УДК 339.1

В.Г. Станіславський
аспірант кафедри бізнес-адміністрування та корпоративної безпеки
Міжнародний гуманітарний університет,
м. Одеса, Україна
Науковий керівник: ***А.Г. Гончарук***
доктор економічних наук, професор,
завідувач кафедри бізнес-адміністрування та корпоративної безпеки
Міжнародний гуманітарний університет,
м. Одеса, Україна

ЕФЕКТИВНІСТЬ УПРАВЛІННЯ ТРАНЗАКЦІЯМИ В УМОВАХ ДЕЦЕНТРАЛІЗАЦІЇ ТА МАСШТАБОВАНОСТІ МЕРЕЖІ BITCOIN

Анотація. *У статті будуть розглянуті проблеми масштабованості мережі класичного блокчейну в умовах збільшення навантаження на мережу і популяризації технології при використанні в децентралізованій платіжній системі bitcoin. Автор спробує зв'язати економічну доцільність, масштабованість мережі і децентралізацію як шляхи збільшення ефективності і гнучкості управління транзакціями біткоїну.*

Ключові слова: *bitcoin, blockchain, SegWit, Lightning Network, децентралізація, масштабованість, управління, транзакції біткоїну.*

Постановка проблеми. Проблема масштабованості біткоїнів пов'язана з початковим обмеженням розробниками розміром в один мегабайт базової структури для зберігання даних (блоку) в його блокчейні [1] [2] [3]. Таке обмеження продиктовано особливістю побудови блокчейну, як повністю реплікованої розподіленої бази даних, що вимагає постійного пересилання між усіма учасниками кожного нового елемента. З ростом популярності біткойнів число транзакцій збільшилося, але через обмеження максимального розміру блоків не всі транзакції «містилися» відразу, періодично виникала черга. У травні 2017 року ситуація сильно погіршилася, очікування включення транзакції в блок сягало кількох днів [4] [5]. В системі біткойнів для прискорення обробки користувач може добровільно призначити комісію. Регулярне виникнення черги призвело до збільшення транзакційних зборів, але не усунуло затримку обробки транзакцій. Це робить використання біткойнів досить дорогим і тривалим, особливо для невеликих платежів – зникає сенс використовувати їх, наприклад, в кафе і барах [4]. Збільшення пропускної здатності біткойна було досить болючою темою в криптосвіті і нерідко приводило до протистояння між майнерами, які перевіряють транзакції біткойнів, і розробниками, які створюють програмне забезпечення для роботи з блокчейном, або розподіленим регістром, який підтримує віртуальний актив. Критики стверджують, що збільшення кількості одиниць або мегабайт, які можуть бути оброблені в транзакції, призведе до зростання витрат для майнерів і витіснить цю групу користувачів, порушивши природне децентралізоване співтовариство верифікаторів валюти.

Аналіз останніх досліджень і публікацій. Проблематика масштабування порушена в статтях таких журналів, як «coindesk.com», «news.bitcoin.com», активно обговорюється на тематичних конференціях і супроводжуються обговореннями в блогах відомих розробників та інвесторів, таких як «antonopoulos.com», «rogerver.com» , «twitter.com/tonevays» тощо.

Виділення невирішених раніше частин загальної проблеми. Криптоспільнота виділяє дві великі проблеми, зокрема помірну централізацію в зв'язку з необхідним збільшенням блоку ланцюга блокчейну. А також фінансовий складник як пряму залежність заробітку власників мережі «Майнерів» від комісій звичайних користувачів. У цій статті автор спробує розібратися в цих двох питаннях, а також розгляне, як звичайні користувачі впливають на навантаження мережі і чому розмір блоку настільки важливий складовий елемент, який змушує криптоспільноту розділятися.

Мета статті. Розглянути наявні проблеми біткоїну, проаналізувати історичні події в межах блокчейну. Визначити найбільш ефективні методи управління транзакціями в умовах граничного розміру блоку, а також розглянути нові технологічні прийоми для збільшення гнучкості транзакцій і розробки протоколу.

