Explainer: Bitcoin mining

July 20, 2017

If you've shopped for a graphics card lately, you probably know about the worldwide shortage — or you may even have seen something about it in the news. Some sources blame miners for buying everything up. But who are these miners?

Miners is the term for people who collect cryptocurrency. Currency miners mine their cryptocurrency at their *farms*, specially tricked-out computers dedicated to the task. You've no doubt heard of the most famous cryptocurrency, Bitcoin, although it's not the only one.

But why is cryptocurrency in the news right now; why the commotion? And if everyone else is mining money, should you do it as well? Let us get to the bottom of what is happening right now.

Alexey Malanov

12 posts

Malware Expert, Anti-

TECHNOLOGY

BITCOIN

BLOCKCHAIN

CRYPTOCURRENCY

EXPLAINER

ONLINE FINANCE

TECHNOLOGIES

Blockchain

First, let us review the basics of bitcoin and blockchain.

You can read about them in detail in one of our posts; my explanation here will be brief.

Bitcoin is a decentralized virtual currency. That means it has no central authority, and nobody trusts anybody; nevertheless, payments are secured. Blockchain helps to make them safe.

Blockchain can be thought of as an Internet diary. The blockchain is a chain of successive blocks holding recorded transactions such as who transferred bitcoins, how many, and to whom. Blockchain may also be referred to as a *ledger* — which is accurate. It also has a couple of features worth noting here.

> *Blockchain, simplified*

The first key feature of the blockchain is that all true participants of the Bitcoin network store the entire chain of blocks with all of the transactions that have *ever* been made, and participants continuously add new blocks to the end of the chain.

The second key aspect is that the blockchain is based on cryptography (hence the "crypto" in "cryptocurrency"). Laws of mathematics, not the reputation of some person or organization, dictate system operation and guarantee that everything works as expected.

Those who add new blocks are called *miners*. As a reward for each new block, its creator receives 12.5 bitcoins nowadays. That's approximately $30,000 according to the exchange rate for July 1, 2017.

Finally, all new bitcoins are minted through the mining process — and that's the only way new bitcoins can be created.

Each new block is created once every 10 minutes. There are two reasons for that.

First, it provides a constant for synchronization. Ten minutes are allocated for distributing a block across the Web. If people could continuously create blocks, then the Internet would be filled with their different versions and it would be hard to sort out which should be added at the end of the blockchain.

Second, the 10 minutes are spent making the new block look "beautiful" — in terms of the math, that is. Only a correct and "beautiful" block will be added to the end of the blockchain diary.

Why blocks should look "pretty"

For a block to be "correct," everything in it must be valid and follow the blockchain's rules. The most important rule is that someone who sends money must possess that amount of money.

A "beautiful" block is one whose digest has many zeroes at the beginning. For more information on what a digest is (or a hash, which is a result of a certain mathematical

transformation of a block), please refer to the article again. However, that is not of fundamental importance right now. To obtain a "beautiful" block, the block has to be "shaken." "Shaking" means that the block is insignificantly changed and then verified to become "beautiful."

Each miner continuously "shakes" candidate blocks with hopes that he or she will be the one who gets lucky and "shakes out" a "beautiful" block, which will be the one included at the end of a blockchain, resulting in that nice $30,000 reward.

If the number of miners increases tenfold, then a block must likewise become tenfold "more beautiful" to be worthy of being added to the blockchain. This method maintains the speed of new block discovery: Regardless of the number of miners, a block will appear only once every 10 minutes. Thus, the odds of getting the reward decreases as the number of miners rises.

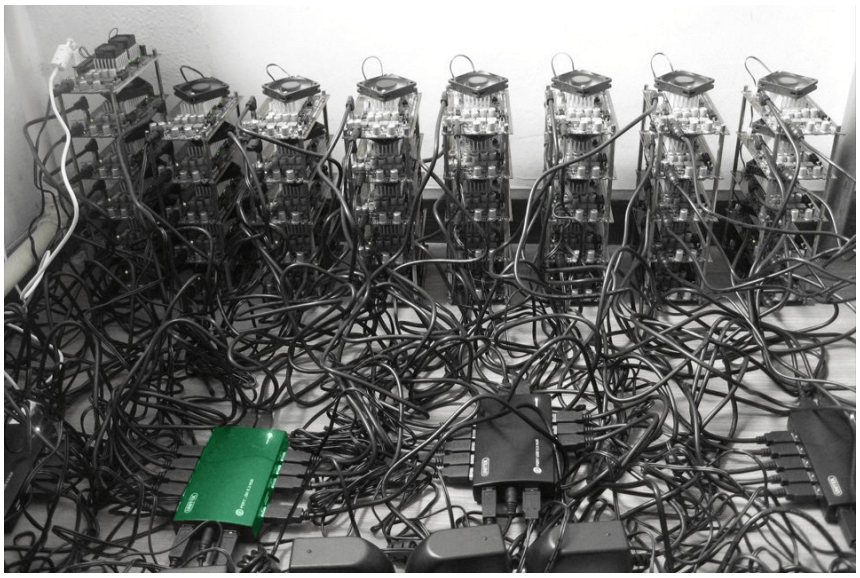
And that is why the blocks need to be "pretty." The requirement prevents someone from rewriting the entire transaction history. Essentially, with each block requiring 10 minutes of combined efforts from all of the miners, there's simply no way for one person to make a forged block "beautiful" and falsify their transaction history working alone.

Miners

In 2009, when only enthusiasts and Bitcoin creators knew about Bitcoin, mining was easy, and one bitcoin was worth about five cents. Let us assume for the sake of example that there were a hundred miners. Therefore, Egbert, an

imaginary miner, could "shake out" one block and get his reward at least once per day.

By 2013, when the exchange rate for bitcoins went north of $100 per bitcoin, so many miner enthusiasts had joined the pack that a stroke of luck could take months to hit. Miners began merging into *pools*, cartels that "shake" the same candidate block together and then share the reward among the participants.



A home farm with a high power output (by 2013 standards).

Then, new hardware appeared: ASIC (application-specific integrated circuit). ASICs are microchips created for a specific task — in this case, to "shake" Bitcoin blocks as effectively as possible.

The mining power of ASICs is substantially higher than that of a general-purpose computer. Huge ASIC-based farms began to appear in China, Iceland, Singapore, and other countries, targeting locations that were cold (such as underground) and, even better, proximal to a hydropower plant for lower electric costs.

Home-based bitcoin mining quickly became pointless, an early casualty of the Bitcoin arms race.

An industrial farm for cryptocurrency mining

Altcoin mining: Why graphics cards have disappeared

Bitcoin is the first and most popular cryptocurrency, but nowadays, we have about 100 alternative cryptocurrencies, also known as altcoins.

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$41,276,360,434	$2514.99	16,412,137 BTC	$1,294,400,000	-5.07%	
2	Ethereum	$25,784,932,572	$277.83	92,806,639 ETH	$1,529,390,000	-13.59%	
3	Ripple	$11,129,123,821	$0.290643	38,291,387,790 XRP *	$191,554,000	-4.68%	
4	Litecoin	$2,068,370,032	$39.99	51,722,957 LTC	$364,736,000	-12.22%	
5	Ethereum Classic	$1,858,471,815	$19.99	92,975,192 ETC	$235,765,000	-11.92%	
6	NEM	$1,458,405,000	$0.162045	8,999,999,999 XEM *	$8,441,160	-12.89%	
7	Dash	$1,223,047,700	$165.60	7,385,732 DASH	$33,916,800	-8.38%	
8	IOTA	$1,119,177,868	$0.402650	2,779,530,283 MIOTA *	$7,554,770	-20.67%	
9	BitShares	$674,430,472	$0.259761	2,596,350,000 BTS *	$73,111,400	-16.71%	
10	Monero	$630,498,135	$42.92	14,688,675 XMR	$14,011,400	-10.18%	

The top 10 cryptocurrencies sorted by market capitalization (the total price of all of the minted coins). Data as of July 1, 2017. Source: coinmarketcap.com

The creators of altcoins do not want mining's cost of entry to become too high or otherwise difficult to meet; thus,

they must devise new criteria for the blocks' required "beauty." The creators want the criteria to hinder the creation of dedicated hardware (ASIC) or delay it for as long as possible. They do what they can to keep the game open to regular people using regular computers to make a tangible contribution to the total network power — and reap the rewards.

In addition, a common graphics card is used for "shaking" altcoins. As it turns out, graphics cards work well for such computations. Hence, the availability of a mining process can increase the popularity of a specific altcoin.

Note Ethereum's spot in the second line of the table above. This relatively new cryptocurrency (launched in 2015) has some unique features, mainly its ability to incorporate into a blockchain not only static information about processed payments but also interactive objects, or smart contacts, that operate in accordance with programmable rules.

We shall discuss in another post why all of this has generated considerable public excitement. For now, we will just state that the new Ethereum properties have sparked big interest from crypto investors and caused rapid growth: Ether started 2017 at $8 and hit $200 by June 1.

Mining Ethereum, in particular, became exceptionally profitable, and that is why miners bought up graphics cards.

A Gigabyte graphics card specifically designed for mining: it lacks irrelevant things like display outputs. Source

If miners stopped mining

What if mining stops paying off — say, if the income does not cover equipment and electricity costs and miners stop mining or start mining another currency. What then? Is it true that if miners stop mining, then Bitcoin will stop working or will become too slow?

No, it is not. As we have already explained, a blockchain constantly adapts its criteria for block "beauty" to maintain its rate of creation. If there are 90% fewer miners, then there will be 90% less calculations required for a new block to be approved. The blockchain itself will stay fully functional.

The absolute value of reward for new blocks decreases over time. This change is programmed into the Bitcoin rules as well. During the first four years (2009–2012), the reward was 50 bitcoins. Currently, the reward is 12.5 bitcoins.

However, the growing exchange rate has more than compensated for the decreased absolute value of reward: 50 BTC were worth only $500 in the middle of 2012, whereas the current reward, 12.5 BTC, is worth $30,000. Besides, someday the miners' revenue will also come from transaction fees.

Conclusions

We have reviewed what mining really is, its purposes, for whom and when mining is advantageous, where the graphics cards have gone, and why some manufacturers release their graphics cards without any display outputs.

Yet, the most intriguing thing, which is how the new Ethereum currency has gained so much popularity, remains behind the scenes. So keep an eye out — we will tell you all about it.

Kaspersky Lab turns 20: Key events and milestones

Then and now. 20 years in-between — all uphill

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

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

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

Global