УДК 004.75

С.О. Медведєва
Д.В. Мальований

BASIC PRINCIPLES OF THE BLOCKCHAIN THECHNOLOGY AND ITS APPLICATION

Вінницький національний технічний університет

Анотація:
У даній доповіді розглянуто основні принципи роботи технології блокчейн, її практичну цінність та способи застосування у науковій, медичній, соціальній та фінансовій сферах.
Ключові слова: блокчейн, блок, хеш, криптовалюта, транзакція, загальна обчислювальна потужність.

Abstract:
This paper deals with the main principles of blockchain technology work, its practical value is explained and the ways of application in economical, medical, social and financial areas are shown.
Key words: blockchain, block, hash, cryptocurrency (digital currency), transaction, total computing power.

Introduction

The aim of this paper is to describe the main principles of the new breakthrough technology known as blockchain. Nowadays this topic is of vital importance because blockchain technology and its application is considered to be one of the most perspective branches of the modern science. The purpose of this work is not to reflect the original documentation, but rather to explain the basics of the blockchain kernel. The article will be useful for everyone who is interested in the study of crypto sciences and wants to get the basic understanding of the principals of their work.

The main concepts

The concept of the blockchain technology is quite new. Its development is credited to a person or a group of people known under the pseudonym Satoshi Nakamoto. Blockchain allows digital information to be distributed but not copied. This approach proved to be a breakthrough and has taken an important place in practically all the activities of modern people. In fact, blockchain technology has created the backbone of a new type of the Internet. Originally devised for the digital currency, Bitcoin, the tech community is now finding other potential uses for it. No doubt, that is the technology of the future.

It is much easier to evaluate the importance of the blockchain if you know the principle of its work. Blockchain is a distributed database existing on multiple computers at the same time. It is constantly growing as new sets of recordings, or 'blocks', are added to it. Each block contains a timestamp and a link to the previous block, so they actually form a chain. The database is not managed by any particular body; instead, everyone in the network gets a copy of the whole database. Old blocks are preserved forever and new blocks are added to the ledger irreversibly, making it impossible to do any manipulations with data or to fake documents, transactions and other kinds of information.[1] All this makes blockchain systems very reliable and independent from the external factors.

In theory, if you are going to hack the system or make some manipulations with the data, that have already been saved in one of the previous blocks, you must take more than 51% of all the clients of the system under your control and then you would have to spend as much computing power as has been spent to make the block you are trying to change and all the next blocks; so, you need a few supercomputers to calculate the hashcode. This effect is caused by the very principle of the blockchain because changes in one block will lead to its hashcode become changed. Thus, the next blocks' hashcode will become changed, too. So, we can come to the conclusion that the blockchain system is the system that cannot be hacked. Consequently, it grants unicity, connectivity and security of all the data stored in it. In addition, this system is open, so everyone can check all the data he needs. [2]

Separate blocks' structure

Another interesting aspect of the blockchain technology is the possibility to create new blocks. Every block consists of a set of some transactions (any computer operations performed on some data) which form the body of the block, the hashcode of the current block and the hashcode of the previous block which are located in the title. The title also contains a timestamp in it. It ensures better security and uniqueness of each block. The hashcode of the current block is calculated on the basis on the blocks' body and the hashcode of the previous block. That means the hashcode of the current block depends on the hashcode of all the previous blocks.

Calculating the hashcode, you can check if the all of the previous blocks remain unchanged. In addition, cryptography is used to guarantee synchronization of the copies of the blockchain on each computer (or node) in the network.

As for the creation of new blocks, only the people who have a unique digital cryptographic key can make changes and fill the current block. Such people are generally known as miners in the sphere of digital crypto currency. They create new blocks on their own computing devices and fill them with the transactions. Then the hashcode is calculated. If the hashcode is less than the pre-set number, the block is considered to be accepted. Otherwise, the block is considered to be rejected. If the block is accepted, the system checks if there any clients who have created the block with the same hashcode. If there are no blocks with the same hashcode, the block is entered into the database and is shared among all the clients (also called nodes). It usually takes about 20 hours to check out all the new blocks. The block having been accepted, the miner who has written it, receives the reward. Thus, the money earned after creating a new block is available to be spent almost a day after the creation of the block. This security measure is used to prevent situations of accepting two blocks with identical hashcodes. [4]

The practical value

The practical value of the blockchain is hard to overestimate. It can improve most of modern branches of science, economy and industry.

For example, you can think of the blockchain as of a digital medical record system: every record is a block which has a label stating the date and the time when the record was done. The medical history is extremely important for diagnosis and treatment purposes, so neither the doctor nor the patient should be able to modify the records already made. Nevertheless, the doctor owns a private key that allows him to make new records, and the patient owns a public key that allows him to access the records anytime. This method makes the data both accessible and secure.

The blockchain technology is relatively young and it has only started to penetrate into different spheres of human activities, but even now it is widely used in cryptocurrencies such as Bitcoin and Ethereum, in banking management and in finance. It is used to keep records of the population in some developed countries.

Conclusion

To sum up, blockchain is one of the most progressive modern digital technologies that grants accessibility and immutability of data, entered to the block. The basic principle used in the blockchain is dependence of the current blocks on the past ones and distribution of the databases between all the users of this blockchain system. Nowadays this technology has not been fully investigated yet. It is still under development and it tends to improve, but it is already used in economics and for population recording. Its greatest value is that it eliminates the chances to hack the system or change the data. Most of modern digital currencies are based on the blockchain principle. Thus, blockchain combines a lot of advantages and can be used to improve all the spheres of humans' life.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.What blockchain is in layman's terms [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://ihodl.com/tutorials/2017-09-04/what-blockchain-laymans-terms/(дата звернення 11.02.19). – Назва з екрана.

2.Блокчейн [Електронний ресурс] : [Веб-сайт]. – Режим доступу: https://uk.wikipedia.org/wiki/Блокчейн (дата звернення 11.02.19). – Назва з екрана.

3.Melanie Swan. Blockchain: Blueprint for a New Economy. — 2015. — 152 p. — ISBN 978-1-4919-2047-3.

4.Nakamoto, Satoshi (2008). Bitcoin: A Peer-to-Peer Electronic Cash System

Мальований Дмитро Вадимович – студент групи 1ІСТ-18Б, кафедра автоматизації та інтелектуальних інформаційних технологій, Факультет комп'ютерних систем і автоматики, Вінницький національний технічний університет, м.Вінниця, e-mail fkca.1ict18.mdv@gmail.com

Медведєва Світлана Олександрівна – викладач кафедри іноземних мов, Вінницький національний технічний університет, м.Вінниця, e-mail Svetlana.med79@gmail.com

Maliovanyi Dmytro Vadymovych – student of 1IST-18B group, Department of Automatization and Intellectual Informational Technologies, Faculty of Computer Systems and Automatics, Vinnytsia National Technical University, Vinnytsia, e-mail fkca.1ict18.mdv@gmail.com

Medvedieva Svitlana Oleksandrivna – the teacher of English, Department of the Foreign Languages, Vinnytsia National Technical University, Vinnytsia, e-mail Svetlana.med79@gmail.com