Основний матеріал. Проблема масштабування мережі і проблема централізації вже давно турбують криптоспільноту, а також інституційних інвесторів спраглих зайти на ринок криптоактивів. Оскільки біткоїни є програмним забезпеченням з відкритим вихідним кодом, будь-який користувач мережі може копіювати, змінювати і вносити свої правила в роботу цього коду, тим самим створюючи нові протоколи і ланцюжки, які є «Форк» і можуть бути «софт» або «хард». З моменту появи біткоїну в 2008 році мережа цієї криптовалюти проходила через безліч «Форків». З їх допомогою розробники намагалися вирішити проблеми масштабування, підвищити низьку пропускну здатність мережі, змінити лімітований розмір блоку і загалом полегшити навантаження на мережу Bitcoin. Активні суперечки розділили криптоспільноту на два табори, одні з яких за збільшення блоку мережі, другі – проти. Автор статті розглядає «біткоїни» як екосистему, яка сповнена залежностей. Перше, що варто взяти до уваги, це те, що біткоїни це саморегульований актив, який не має єдиного центру або розробника. Це open source продукт, а це означає що весь світ має право вивчати, змінювати і голосувати за зміни даного продукту. Майнери, як власники мережі, обслуговують звичайних користувачів і створюють оптимальні умови для їх роботи, а користувачі своєю чергою забезпечують оптимальні умови для майнерів. І тим і тим дуже вигідно підтримувати і розвивати цей продукт. Оскільки біткоїн створений на дефляційній платформі, емісія весь час скорочується, а монети, які вже знаходяться в обороті, починають дорожчати. Тут же логічно припустити, що зростаюча аудиторія користувачів стимулює попит і пропозицію, що своєю чергою то збільшує то зменшує номінальну ціну біткоїну. Розглянемо технічні аспекти використання для звичайного користувача. 1 BTC = 1000 mBTC = 100 000 000 Satoshi, mBTC – це міллібіткоїн (BTC і mBTC – це як міліметр і метр), Сатоши – це 10 в 8 ступені біткоїна, мінімальна одиниця цієї криптовалюти, названа на честь засновника Bitcoin – Сатоши Накамото. Граничний розмір блоку блокчейна на момент написання статті становить 1мб. Чим більше адрес беруть участь в транзакції – тим довше виходить код, тому що не можна просто так ділити біткоїни. Кожна адреса, з якої отримані кошти – це ± 148 байтів. Кожна адреса, на яку йдуть кошти, – це ± 34 байти. Кожна транзакція займає ще ± 10 байтів, незалежно від кількості адрес, які в ній беруть участь. Наприклад, ви отримали 1 BTC від Мишка, 2 BTC від Яни, 5 BTC від Жені, а потім відправили всі ці BTC (8 штук) Каті, отже, в цій транзакції бере участь 4 адреси!

