

# BITCOIN

Vinnysia National Technical University

## Анотація

*В даній доповіді роботі розглядається Біткоїн - перша і найпопулярніша криптовалюта, яка не має єдиного центру емісії та дозволяє здійснювати будь-які операції анонімно, без ідентифікації користувача. Транзакції із цифровим підписом між двома вузлами передаються до всіх вузлів peer-to-peer мережі, а самі дані про переміщення коштів зберігаються у розподіленій базі даних. Щоб уникнути можливості витратити чужі гроші або використання своїх коштів двічі використовуються криптографічні методи.*

**Ключові слова:** криптовалюта, Біткоїн, peer-to-peer мережі, майнінг.

## Abstract

*Bitcoin is considered in this work. Bitcoin is the first and most popular cryptocurrency that does not have one emission centre and allows to carry out any operations anonymously without user identity. Transactions between two nodes are transmitted to all nodes of peer-to-peer network a with digital signature and the data of all transactions is stored in a distributed database. To prevent spending other's money or someone's own money twice system uses cryptographic methods.*

**Keywords:** cryptocurrency, Bitcoin, peer-to-peer networks, mining.

A cryptocurrency (or crypto currency) is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency [1]. Cryptocurrencies are a subset of alternative currencies, or specifically of digital currencies.

Bitcoin, the world's "first decentralised digital currency", was launched in 2009 by a mysterious person known only by the pseudonym Satoshi Nakamoto, whose true identity is still unknown. Since then, numerous cryptocurrencies have been created [2]. These are frequently called altcoins, as a blend of bitcoin alternative. The value of a single Bitcoin has fluctuated wildly, reaching a high of around \$1,000 in late 2013 before falling to less than half that level, and then rebounding in 2016. What exactly is Bitcoin, and how does it work?

Unlike traditional currencies, which are issued by central banks, Bitcoin has no central monetary authority. Instead it is underpinned by a peer-to-peer computer network [3] made up of its users' machines, akin to the networks that underpin BitTorrent, a file-sharing system, and Skype, an audio, video and chat service. Bitcoins are mathematically generated as the computers in this network execute difficult number-crunching tasks, a procedure known as Bitcoin "mining". The mathematics of the Bitcoin system was set up so that it becomes progressively more difficult to "mine" Bitcoins over time, and the total number that can ever be mined is limited to around 21 million. There is therefore no way for a central bank to issue a flood of new Bitcoins and devalue those already in circulation.

The entire network is used to monitor and verify both the creation of new Bitcoins through mining, and the transfer of Bitcoins between users. A log is collectively maintained of all transactions, with every new transaction broadcast across the Bitcoin network. Participating machines communicate to create and agree on updates to the official log. This process, which is computationally intensive, is in fact the process used to mine Bitcoins: roughly every 10 minutes, a user whose updates

to the log have been approved by the network is awarded a fixed number of new Bitcoins. This has prompted Bitcoin fans to build ever more powerful computers for using in Bitcoin mining.

Bitcoins can be bought and sold in return for traditional currency on several exchanges, and can also be directly transferred across the internet from one user to another using appropriate software. This makes Bitcoin a potentially attractive currency able to settle international transactions, without messing around with bank charges or exchange rates. Some internet services (such as web hosting and online gambling) can be paid for using Bitcoin. The complexity and opacity of the system means it also appeals to those with more nefarious purposes in mind, such as money laundering or paying for illegal drugs. But most people will be reluctant to adopt Bitcoin while the software required to use it remains so complex, and the value of an individual Bitcoin is so volatile. Just as BitTorrent was not the first file-sharing service and Skype was not the first voice-over-internet service, it may be that Bitcoin will be a pioneer in the field of virtual currencies, but will be overshadowed by an easier-to-use rival.

#### СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ / REFERENCES

1. Crypto Currency [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: [www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html](http://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html) – Назва з екрана.
2. Digital Currencies: Principles, Trends, Opportunities, and Risks by Paolo Tasca :: SSRN [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: [papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2657598](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2657598) – Назва з екрана.
3. Collaborative applications over peer-to-peer systems—challenges and solutions | SpringerLink [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: [link.springer.com/article/10.1007%2Fs12083-012-0157-3](http://link.springer.com/article/10.1007%2Fs12083-012-0157-3) – Назва з екрана.

*Науковий керівник: Зубенко Оксана Вячеславівна, викладач кафедри іноземних мов, Вінницький національний технічний університет, Вінниця*

*Дажура Олена Вікторівна, студентка групи 2ПІ-14б, факультет Інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: [molkohelen@gmail.com](mailto:molkohelen@gmail.com)*

*Supervisor: Zubenko Oksana, teacher of English, the Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia*

*Dazhura Olena, student of group 2PI-14b, Faculty for Information Technologies and Computer Engineering. Vinnytsia National Technical University, Vinnytsia, e-mail: [molkohelen@gmail.com](mailto:molkohelen@gmail.com)*