Список литературы:

1. Халтуринский Н. А., Крупкин В. Г. О механизме образования огнезащитных вспучивающихся покрытий // Пожаровзрывобезопасность 2011 том 20 №10. – С. 33-36
2. Решетников И. С., Халтуринский Н. А. О моделировании горения коксообразующих полимерных систем // Химическая физика. – 1997. – Т. 16, № 3. – С. 102.
3. Решетников И. С., Халтуринский Н. А. Некоторые особенности теплопереноса в пенококсах, образующихся при горении // Хим. физика. – 1997. – Т. 16, № 10. – С. 104-108.
4. Reshetnikov l. S., Khalturinskij N. A. Three-dimensional model of heat transfer in foamed chars // Advances in Computational Heat Transfer: Intern. Symp. – Izmir: Cesme, 1997. – P. 334.
5. Яблокова М. Ю., Решетников И. С., Халтуринский Н. А. Полимерные смеси – путь к созданию композиций с регулируемыми свойствами для огнезащитных покрытий // Фундаментальные проблемы науки о полимерах: междунар. конф. – М., 1997. – С. 2.

HOW DOES A BLOCKCHAIN WORK?

Islomjon Abdullayev,
Independent researcher,
islomjon7200@gmail.com)

Satoshi Nakamoto mentioned the Bitcoin as a combinational integration of e-signatures, which can also be called “blockchain”. The blockchain creates a chance for bitcoin transfer among users without a need for third parties (financial institutions). The illustration of the blockchain usage can be exemplified with the Bitcoin in Figure 1. The reason behind why the e-currencies are called “cryptocurrencies” is that blockchains such as Bitcoin utilizes cryptography to regulate the transactions. Balance of the Bitcoin users are secured with a private key. The legal permission for transactions is given by a group of users known as “miners”, they benefit from sharing database and distributing processing and receiving additional bitcoins in exchange.

Figure 1. Working process of the Bitcoin blockchain

Alice lends Bob for lunch. So that to create a new Bitcoin wallet, Bob installs an app on his phone. A wallet app and a wallet can work the same as a mobile banking app and a bank account respectively.	It is required two types of information to pay back to her: Bob’s private key and Alice’s public key.	Alice’s public key can be accessed through scanning her QR code from her smartphone or getting her email address.	The app works as an alerting machine for the miners around the world about the ongoing transaction. Then, the miners provide legalising activity for the transaction.	The miners check the Bob’s wallet whether there is enough bitcoins to make payment.	In a given period of time, there will be many transactions pending to occur. In the net, all of the transactions are grouped creating a block according to their timeframe and verified by the miners. Certain identification number and creation time is allocated to each block, as well as creating reference to the previous block.

**With the help of the public key, the user can send money to any account, however, private key is the one that allows to release the money out of the wallet.*

What is in a blockchain?

No matter how complex is the blockchain, it is also a type of platform in which transactions are recorded and copied to the all computers in the network. Therefore, a blockchain is also known as “a distributed ledger”. A blockchain consists of blocks and these blocks are used to store the data. A block has two basic integral parts:

- ***It is header*** that consists of metadata such as a reference number, creation time of the block and the link between current and previous block.
- ***It is content***, which works as a history for the database and includes confirmed list od electronic assets, previous transactions and their capacity and address of the parties.

Taking the latest block of the chain in to consideration, the history of other blocks linked to the current one can be viewed and this makes all the blocks from the very first one to the last available and verifiable. Since the use of crypto currencies has been raising rapidly, verification process has become harder and this process eased by blockchains.





Once a block is created in the network, the miners check it for legality and this process is concerned with complex cryptographic check it for legality and this process is concerned with complex cryptographic calculations.

When the cryptographic problem is solved, it will exposed to the whole network.

The new blockchain is added and the system allocates 25 bitcoins to the winning miner. The blockchain is created as a block joins to the previous one.

Once Bob opens the transaction, confirmation about the bitcoin transfer is sent to both of them within ten minutes.