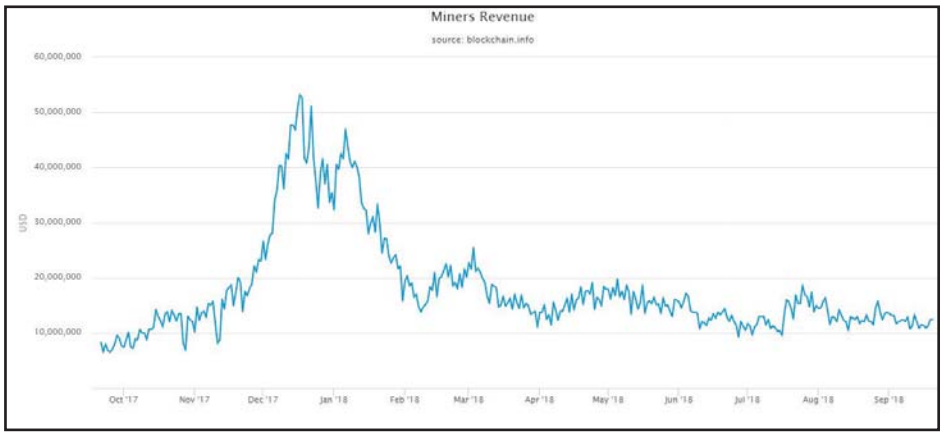
148 × 2 + 34 × 2 + 10 = 374 байти. 34х2, тому що окремою адресою служить адреса майнера для сплати комісії. Розумно припустити, що якщо обмеження блоку складає 1 мб, і чим більше адрес бере участь в транзакції, тим більше місця вона займає. Час перебування блока в середньому 10 хвилин. В один блок може потрапити тільки 2000-3000 транзакцій, а всі інші транзакції чекають своєї черги в так званому mempool. Першим проходить той, хто дасть більше грошей! Важливе зауваження: користувачі зазвичай дивляться, яку комісію вони платять за транзакцію, а майнери дивляться, скільки коштує кожен байт транзакції. Майнер, він же власник мережі, вільний сам вибирати, яким чином формувати блок і які транзакції в нього записувати, адже він з цього заробляє і конкурує з іншими майнерами. Розумно припустити, що більше шансів на те, що майнер вибере 2 транзакції з виставленою комісією в 0.3 ніж 1 транзакцію з комісією в 0.5 з урахуванням, що вона займає теж місце. Або наприклад, в черзі стоїть 10 000 транзакцій, пройти в наступному блоці може тільки 2 500. 9 000 транзакцій стоять з комісією 1 Сатоши / байт. Немає сенсу ставити комісію 8 Сатоши / байт, адже навіть при 2 Сатоши / байт ваша транзакція потрапить в перший же блок. Вартість транзакції в мережі біткоїнів не залежить від суми транзакції, вона залежить від кількості адрес, які беруть участь в ній. Отже, буде вірно припустити, що здебільшого, під час переведення великої суми, ця сума буде зібрана з декількох «вхідних транзакцій». Виходить, що не розібравшись з комісійними зборами, звичайний користувач має всі шанси переплатити комісію, особливо якщо ця комісія визнана за стандарт в будь-якому біткоїн гаманці, який може бути розроблений ким завгодно. Звичайно ж, мінімізація транзакційних витрат дуже важлива для звичайного користувача, але давайте розглянемо всі ризики майнерів. Нагорода за знаходження блоку стартувала з 50 BTC і зменшується на половину кожні 210 000 блоків, тобто ділиться навпіл. Складність змінюється кожні 2 016 блоків і залежить від часу, який буде потрібний для знаходження попередніх 2 016 блоків. Якщо блок буде знаходитися кожні 10 хвилин (як це замислювалося спочатку для рівномірної емісії), знаходження 2 016 блоків займе рівно 2 тижні. Якщо попередні 2 016 блоків були знайдені за термін більше 2-х тижнів – складність буде зменшена, якщо менше – складність буде збільшена. Чим більше (або менше) часу було витрачено на знаходження попередніх 2 016 блоків, тим більше зменшиться (або збільшиться) складність. Хоча розробники характеризують процес майнінгу як «Лотерею», можна припустити, що сильне збільшення складності централізує систему, віддаючи переваги більш сильним «пулам», в яких зосереджена більша кількість майнерів. Отже, іншим майне-

