needs to read through the entire transaction journal and count the money. Sounds quite cumbersome, yet a computer will manage the task with ease.

So, if the numbers add up right, Johnny then accurately writes down a new page in his journal and accepts the transactions. Separate lines/transactions that are now included in the page needn't be passed around the class; they can be disposed of, and the new page passed around instead.

If something is wrong (someone does not have enough money for a transaction, or the page number seems odd, or hashes don't match), Johnny says, "That's fishy," get rids of the entire page, and then goes back to business as usual.

A collection of numbered pages (blocks) is, in essence, *blockchain*. It's very simple, and no magic is involved.

Graphomania

If this process is not controlled by any additional rules, each student would start their own version of page #123. As a result, there would be 30 versions of the transaction journal circulating in the class. How would one know which one is correct? A certain routine makes that possible: The page is created once every 10 minutes, so it can be distributed to the entire class, and the writer responsible for keeping the journal is chosen randomly.

With Bitcoin, they decided to deal with that in the following way. Students have to do some useful task — like solving randomly picked math problems from the textbook. Whoever is the first to solve the problem collects all of the notes and starts to create a new page. While others continue solving the problem, that star student's page is distributed among the class, is accepted by

everyone, and then the class would start solving another math problem.

It's not an issue if the pages are written down by a sole A student; it's much more important it's someone with high speed of execution. And if there are many A students in a class, problems are solved faster, and the group can upgrade to the next chapter of the textbook.

However, if only Karl, a straight A student, is always entrusted with the task of compiling pages, he might be in power to deny Johnny any chances to pass virtual money to anyone. Anyone willing to do so should be a real badass student — she or he should possess computing capacity exceeding half of aggregated computing capacity of all Bitcoin users (which is yielded by millions of computers all over the world). So, should Karl be capable of that (meaning he invested that much in computing capacity), petty cheating would not make any sense.

There is another peculiarity. An A student also writes down the solution to the math problem on the page (mind you, this math problem is not really random but relevant to the page itself). It's essential to prevent one from forging all pages from 123 to the current one even in a year's time. A cheater otherwise would have to solve a *huge* number of problems.

Benefit

With the aforementioned approach, our journal is evenly incremented by new, correctly filled pages.

1. This process does not depend on the number of participants.
2. This process is decentralized. It cannot be shut down or forged — any contributor to the system

can check the integrity of all the pages any time they want.

3. This process is anonymous, provided a digital name cannot be traced to the real one. Any Johnny can prove the wallet pertaining to a particular digital last name belongs to him — if he has a corresponding digital signature, he can use the wallet. But it would be extremely challenging to prove that the wallet belongs to Johnny in real life if Johnny himself doesn't want it to be proved.

4. No fee is charged. However, you can pay an A student to ensure your transaction is copied to the page in fast-track mode.

5. Once done, a transaction cannot be reversed — meaning no one can cross out the line stating Billy has passed money to Johnny (as each page relates to the previous one). Once one page is altered (even with consent from other participants), the rest of the pages must be altered too, which means many, very many math problems should be solved. When in doubt, participants would trust the longest chain of pages.

> *Why are tech giants betting on #BitCoin? – http://t.co/xcGx5EOPFC pic.twitter.com/MImFiCndcD*
>
> *— Kaspersky Lab (@kaspersky) April 6, 2015*

If I bribe more than a half of the class (preferably, A students), I can spin the students off into a separate classroom and start an alternative history in which I never passed my money to anyone. After that, I can return to the former class and present them a longer journal of transactions. This trick is the essence of the so-called 51 per cent attack (though we have already discussed why it would be very challenging in real life, as we showed in the example of Karl, the straight A "badass").

Where the money comes from

Initially, all bitcoins could have been distributed among lucky ones who compiled the very first page. But that would have been both unfair and pointless. To get more people involved in the system, the founders agreed to distribute money incrementally: The person who solves a problem and starts a new page would put a line at the top saying: "Credit me with 50 coins out of nowhere."

Also, everyone agrees the page is correct if the amount is exactly 50, and that in a couple of years 50 will become 25, and so on. As a result, people grow their assets, but the total amount of coins is limited: There can be no more than 21 million bitcoins (as of today, about 15 million have been "emitted").

