УДК 004.67
МРНТИ 81.93.29

OVERVIEW OF CHALLENGES FACING BLOCKCHAIN-BASED CRYPTOGRAPHIC CURRENCIES

ZH.M. BEKAULOVA[1], G.U. MAMATOVA[2], G.A. TOLGANBAYEVA[1]

[1]International Information Technology University (IITU)
[2]Academy of Civil Aviation

Abstract: *Blockchain, the foundation of Bitcoin, has received extensive attentions recently. Blockchain serves as an immutable ledger, which allows transactions take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. However, there are still many challenges of blockchain technology such as scalability and security problems waiting to be overcome. Blockchain has numerous benefits such as decentralization, persistency, anonymity and auditability. This paper presents a comprehensive overview on blockchain technology. We provide an overview of blockchain architecture firstly and compare some typical consensus algorithms used in different blockchains. Furthermore, technical challenges and security issues are briefly listed. We also lay out possible future trends for blockchain. In general, everything that can be written down on paper can be written in a blockchain with only one difference in a blockchain it is simply impossible to substitute or forge records. In contrast to computer security taken in a traditional sense, the notion of identification is as important here as that of authentication. Every time a transaction or block of data is added to the chain a majority of the network must verify its validity. In the case of a contractual blockchain, the identification must take into account the complete person-identity-proof sequence to create legal effects. This article reviewed challenges that might arise on every step of integrating decentralized peer-to-peer cryptocurrency into our daily lives. It discussed implementation details and problems and challenges that might arise during the cryptocurrency adoption phase. Despite the possible challenges, cryptocurrencies might still shape the future of digital payments and create their own niche.*

Keywords: *Blockchain, ledger, entity, database, crypto-currencies*

ПРОБЛЕМЫ КАСАЮЩИХСЯ КРИПТОГРАФИЧЕСКИХ ВАЛЮТ НА ОСНОВЕ БЛОКЧЕЙН

Аннотация: *Blockchain – это основа Биткойн, которая имеет большое привлечение внимания. Технология служит неизменным регистром, которая позволяет децентрализованно осуществлять транзакции. Появляются приложения на основе блокчейна, охватывающие множество областей, включая финансовые услуги, Интернет вещей (IoT) и так далее. Тем не менее, есть еще много проблем этой технологии, таких как масштабируемость и проблемы безопасности, которые еще предстоит решить. Блокчейн имеет множество преимуществ, таких как децентрализация, постоянство, анонимность и возможность аудита. В этой статье представлен всеобъемлющий обзор технологии блокчейна. Сначала проводится обзор архитектуры блокчейна и сравниваются некоторые типичные согласованные алгоритмы, используемые в разных блокчейнах. Также кратко перечислены технические проблемы и проблемы безопасности. Затем будут изложены возможные будущие тенденции для блокчейна. В общем, все, что может быть записано на бумаге, может быть записано в блокчейне с одним лишь отличием, которое просто невозможно изменить или подделать. В отличие от компьютерной безопасности, взятой в традиционном смысле, понятие идентификации здесь так же важно, как и понятие аутентификации. Каждый раз, когда транзакция или блок данных добавляются в цепочку, большая часть сети должна проверить ее правильность. В случае контрактной блокчейна идентификация должна учитывать полную последовательность доказательства личности для*

создания юридических последствий. Также, рассматриваются проблемы, которые могут возникнуть на каждом этапе интеграции децентрализованной одноранговой криптовалюты в нашу повседневную жизнь. В нем обсуждались детали реализации, а также проблемы, которые могут возникнуть на этапе принятия криптовалюты. Несмотря на возможные проблемы, криптовалюты могут по-прежнему формировать будущее цифровых платежей и создавать свою собственную нишу.

Ключевые слова: *блокчейн, регистр, база данных, криптовалюта*

БЛОКЧЕЙН НЕГІЗІНДЕГІ КРИПТОГРАФИЯЛЫҚ АКТИВТЕРГЕ АРНАЛҒАН МӘСЕЛЕЛЕР

Аңдатпа*: Биткоиннің іргетасы Blockchain-ға жақында айрықша көңіл бөлінді. Blockchain орталықсыздандырылған тәртіпте транзакциялардың орындалуына мүмкіндік береді. Blockchain негізіндегі қосымшалар қаржы қызметтерін, беделі мен Интернетті (IoT) және басқа да көптеген салаларды қамтиды. Дегенмен, қиындықтар мен қауіпсіздіктің еңсеруін күткен проблемалар секілді Blockchain технологиясының әлі күнге дейін біраз қиыншылықтары бар. Blockchain-де орталықсыздандыру, тұрақтылық, жасырындық пен сенімділік сияқты біршама артықшылықтары бар. Бұл мақалада блоктау технологиясы бойынша кеңейтілген шолу берілген. Біз ең алдымен Blockchain архитектурасына шолу жасаймыз және әртүрлі блокталуларда пайдаланылатын кейбір консенсустық алгоритмдерді салыстырамыз. Сонымен қатар, техникалық және қауіпсіздік мәселелерге қысқаша тоқталамыз. Сондай-ақ келешекке арналған болашақ трендтерді қарастырамыз. Жалпы алғанда, қағазға жазуға болатын барлық нәрсе Blockchain-ға жазылуы мүмкін, тек Blockchain-дегі бір ғана айырмашылық бар, ол жазбаларды ауыстыру немесе жазу мүмкін емес. Дәстүрлі мағынада компьютерлік қауіпсіздіктен айырмашылығы, сәйкестендіру ұғымы түпнұсқаландыру сияқты маңызды. Әрбір транзакция немесе деректер блогы тізбеге қосылған сайын желінің көпшілігі оның жарамдылығын тексеруі керек. Келісімшарттық блок-схема жағдайында сәйкестендіру толық заңды тұлғаны есепке алу керек, ол заңды салдарларды жасау үшін сәйкестендірілмеген дәйектілік. Мақалада орталықсыздандырылған теңдестірілген криптовалютаны күнделікті өмірімізге біріктірудің әрбір қадамында туындауы мүмкін қиындықтар қарастырылды. Сондықтан криптовалюталарды қабылдау кезеңінде туындауы мүмкін мәселелер талқыланады. Туындайтын кедергілерге қарамастан, криптовалюталар әлі де цифрлы төлемдердің болашағын қалыптастырып, өз орнын құруы мүмкін.*

Түйінді сөздер: *Блокчейн, блок-тізбек, дерек, криптовалюта*

INTRODUCTION

Cryptographic payment systems based on the Blockchain technology started to emerge after the concept was described in a white paper written by the creator of Bitcoin, Satoshi Nakamoto, in 2008. Bitcoin was a first decentralized cryptocurrency powered by its users to ensure trust in transactions and network security, and it had to overcome certain challenges before being widely recognized and adopted.

The purpose of the article is to identify and analyze challenges that cryptocurrencies may face, taking Bitcoin as the main example. The article will focus on security challenges and challenges that might emerge during cryptocurrency adoption phase.

Architectural challenges

Since the main purpose of Bitcoin was to create a decentralized payment environment, one of the main advantages of Bitcoin over traditional currencies is absence of central regulating authority or middlemen. Payments in such environment need to be done between two consenting parties without the involvement of a trusted third party. As a first security frontier, the transaction has to be signed with the owner's private key. This proves the fact of payment and ensures that trans-action cannot be altered in the future [4].

To finalize payment, the transaction has to be added to the Bitcoin blockchain, and that is where the distributed consensus mechanism comes into action. Bitcoin distributed consen-

sus system "enforces a chronological order in the blockchain, protects the neutrality of the network, and allows different computers to agree on the state of the system. To be confirmed, transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all following blocks" [4].

The system uses the concept of proof-of-work to issue new coins and record past transactions at the same time, thereby incentivizing users to use computing powers of their machines to "mine" bitcoins. The computing resources are used to solve a difficult cryptographic problem, and whoever solves it first is allowed to generate new coins and record pending transactions onto the Blockchain network. The more computing power a user possesses, the higher the chance of solving the puzzle. However, note that the user with the highest computing power is not guaranteed to solve the puzzle, since the chances of solving the puzzle are distributed proportionally to computing power of bitcoin miners (users who try to solve the puzzle). According to theoretical foundation of Bitcoin, the best way to solve the puzzle is to randomly guess, so the deciding factor in solving it is the number of guesses per unit of time, which is proportional to computing power. This mechanism ensures that no individual party can control what gets saved on the block chain [1].