рам залишається тільки об'єднуватись в такі ж пули, все більше централізуючи систему. Для забезпечення дешевизни транзакцій, виступаючи таким чином «антимонопольною комісією» (ціновим регулятором), кріптоспільнота запропонувала збільшити розмір блоку для збільшення пулу і зменшення черги транзакцій, що дозволило б зменшити комісії користувачів. Підтримувати блокчейн – дороге задоволення. Щоб записати транзакцію на тисячах серверів, а деякі з них можуть виявитися ворожими системі, потрібно витрачати значно більше коштів, ніж на запис транзакції на одному централізованому сервері. Автор вважає, що у свій потяг залишити біткоїни дешевими, прихильники цієї ідеї поширюють політику, яка загрожує безпеці мережі. Ідея полягає в тому, що більший простір усередині блоку веде до більшої кількості користувачів, дешевих транзакцій, а це значить – число вузлів (людей, які тримають так званий «повний клієнт» і зберігають у себе копію всього блокчейну, що підтверджує, що мережа цілісна) буде збільшуватися. Таким чином, криптоєнтузіасти вважають, що мережа буде більш надійною. Повний розмір блокчейну на момент написання статті становить понад 200 ГБ [6]. На думку автора, це досить великий простір, який вимагається від користувача, щоб підтримувати «повний вузол». Швидше за все, звичайні користувачі обійдуться легким гаманцем, який дозволяє переказувати та отримувати біткоїни, ніяк не додаючи надійності самій мережі. Багато криптоєнтузіастів вважають, що збільшена продуктивність жорстких дисків, пропускна здатність мереж, а також обчислювальна потужність комп'ютерів майбутнього поглинуть вартість утримання мережі зі збільшеними блоками. Автор вважає, що все це не має значення. Коли блок транзакцій знаходиться майнером, він повинен бути поширений по всій мережі. Таким чином, є аспект, який впливає на гонку між майнерами за право першим знайти і поширити блок – це інтервал часу, який необхідний блоку для поширення (якщо бути більш точним, то це інтервал часу між знаходженням блоку одним з конкуруючих майнерів і моментом, коли цей блок отримає перший сторонній вузол мережі). Покращення комп'ютерної та мережевої продуктивності зачіпають всіх майнерів рівною мірою. З іншого боку, якщо інтервал збільшиться (а він збільшиться, якщо мережа почне виробляти блоки по 2, 4, 8 або 20 мегабайт), майнери почнуть виробляти більше «кинутих блоків», тобто блоків транзакцій, які вже не потрібні, оскільки інший блок, вироблений іншим майнером, вже поширюється по мережі. Таким чином, великі блоки змусять майнерів далі централізуватися, щоб зменшити інтервал, спостерігаючи, як більші майнери діляться знайденим блоком спочатку зі своїми партнерами, а вже потім відсилають його в іншу мережу. Через те, що прийняття «софт» і «хард» форків схвалюється більшістю майнерів шляхом голосування, монополізація майнінг ринку і централізація загрожують самій суті та ідеї блокчейну і біткоїну. Потрібно враховувати, що «Майнери» зацікавлені в підвищенні свого доходу. Зменшення доходу від генерації блоку кожні 210 000 блоків, вимагає від майнерів знаходити нові механізми отримання прибутку. Виходить, що конкуренцію майнерів за генерацію блоку можна розбити на кілька позицій:

– включення в блок найбільш оптимальних транзакцій для максимального прибутку від комісій;

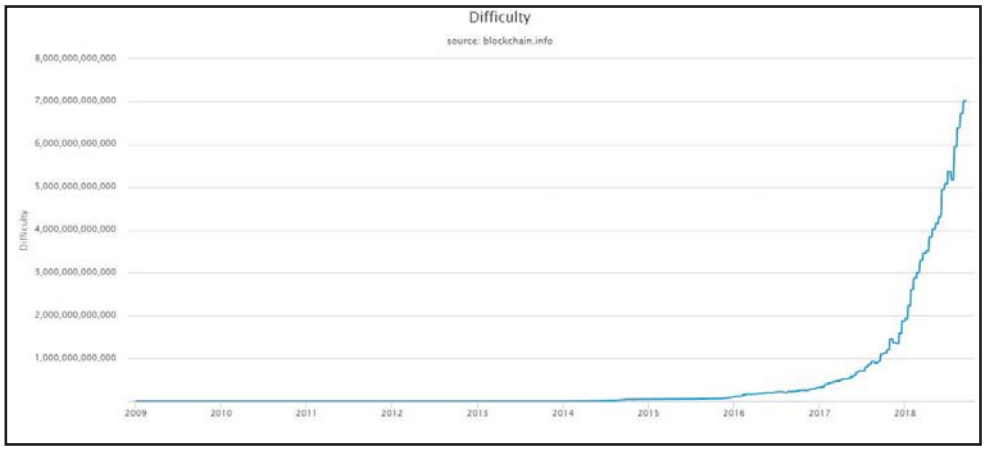
– найбільш швидке знаходження хешу блоку для його генерації.