Thanks to this principle, many people wanted to join the project as early birds and earn some money by dint of being the first — later, the money would be distributed in smaller portions and to more participants. Also, more and more people are working really hard to nail those math problems as fast as possible.

So, now a lot of people possess of a lot of cryptocurrency. And now is when we announce that the cryptocurrency is the stock of the new Money Of The Future, Inc., and start trading it on the stock exchange for real money. The cryptocurrency is sold at a market price which starts to

grow: Many want to get their hands on the money of the future. For many people, the most favorable option would be to purchase the cryptocurrency, now that it's given away in lots of 25 just once every 10 minutes, and also getting it that way means you have to solve some math problems … yes, it's easier to purchase than to mine.

Then online merchants realize that the coins can be exchanged for real money at the stock exchange, and they start to accept cryptocurrency — considering it constantly grows in price, that's a wise move.

Some criticism

Now that readers are up to speed with the concept of Bitcoin, I'll get a bit biased about it.

1. Bitcoins *are* a real innovation. A mysterious author (or an even more mysterious group of authors) did quite well right away, at the first shot, and their idea is still working.

2. Bitcoins are pure gold for various illegal deeds. Weapons and drugs trading, bribery, and extortion all become easy to manage because transactions are very hard to trace and impossible to shut down. In the offline world, people would just pay in cash in such cases, but online, traditional payment systems are controlled and not anonymous — hence the value of Bitcoin.

> *Many people think that #Bitcoin and other #cryptocurrency are made for criminals. It's really not the case #klcsw pic.twitter.com/B318zHv69t*
>
> *— Kaspersky Lab (@kaspersky) November 28, 2014*

3. For legal deeds, decentralization and anonymity are useless and even harmful. We have been using Visa/MasterCard, bank transfers, and PayPal/WebMoney for ages. These systems have their flaws but also useful features:

a. We pay fees (especially when sending a payment that crosses borders), but we get a valuable service.

b. The transfers take some time, but they are checked and can be revoked.

Bitcoin is faster and cheaper, but to enjoy its benefits, we have to burn an awful amount of electricity, and duplicate information over and over. If we decided to hand over those tasks to, say, PayPal, it would not be any worse.

4. People like bitcoins because they constantly grow in price. It's like a Ponzi investment producing more and more bubbles. People won't completely lose interest in the scheme, and the more willing buyers there are, the greater the demand. That's why those who already bought their share of coins actively promote "the money of the future" — to stir up interest and thus increase the price. Demand is clearly surpassing supply, which shrinks over time.

5. People dislike bitcoins because they constantly grow in price. Traditional economy is regulated by a central bank, which ensures the volume of available money corresponds to the volume of goods and services, making the latter become a bit cheaper over time. As for bitcoins, this process is distorted: Bitcoins are continually and abruptly growing in price, which means it's unprofitable to spend them on goods; better to spend real currency and leave the bitcoins for later (or, likely, forever).

6. Why regulators don't like Bitcoin.

a. It's a Ponzi scheme. If the people of one country rushed to buy out bitcoins and then the bubble bursts (as it does

every couple of years), it would mark the start of a crisis. That's why Ponzi schemes are out of bounds in most countries.

b. Bitcoin is associated with drugs, tax avoidance, murky incomes, and terrorism — precisely due to the absence of control. Regulators therefore ban cryptocurrencies and urge people to use the traditional tools that are widely available everywhere.

7. As for using blockchain in areas beyond exchange, the majority of projects that involve blockchain manage the same tasks in a centralized manner. They are able to do so by using one or more computing hubs, which come a lot cheaper in terms of computing power and efficiency. In the aforementioned chalkboard example, it's obvious that writing transactions on the board is much easier than doing the same discreetly, in notepads under a desk. But, of course, that's true if there's no overbearing teacher to suddenly erase the chalkboard.

That's it. Now you are more familiar with Bitcoin and blockchain that the majority of the planet. Feels good to be so smart, doesn't it?

‹ The Cost of Cryptomalware

Tip of the week: How to protect your data... ›

Read Next

THREATS

How Kaspersky Lab products protect against miners

NEWS

Transatlantic Cable Podcast – Episode 14

NEWS

Transatlantic Cable podcast, episode 13

SPECIAL PROJECTS

5 things we learned at the Kaspersky Cybersecurity Summit

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 ou technical support team.

Connect With Us

Blog List

Securelist

Threatpost

Eugene Personal Blog

Global