Each step in the block followed and finally Alice receives the money.

What are the differences between public and private blockchains?

Blockchains can be divided to public and private as other types of database. The bitcoin can be example of public one since there is no restriction to write or read any data from the ledger with appropriate bitcoin software. On the other hand, private blockchains include the participants called a priori and acquires the right to update the ledger. The public and private blockchain participants may be from the same or different organization and the relationship among them are regulated with informal arrangements, formal contracts or confidentiality agreements.

When there is no trust among the participants, the public blockchains need extra mechanisms to promote the integrity of the data. As there is no authority to regulate the works of the participants in the decentralised network, this adds complexity to the process. In an example of the bitcoin blokchain a new transaction to the blockchain can only be added if the complex mathematical problem (“proof-of-work”) is solved by the participant. The process indicated above is known as “mining”. The miners’ effort to solve the mathematical problem without being familiar with each other indicates the validity of the transactions.

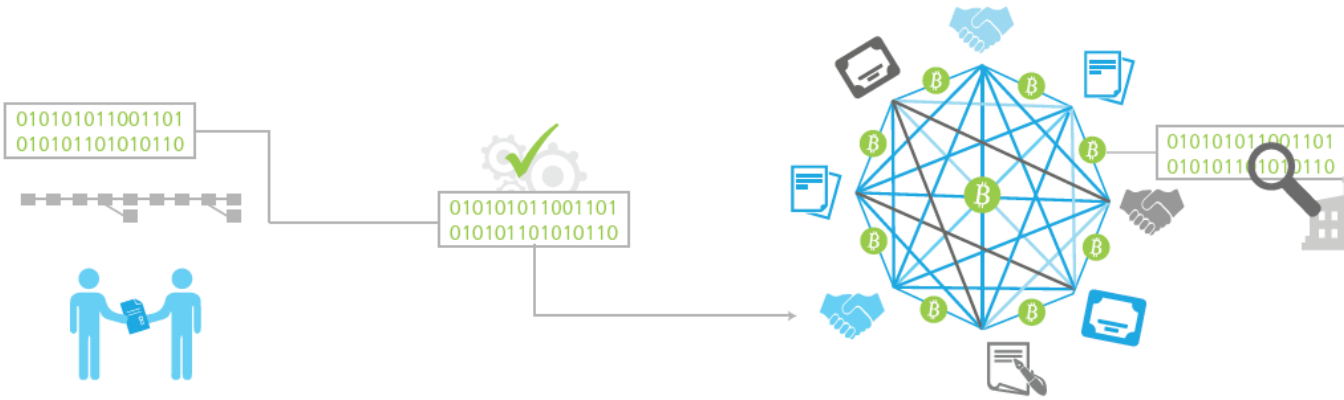
What alternatives are there to the Bitcoin blockchain?

A blockchain is used in many ways. Recently, different types of blockchain, to gather with bitcoin blockchain, have become popular. However, they have not reached the same level as the bitcoin blockchain despite their additional benefits such as higher speed, higher volume of data storage and higher level of functionality. Litecoin is one example of the competitor for bitcoin with lower data capacity, but higher speed in transactions. Moreover, one of the simpler type of chain of blocks creation with lower cost on international payment through bank and non-bank financial institutions is the

Ripple Transaction Protocol. The way of validating the transactions on Bitcoin and Ripple's distributed ledger differs with the proof-of-work and consensus respectively due to level of trust.

On the other hand, Ethereum is an open-source funded project like the Bitcoin blockchain, however gives a chance to network participants to regulate their own contracts and follows a certain rules and regulations. The most important aspect is the smart contracts that can allow the transformation of the business initiatives in different industry sectors. In figure 2, the way in which Bitcoin-based smart contracts opens the way for transparency in investment banking.

Figure 2. Using the Bitcoin blockchain for smart contracts



1. An option contract with parties involved will be in the form of codes in the blockchain. Despite anonymity of individuals, the public ledger is the place for the contract.

2. A triggering event like an expiration date and strike price is hit and the contract executes itself according to the coded terms.

3. Keeping the privacy of the users, the regulators can understand the activity in the market with the help of the blockchain.

Additionally, existing cloud platforms of the technology companies like Microsoft have been making available "Blockchain-as-a-Service" (BaaS). Developers from organizations are prompted by BaaS to deploy private and semi-public blockchains using Bitcoin, Ripple, Ethereum and other protocols.

What blockchains are common to all blockchains?

• ***Real-time distribution of a blockchain occurs in a number of computers:*** the blockchain do not have a central governance body and one copy of the records is accessible for users and participants of the network. Therefore, there will not be need for central governance through financial bodies like banks and brokerage firms.

•***A blockchain uses many participants in the network to reach consensus:*** the computers of the participants are highly used for authenticating and verifying the blockchain and escaping from the repetition of the same transaction. New blocks are allowed to adopt only if the majority of the participants verifies them.

•***A blockchain uses cryptography and digital signatures to provide identity:*** the transactions can be linked to the cryptographic identities, that are anonymous and gives possibility to define real-life identities through dealing reversely.

•***A blockchain is time-stamped:*** transactions on the blockchain are time-stamped and this helps to track and verify the information.

•***A blockchain is programmable:*** the blocks includes the instructions in it, for instance “if” this “then” do that “else” do this, permits the transactions to happen if certain conditions are matched.

How does a blockchain deliver value?

The nature of Systems, which are working for processing transactions, are not centralized and distributed as the nature of blockchain. Blockchain helps to make current value creation process to be more transparent and user-friendly for some applications. Figure 3 visualises this. One of the developers of the blockchain, Jeff Garzik, advises not to use and rely on it too much: “Do not try to stuff every feature into the Bitcoin protocol. Let do it what it does best. Built systems on top of Bitcoin which use its strengths…. Putting all the world’s coffee transactions, and all the world’s stock trades, and all the world’s Internet of Things device samplings, on the Bitcoin blockchain seems misguided”.

Applications that works with blockchain concerns with both practical and philosophical limits. Thinking more deeply, linking user with institutions using shared ledger gives a chance to end frictions to make transactions faster and cheaper. Blockchain makes organisations to be more different from traditional business in terms of value creation.

Blockchain seems to be obstacle for traditional value exchange institutions such as banks.

The disintermediation is threatened by public blockchains due to connection with peer-to-peer networks. Consumers benefit from the value that came back from the main institutions.

It is also important to claim that during the time when the major transactions benefits from decentralised approach of blockchains, there are still other transactions that should be dealt with traditional approach (veto suspect transactions) despite extra complexity.

Endnotes:

1. “Bitcoin: A Peer-to-Peer Electronic Cash System”, Satoshi Nakamoto, 2008. See also: https://Bitcoin.org/Bitcoin.pdf.
2. “Digital Gold: The Untold Story of Bitcoin”, Nathanial Popper, May 2015.
3. http://blockchain.bankofenglandearlycareers.co.uk/.
4. “Deep shift: Technology tipping points and societal impact”, World Economic Forum, September 2015. *http://www3. weforum.org/docs/ WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.*
5. http://www.coindesk.com/visa-europe-announces-blockchain-remittance-proof-of-concept/.
6. “RBS Trials Ripple as Part of £3.5 Billion Tech Revamp”, Grace Caffyn, CoinDesk, June 2015: http://www.coindesk.com/ rbs-trials-ripple-part-3-5-billion-tech-revamp/.
7. http://siliconangle.com/blog/2015/06/09/westpac-anz-trial-ripples-blockchain-ledger-system-but-say-no-to-Bitcoin-for-now/.
8. http://www.ibtimes.co.uk/cryptocurrency-round-blockchain-bug-commonwealth-bank-australia-embraces-Bitcoin-1503832.
9. http://cointelegraph.com/news/114717/citi-develops-3-blockchains-with-own-citicoin-token.