Можна припустити, що зменшення вдвічі нагороди за блок стимулює майнерів генерувати блоки меншого розміру і штучно створювати умови для зростання комісій. Але також потрібно враховувати той факт, що майнери також намагаються виграти і за рахунок розміру блоку і сукупного розміру комісій. До того ж всім, за умови одночасного знаходження блоку іншим майнером, потрібно врахувати інтервал часу для поширення блоку по мережі, і перевірки його іншими вузлами, що залежить від багатьох факторів.

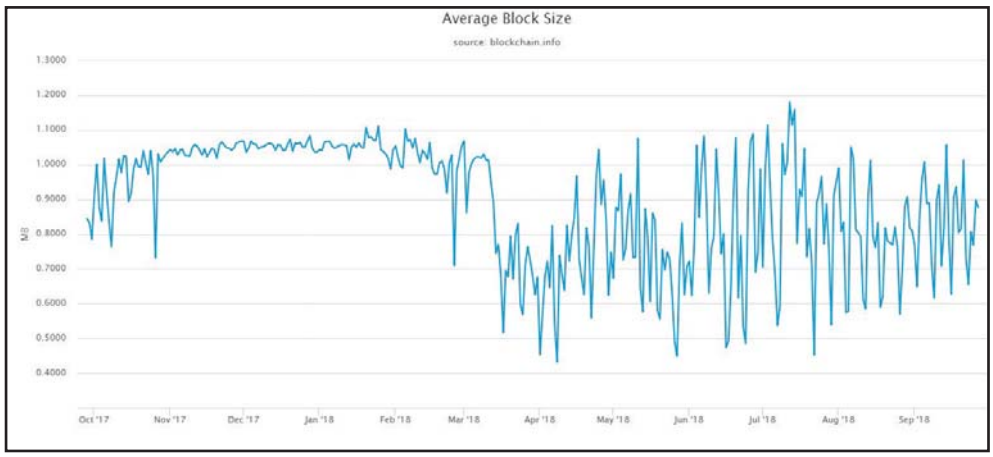


Графік 1. Дохід майнерів за період жов. 2017 р. – вер. 2018 р. [6]

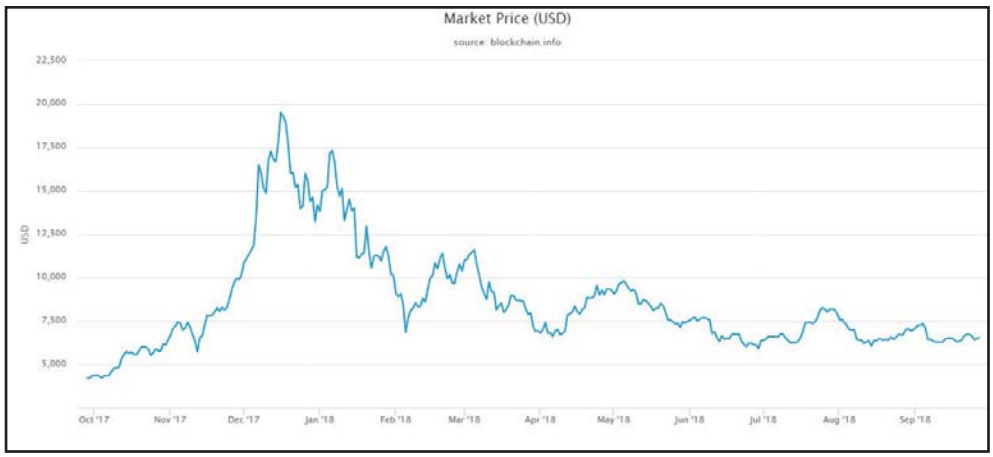
Середній розмір блоку свідчить про кількість транзакцій або про їх сукупну вартість, тому приводити графік кількості транзакцій автор вважає недоцільним.



