

## WHAT BITCOIN IS AND HOW TO MINE IT

Vinnitsia National Technical University;

### Анотація

*В даній статті розглянуто поняття криптовалюти, а саме біткоіну, а також досліджена процедура добування даної криптовалюти.*

**Ключові слова:** біткоін, криптовалюта, майнинг, економіка.

### Abstract

*This article focuses on the definition of bitcoin, it's characteristics and describes the process of mining (achieving) bitcoins.*

**Keywords:** bitcoin, cryptocurrency, mining, economics.

### Introduction

Bitcoin is a form of digital currency created and held electronically. No one controls it. Bitcoins aren't printed like dollars or euros – they're produced by people, and businesses running computers all around the world, using software that solves mathematical problems.

It's the first example of a growing category of money known as cryptocurrency.

### What is Bitcoin?

Bitcoin is a cryptocurrency and a payment system invented by an unidentified programmer, or group of programmers, under the name of Satoshi Nakamoto. Bitcoin was introduced on 31 October 2008 to a cryptography mailing list, and released as open-source software in 2009. There have been various claims and speculation concerning the identity of Nakamoto, none of which are confirmed. The system is peer-to-peer and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in a public distributed ledger called the blockchain, which uses bitcoin as its unit of account. Since the system works without a central repository or single administrator, the U.S. Treasury categorizes bitcoin as a decentralized virtual currency. Bitcoin is often called the first cryptocurrency, although prior systems existed and it is more correctly described as the first decentralized digital currency. Bitcoin is the largest of its kind in terms of total market value.

Bitcoins are created as a reward in a competition in which users offer their computing power to verify and record bitcoin transactions into the blockchain. This activity is referred to as mining and successful miners are rewarded with transaction fees and newly created bitcoins. Besides being obtained by mining, bitcoins can be exchanged for other currencies, products, and services. When sending bitcoins, users can pay an optional transaction fee to the miners. This may expedite the transaction being confirmed.

What makes it different from normal currencies? Bitcoin can be used to buy things electronically. In that sense, it's like conventional dollars, euros, or yen, which are also traded digitally. However, bitcoin's most important characteristic, and the thing that makes it different to conventional money is that it is decentralized. No single institution controls the bitcoin network. This puts some people at ease because it means that a large bank can't control their money.

Who created it? A software developer called Satoshi Nakamoto proposed bitcoin, which was an electronic payment system based on mathematical proof. The idea was to produce a currency independent of any central authority, transferable electronically, more or less instantly, with very low transaction fees.

Who prints it? No one. This currency isn't physically printed in the shadows by a central bank, unaccountable to the population, and making its own rules. Those banks can simply produce more money to cover the national debt, thus devaluing their currency. Instead, bitcoin is created digitally, by a community of people that anyone can join. Bitcoins are 'mined', using computing power in a distributed network. This network also processes transactions made with the virtual currency, effectively making bitcoin its own payment network.

So you can't churn out unlimited bitcoins. The bitcoin protocol – the rules that make bitcoin work – says that only 21 million bitcoins can ever be created by miners. However, these coins can be divided into smaller parts (the smallest divisible amount is one hundred millionth of a bitcoin and is called a 'Satoshi', after the founder of bitcoin).

What are its characteristics? Bitcoin has several important features that set it apart from government-backed currencies.

1. It's decentralized. The bitcoin network isn't controlled by one central authority. Every machine that mines bitcoin and processes transactions makes up a part of the network, and the machines work together. That means that, in theory, one central authority can't tinker with monetary policy and cause a meltdown – or simply decide to take people's bitcoins away from them, as the Central European Bank decided to do in Cyprus in early 2013. And if some part of the network goes offline for some reason, the money keeps on flowing.

2. It's easy to set up. Conventional banks make you jump through hoops simply to open a bank account. Setting up merchant accounts for payment is another Kafkaesque task, beset by bureaucracy. However, you can set up a bitcoin address in seconds, no questions asked, and with no fees payable.

3. It's anonymous. Well, kind of. Users can hold multiple bitcoin addresses, and they aren't linked to names, addresses, or other personally identifying information. However...

4. It's completely transparent. ...bitcoin stores details of every single transaction that ever happened in the network in a huge version of a general ledger, called the blockchain. The blockchain tells all. If you have a publicly used bitcoin address, anyone can tell how many bitcoins are stored at that address. They just don't know that it's yours. There are measures that people can take to make their activities more opaque on the bitcoin network, though, such as not using the same bitcoin addresses consistently, and not transferring lots of bitcoin to a single address.

5. Transaction fees are miniscule. Your bank may charge you a £10 fee for international transfers. Bitcoin doesn't.

6. It's fast. You can send money anywhere and it will arrive minutes later, as soon as the bitcoin network processes the payment.