Each new block has to contain the cryptographic has of the previous block. This way, the chain of blocks can tracked down to the very first block. Changing any piece of data in any block in the blockchain will result into breaking cryptographic integrity, which can be immediately known to all nodes on the system.

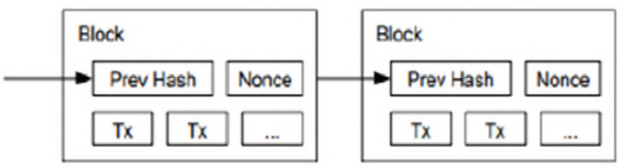

Figure 1- Example of blocks containing hashes of the previous blocks [1]

Security issues

While the implementation of Blockchain based cryptographic currencies is justified by research, such systems might still have vulnerabilities. This section will discuss possible vulnerabilities of such crypto-currencies and methods to prevent malicious attacks.

Record hacking, that is, making unauthorized changes in Blockchain blocks, would require overwriting some amount of consequent blocks. The computing power needed to change that amount of blocks grows exponentially with the length of the Blockchain to be changed [1]. That means, if an attacker wanted to change a substantial number of records, it would only be possible with an immense computing power [3].

Double spending attack is, as its title suggests, spending the same coin two or more times. Receiver of the payment needs to confirm validity of the transaction by checking the Blockchain, so the attacker needs to wait for the transaction to be registered on the block-chain for the first receiver to confirm. Then, if the attacker alters the original Blockchain blocks to make further transactions using the same coin, other receivers would be able to verify validity of those deceiving trans-actions. As in record hacking, this attack also involves altering the Blockchain records with the length of the altered chain of one block. This makes it more realistic to conduct this attack than trying to alter a long chain of blocks [3].

The previous two attacks are commonly known as "51% attacks", since it would require attackers to have more than 50% of computing power of the entire blockchain network to realistically conduct those attacks due to the architecture of bitcoin network. As researchers state, the chances for attackers to break the Bitcoin are virtually zero, since it has grown into a very large network. However, it is very possible to conduct a 51% attack against a younger and smaller payment system based on the same paradigm [3].

Following are the results of the calculation of probability of the attacker catching up, as provided by Nakamoto (2008) [1]:

p = probability an honest node finds the next block

q = probability the attacker finds the next block

qz = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & if\ p \le q \\ (q/p)^z & if\ p > q \end{cases}$$

Then, the probability of the attacker catching up would be

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

where

$$\lambda = z\frac{q}{p}$$

This probability drops exponentially with z, and the attack requires q to be large enough, i.e. the attacker having large enough computing power, comparable with the rest of the network. As was stated above, smaller cryptocurrencies are much more prone to these types of attacks, and the larger ones are relatively safe.

While 51% attacks are directed at the entire network, attacks such as eclipse attacks are directed at single network nodes. Eclipse attack utilizes bitcoin proto-col, which assumes no cryptographic authentication between nodes and each node is only connected with several other randomly selected nodes, not the entire set of nodes on the network. This opens up the vulnerability where the attacker controls only those several nodes, and thus monopolizes all the incoming and outgoing traffic of the victim. This can lead to different unfavorable consequences for the victim, such as seeing non-original version of blockchain or wasting computing power mining coins without a chance to success [5].

Heilman et al (2015) simulated two types of attacks: "(1) infrastructure attacks, modeling the threat of an ISP, company, or nation-state that holds several contiguous IP address blocks and seeks to subvert bitcoin by attacking its peer-to-peer network, and (2) botnet attacks, launched by bots with addresses in diverse IP address ranges" [5].

As Heilman et al (2015) state, other attacks can be performed on top of the eclipse attack:

Engineering block races. A block race condition is when multiple miners discover blocks simultaneously. In a block race, only one block will become a part of blockchain, and miners which have discovered other blocks receive no reward. The attacker can prevent the blocks discovered by eclipsed miners from reaching the main blockchain, so that the victims would waste their computing resources without a chance for reward [5].

Splitting mining power. Eclipsing some fraction of the network makes it more probably to launch 51% attack on the rest of the network [5].

Selfish mining. The attacker increases his chances for reward by not showing discovered by him blocks to eclipsed miners. Eclipsed miners work on their version of blockchain and therefore chances for the attacker to discover new blocks in the original blockchain are in-creased [5].

0-confirmation double spend. This attack exploits merchants who provide goods to customers without seeing a confirmation of transaction on blockchain. If such merchants is eclipsed, malicious customer can spend the same coin twice: in original blockchain and in the eclipsed version of blockchain. Since the merchant cannot access nodes in the original network, first transaction will be added to the blockchain, and the merchant will not receive the money [5].

N-confirmation double-spend. If the merchant requires transaction to be confirmed in a block of depth N −1 in the blockchain to send the goods, the attacker can send this transaction to eclipsed miners, which will add the transaction to the eclipsed version of the blockchain. The attacker can then show this version of the blockchain to the merchant and receive the goods, while retaining his money on the original version of the blockchain [5].

Traditionally, to prevent eclipse attacks it is recommended to disable incoming connections or pick outgoing connections only to whitelisted miners. However, this undermines the ideology of decentralized peer-to-peer payment system, so eclipse attack prevention techniques should be implemented on the protocol level [5].

Adoption challenges

To make a cryptocurrency widespread and trusted, solving technical problems is not enough – there are other things to consider. This paragraph will discuss what could prevent cryptocur-

rencies from becoming widely adopted, taking Bitcoin as an example.

As Luther (2015) claims, the largest preventer of adopting Bitcoin is the incumbent-moneys problem. There are certain costs associated with switching from incumbent monies to Bitcoins – network effects, government sponsorship and legal-tender status.

As stated by Shapiro and Varian (1999), "Network effects occur when the value of a product or service increases according to the number of others using it" [6]. Incumbent monies are entirely adopted by general public, which cannot be said about cryptocurrencies, so cryptocurrencies have to offer something substantial to justify switching to them [2].

Incumbent monies are also sponsored by government, which uses them as an instrument to meet its strategic objectives. Governmental support also makes incumbent monies more trusted for people. In addition to that, cryptocurrencies usual lack legislation built around them, and they usually do not have a legal status of currency. Moreover, governments of some countries even banned cryptocurrencies. Therefore, the cost of switching to cryptocurrencies is currently high [2].

The other issue with cryptocurrencies is that there are many of them. Cryptocurrencies provide different functionality and compete with each other for the user base [2]. Variety of cryptocurrency types does not have a positive impact on the number of users of each, which impedes their perceived value due to network effects.

Despite all of the above, Luther (2015) predicts: "The Blockchain technology will be widely adopted to process digital payment. Bitcoin and other cryptocurrencies, to the extent that they survive at all, will likely function exclusively as niche monies. Bitcoin or some other cryptocurrency might function as more than a niche money in countries with especially weak currencies, even though these countries would seem to pose the greatest regulatory risk to bitcoin".

CONCLUSION

To conclude, the new technology of Blockchain is very relevant and widely used. This reliable and open technology will soon change our life. This article reviewed challenges that might arise on every step of integrating decentralized peer-to-peer cryptocurrency into our daily lives. It discussed implementation details and problems, security issues along with ways to overcome them, and challenges that might arise during the cryptocurrency adoption phase. Despite the possible challenges, cryptocurrencies might still shape the future of digital payments and create their own niche.

REFERENCES

1. Heilman, E., 2015. *Eclipse Attacks on Bitcoin's Peer-to-Peer Network. Proceeding SEC'15 Proceedings of the 24th USENIX Conference on Security Symposium*.
2. Luther, W. J., 2015. Bitcoin and the Future of Digital Payments. *SSRN Electronic Journal. doi:10.2139/ssrn.2631314,* pp. 7-8.
3. Nakamoto, S., 2008. *Bitcoin: A peer-to-peer electronic cash system*.
4. Press., C. S. a. H. R. V., 1999. *Information Rules*: Harvard Business School.
5. S. Haber, W. S., 1991. "How to time-stamp a digital document". *In Journal of Cryptology,* pp. 99-111.
6. Tsilidou, G. F. a. A.-L., 2015. *Further applications of the blockchain*.
7. Xu, J. J., 2016. Are Blockchains immune to all malicious attacks?. *Financial Innovation,* pp. 2(1), 25.