Графік 2. Середній розмір блоку за період жов. 2017 р. – вер. 2018 р. [7]



Графік 3. Складність генерації блоку за період 2009 р. – 2018 р. [8]



Графік 4. Ринкова ціна BTC в USD за період жов. 2017 р. – вер. 2018 р. [9]

Автор статті виділяє кілька позицій, які є взаємопов'язаними, виходячи з аналізу графіків:

– Дохід майнерів дуже залежить від курсу.

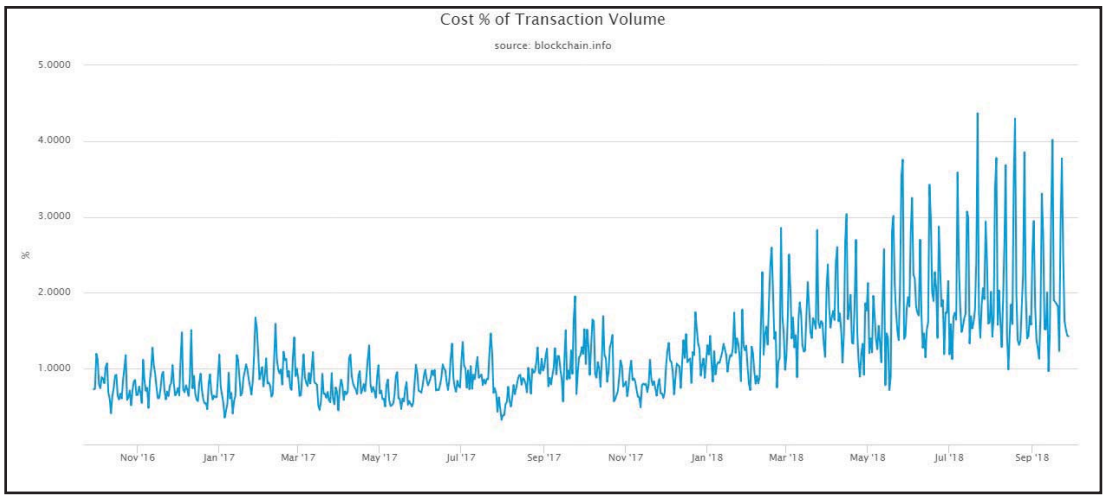
– За період з січня по лютий 2017 величина блоку була більш менш стабільна на тлі високого курсу і навпаки.

– Майнери зацікавлені в зростанні курсу біткоїну у зв'язку зі зменшенням вдвічі нагороди за блок і суттєвим ускладненням видобутку блоку (Графік 3. період з 2017 по 2018 рік).