7. It's non-repudiable. When your bitcoins are sent, there's no getting them back, unless the recipient returns them to you. They're gone forever.

So, bitcoin has a lot going for it, in theory. But how does it work, in practice?

### **How to mine Bitcoins**

Before you start mining Bitcoin, it's useful to understand what Bitcoin mining really means. Bitcoin mining is legal and is accomplished by running SHA256 double round hash verification processes in order to validate Bitcoin transactions and provide the requisite security for the public ledger of the Bitcoin network. The speed at which you mine Bitcoins is measured in hashes per second.

The Bitcoin network compensates Bitcoin miners for their effort by releasing bitcoin to those who contribute the needed computational power. This comes in the form of both newly issued bitcoins and from the transaction fees included in the transactions validated when mining bitcoins. The more computing power you contribute then the greater your share of the reward.

To begin mining bitcoins, you'll need to acquire bitcoin mining hardware. In the early days of bitcoin, it was possible to mine with your computer CPU or high speed video processor card. Today that's no longer possible. Custom Bitcoin ASIC chips offer performance up to 100x the capability of older systems have come to dominate the Bitcoin mining industry.

Bitcoin mining with anything less will consume more in electricity than you are likely to earn. It's essential to mine bitcoins with the best bitcoin mining hardware built specifically for that purpose. Several companies such as Avalon offer excellent systems built specifically for bitcoin mining.

Once you've received your bitcoin mining hardware, you'll need to download a special program used for Bitcoin mining. There are many programs out there that can be used for Bitcoin mining, but the two most popular are CGminer and BFGminer which are command line programs.

If you prefer the ease of use that comes with a GUI, you might want to try EasyMiner which is a click and go windows/Linux/Android program.

Once you're ready to mine bitcoins we recommend joining a Bitcoin mining pool. Bitcoin mining pools are groups of Bitcoin miners working together to solve a block and share in its rewards. Without a Bitcoin mining pool, you might mine bitcoins for over a year and never earn any bitcoins. It's far more convenient to share the work and split the reward with a much larger group of Bitcoin miners.

The following pools are believed to be currently fully validating blocks with Bitcoin Core 0.9.5 or later (0.10.2 or later recommended due to DoS vulnerabilities): BitMinter, CK Pool, Eligius.

The next step to mining bitcoins is to set up a Bitcoin wallet or use your existing Bitcoin wallet to receive the Bitcoins you mine. A Bitcoin wallet is like a traditional wallet and can be software, mobile or web-based. Bitcoin hardware wallets are also available.

Bitcoins are sent to your Bitcoin wallet by using a unique address that only belongs to you. The most important step in setting up your Bitcoin wallet is securing it from potential threats by enabling two-factor authentication or keeping it on an offline computer that doesn't have access to the Internet. Wallets can be obtained by downloading a software client to your computer.

### **Conclusion**

Bitcoin is a digital asset designed by its inventor, Satoshi Nakamoto, to work as a currency. It is commonly referred to with terms like: digital currency, digital cash, virtual currency, electronic currency, or cryptocurrency.

The question whether bitcoin is a currency or not is still disputed. Bitcoins have three useful qualities in a currency, according to The Economist in January 2015 they are "hard to earn, limited in supply and easy to verify". Economists define money as a store of value, a medium of exchange, and a unit of account and agree that bitcoin has some way to go to meet all these criteria. It does best as a medium of exchange, as of February 2015 the number of merchants accepting bitcoin has passed 100,000. As of March 2014, the bitcoin market suffered from volatility, limiting the ability of bitcoin to act as a stable store of value, and retailers accepting bitcoin use other currencies as their principal unit of account.

### **СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ**

1. Andreas M. Antonopoulos. *Mastering Bitcoin* / A.M. Antonopoulos. — O'Reilly, 2015. — 640 pages.
2. Brian Kelly. *The Bitcoin Big Bang* / B. Kelly. — Wiley, 2012. — 547 pages.
3. Michael J. Casey. *The Age of Cryptocurrency* / M.J. Casey, P. Vigna. — St. Martin's Press, 2013. — 492 pages.

**Концевой Антон Александрович** — студент групи 2СІ-146, факультет комп'ютерних систем та автоматички, Вінницький національний технічний університет, Вінниця, e-mail: anton.96k@gmail.com

Науковий керівник: **Тулчак Людмила Володимирівна** – старший викладач англійської та німецької мов, кафедра іноземних мов, Вінницький національний технічний університет, Вінниця

**Kontsevoy A.O.** — Student of group 2SE-14, Faculty of Computer Systems and Automatics, Vinnytsia National Technical University, Vinnytsia, email : anton.96k@gmail.com

Supervisor: **Tulchak Liudmyla V.** – Senior Teacher of Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia