УДК 81 -114.2

E. Shcherbina
V. Mesyura

THE PROBLEM OF BITCOIN BLOCKCHAIN SCALABILITY AND APPROACHES TO ITS SOLUTION

Vinnytsia National Technical University

Анотація
Проаналізовано проблему масштабування біткоїн блокчейну. Розглянуто підходи до її вирішення. Виділено основні типи рішень: оф-чейн протоколи, сайдчейни, централізовані сервіси агрегації транзакцій.
Ключові слова: криптоалюти, біткоін, масштабування, оф-чейн, сайдчейн.

Abstract
The problem of bitcoin blockchain scaling is analyzed. Approaches to its solution are considered. The main types of solutions are highlighted: off-chain protocols, side chains, centralized transaction aggregation services.
Keywords: crypto-currency, bitcoin, scaling, off-chain, side chain.

Introduction

Today, there is a widespread payment method in the world using electronic wallets and cryptocurrency. There are several hundred different cryptocurrencies, but the most popular of them is Bitcoin, an electronic currency that was conceptualized in 2008 by its developer, Satoshi Nakamoto[1].

Main part

Bitcoin, or Bitcoin, is an electronic currency, the concept of which was voiced in 2008 by Satoshi Nakamoto and introduced in 2009, is based on a self-published document by Satoshi Nakamoto. The total capitalization of the bitcoin market as of December 5, 2017, when the exchange rate reached $ 12,000, is $ 200 billion. The average price of one bitcoin as of November 30, 2017 is over $ 10,000 [2]. In December 2017, it became the sixth capitalized currency in the world, beating the ruble, the pound and the South Korean won. On December 7, the course reached its historic next high of $ 17.7 thousand. the next increase to 20 thousand dollars took place on December 17, then the course dropped to 16 thousand. In 2018, the course continued to fall. Periodically, rising and falling by 10-20%, as of April 5, 2018 costs $ 6800.

The problem of scaling in bitcoin blockchain

In order to achieve the decentralization of bitcoin, all its participants are considered equal. In this way, each of the participants (nodes) must keep a complete transaction log and participate in network messaging containing transactions and blocks. Due to this reason we face the problem of scaling [3].

There are several basic approaches to solving this problem:

1. Off-chain protocols
2. Sidechain protocols
3. Centralized optimizations.

These approaches are not mutually exclusive, so they can be combined when implementing a blockchain system. Off-chain and sidechain solutions have been comprehensively reviewed and analyzed by well-known scientists, and the work will focus on solving problems using centralized transaction aggregation systems [4].

Centralized transaction aggregation systems

A bitcoin transaction consists of the following basic elements:

1. Version
2. Inputs
3. Outputs
4. Locktime

The main idea of centralized transaction aggregation service is to accumulate customer intentions to complete transactions over time and aggregate them into one large transaction. This makes it possible to "save" on the "Version" and "Locktime" fields [5]. Also, if multiple transactions are performed for the same recipient in the final transaction, there will be less “Outputs”. Because Output includes scriptPubKey (locking_script), this is a significant optimization [7].

This service offers the following benefits:

1. The average transaction size decreases, resulting in less blockchain load.
2. End users pay a lower transaction fee [7].

Conclusions

Today, there are three main approaches to solving the problem of blockchain scaling: off-chain protocols, sidechain protocols, centralized optimizations. A centralized transaction aggregation approach was considered. Input work will be implemented software implementation of this approach.

REFERENCES

1. W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.
2. H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.
3. D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.
4. S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.
5. A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.
6. R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.
7. W. Feller, "An introduction to probability theory and its applications," 1957.

Щербіна Євгеній Сергійович *— аспірант кафедри КН, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: sototonamitol@gmail.com*

Месюра Володимир Іванович*— канд. техн. наук, доцент, професор кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця.*

Evgeniy S. Scherbina *— postgraduate of the Computer Sciences Chair, Vinnytsia National Technical University, Vinnytsia, e-mail: sototonamitol@gmail.com*

Volodymyr I. Mesyura *— Ph.D., Assistant Professor, Professor of the Computer Science Chair, Vinnytsia National Technical University, Vinnytsia.*

Supervisor: *Stepanova Iryna Sergiivna, head of Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia, stepanova_is@i.ua*