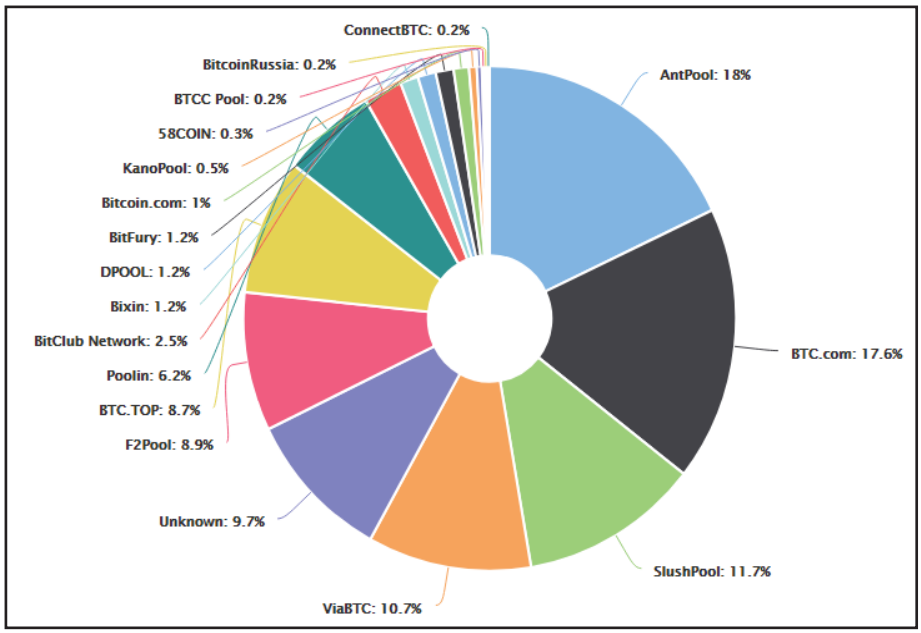
– Централізація майнерів в пули і зменшення їх кількості загрожує стабільності системи і курсу біткоїну, але одночасно з цим неминуче у зв'язку з суттєвим ускладненням видобутку блоку (Графік 3. період з 2017 по 2018 рік).

– Досить стабільний, граничний розмір блоку в момент піку курсу валюти може свідчити про спекулятивний характер транзакцій, оскільки для проведення транзакції в умовах заповнених блоків довелося б платити гранично високі комісії, в чому і зацікавлені майнери.

Подивившись на графік 5 і 6, розташовані нижче показники можна зіставити з показниками графіків 1–4.



Графік 5. Дохід майнерів в % віл об'єму транзакцій за період жов. 2017 р. – вер. 2018 р. [10]



Графік 6. Приблизна оцінка розподілу кількості переборів хешу між основними пулами для майнінгу [11]

Виходячи з розглянутих вище теоретичних припущень автора, наведених графіків і технічних особливостей протоколу blockchain і самого bitcoin, автор статті описує наступні припущення:

– Великий розмір блоку, який ми спостерігали в кінці 2017 року, можливо був результатом високого курсу і навпаки (див. Графік 2).

– З 2017 по 2018 рік складність видобутку блоку збільшилася в 7 разів (див. Графік 3), що може свідчити про підвищення конкуренції у майнерів і збільшення сукупних потужностей.

– Також ми можемо спостерігати збільшення доходу майнерів у відсотках від обсягу транзакції за період жовтен 2017 р. – вересень 2018 р., незважаючи на значне зниження курсу біткоїну (див. Графік 4,5).

– Автор пов'язує велику різницю у величині блоків протягом усього 2018 року з ідентичною стрибкоподібною поведінкою графіка 5, який показує дохід майнерів у відсотках від обсягу транзакції, а також графіку 6, що показує відсоткове співвідношення потужностей головних майнінг пулів. На думку автора, кожен з майнінг пулів веде власну політику створення блоку, маніпулюючи своїми потужностями. Таким чином, можна пояснити, що деякі пули збирають побільше транзакцій в блок, коли інші утискають блок до мінімуму, можливо провокуючи штучне збільшення комісій. Такі блоки, всього лише з 1 транзакцією в блоці, можна побачити у найбільшого майнінг пулу AntPool, наприклад блоки: 543276, 543287, 543301, 543322, 543339, 543341, 543372, 543379, 542381, 543385. Мало того, що ці блоки йдуть підряд з невеликою різницею, так вони ще обробляють 1 транзакцію і отримують нагороду за блок у розмірі 12.5 біткоїну (на момент написання статті це більше 83 000 $).

