УДК 004.8

Щербіна Є.С.
Месюра В.І.

ПРОБЛЕМА МАСШТАБУВАННЯ БІТКОЇН БЛОКЧЕЙНУ ТА ПІДХОДИ ДО ЇЇ ВИРІШЕННЯ

Вінницький національний технічний університет

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.

Вступ

На сьогоднішній день у світі дуже розповсюджений спосіб оплати з використанням електронних гаманців та готівки, переведеної у криптовалюту. Існує декілька сотень різних криптовалют, проте найпопулярнішою з них є біткоін - електронна валюта, концепт якої був озвучений і 2008 році її розробником - Сатосі Накамото[1].

Основна частина

Bitcoin, або Біткоїн — електронна валюта, концепт якої був озвучений 2008 року Сатосі Накамото, і представлений ним 2009 року, базується на самоопублікованому документі Сатосі Накамото. Повна капіталізація ринку біткоїнів на 5 грудня 2017 року, коли курс сягав 12 000 $, становить 200 млрд USD. Середня ціна одного біткоїна на 30 листопада 2017 року — понад 10 000 $[2]. У грудні 2017 року став шостою за капіталізацією валютою світу, обійшовши рубль, фунт і південнокорейську вону. 7 грудня курс досяг свого історичного чергового максимуму в 17,7 тис. дол. наступний ріст до 20 тис доларів відбувся 17 грудня, потім курс впав до 16 тис. У 2018 році курс продовжив падати. Періодично підіймаючись і падаючи на 10-20%, станом на 5 квітня 2018 року коштує 6800 дол.

Проблема масштабування в біткоїн блокчейні

Для досягнення децентралізації біткоїну всі її учасники розглядаються як рівнозначні. Таким чином кожен з учасників (вузлів) має зберігати весь реєстр транзакцій та приймати участь у мережевому обміні повідомленнями, що містять у собі інформацію про транзакції та блоки. Саме через це ми стикаємося з проблемою масштабування[3].

Існує декілька основних підходів до вирішення даної проблеми:

1. Оф-чейн протоколи
2. Сайдчейн протоколи
3. Централізовані оптимізації.

Дані підходи не є взаємовиключними, отже можуть бути поєднані при реалізації блокчейн системи. Рішення проблеми за допомогою оф-чейн та сайдчейн протоколів були вичерпно розглянуті та проаналізовані відомими вченими, робота буде сфокусована на вирішенні проблеми за допомогою централізованих систем агрегації транзакцій[4].

Централізовані системи агрегації транзакцій

Транзакція у біткоїні складається з таких основних елементів:

1. Version

2. Inputs
3. Outputs
4. Locktime

Основна ідея сервісу централізованої агрегації транзакцій полягає у тому щоб накопичувати наміри клієнтів виконати транзакції напротязі деякого часу та загрегувати їх в одну велику транзакцію. Завдяки цьому є можливість “зекономити” на полях “Version” та “Locktime”[5]. Також у разі виконання декількох транзакцій для одного і того ж отримувача у кінцевій транзакції буде менша кількість “Outputs”. Оскільки “Output” включає в себе scriptPubKey (locking_script) - це є суттєвою оптимізацією[7].

Даний сервіс надає наступні переваги:

1. Зменшується середній розмір транзакції, внаслідок чого зменшується навантаження на блокчейн.
2. Кінцеві користувачі сплачують меншу комісію за транзакцію[7].

Висновки

На сьогоднішний день можна виділити три основні підходи до вирішення проблеми масштабування блокчейну: оф-чейн протоколи, сайдчейн протоколи, централізовані оптимізації. Було базово розглянуто підхід з централізованою агрегацією транзакцій. Вході роботи буде здійснено програмну реалізацію даного підходу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

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.*