Автор статті розглядає кілька підходів для підвищення ефективності управління транзакціями для звичайних користувачів, не зменшуючи при цьому доходи майнерів. Lightning Network – це проект в розробці, метою якого є усунення проблеми масштабованості біткойнів шляхом масштабування «поза мережею». Він призначений для забезпечення поновлення стану мікроканалу без використання будь-яких блокувань (в звичайному, не змагальному випадку), що робить мікроплатежі виправданими (і без комісії). Для того щоб скористатися протоколом, користувачам необхідно відкрити платіжний канал, записуючи цю інформацію в блокчейн, і використовувати його у разі потреби для проведення транзакцій. Після чого вони можуть закрити канал і вивести кошти. Тоді в блокчейн записується інформація про закриття каналу, а підсумкова інформація про транзакції йде на підтвердження майнерам. Тобто буде можливо відкривати платіжний канал з лімітованою кількістю монет, які можна буде тільки витрачати. Для отримання монет потрібно буде відкривати інший канал з відправником. По закінченню операцій дані оффчейн транзакцій записуються в справжній блокчейн, який підтвердить їх після 1 000 блоків, і тільки після цього гроші надійдуть на рахунки. До цього моменту це будуть лише записані зобов'язання. Про популярність і адаптацію протоколу свідчить і підтримка серед розробників і криптоспільноти загалом. Дана технологія допоможе популяризувати біткоїни і суттєво збільшити аудиторію користувачів, за допомогою «офф чейн» транзакцій знизити комісії, а також не позичати зайве місце і час в mempool і самому блокчейні [12], оскільки користувачам не доведеться записувати кожну транзакцію в блокчейн, а тільки результат ланцюжка операцій. Автор статті вважає, що Lightning Network буде найбільш ефективним у спільній реалізації з уже діючим Segwit. Також варто звернути увагу, що впровадження SegWit дозволило розробникам Bitcoin Core на початку 2018 року провести дослідження ефективності технології мультипідписів Шнорра [13], як вирішення проблем масштабованості Bitcoin. Згідно з ведучим розробником технології Пітером Велле, дана схема являє собою комбінацію алгоритму підпису і верифікації, коли кілька підписантів, кожен зі своїм власним відкритим і закритим ключем, підписують одне повідомлення. В результаті, замість існуючої схеми генерації індивідуальних підписів до кожної нової транзакції підписанти можуть використовувати всього одну. Цей єдиний підпис може бути верифікований ким завгодно, хто також знає повідомлення і відкриті ключі підписантів. Оскільки дана технологія припускає групування цифрових підписів і ключів, то це зробить транзакції менше, а їх верифікацію швидше, тим самим вирішивши проблеми низької пропускної здатності мережі і високих комісійних зборів. Розглянувши вищезгадані економічні, соціальні та технічні аспекти біткоїну як криптоактиву, автор статті дійшов висновку, що наразі біткоїн дуже залежить від суспільних настроїв і як технічний засіб позбавлений деяких природніх економічних властивостей, але все ще підвладний різним видам економічних та фінансових маніпулювань. Але як open source продукт, який може бути позбавлений всіх потрібних властивостей фіатних валют та технічних недоліків, біткоїн має усі шанси стати дуже практичним і доцільним у щоденному використанні.

ЛІТЕРАТУРА

1. The Three Major Bitcoin Protocols Explained, Investopedia (18 October 2016).
2. Andrew Marshall. Bitcoin Scaling Problem, Explained, The Coin Telegraph (2 March 2017). Проверено 4 июля 2017.
3. Andreas M. Antonopoulos. Mastering Bitcoin. Unlocking Digital Crypto-Currencies. O'Reilly Media, April 2014. ISBN 978-1-4493-7404-4.
4. Козловский С. Биткоин распался на две валюты: как это произошло. Русская служба Би-би-си (1.08.2017).
5. Jordan Pearson. 'Bitcoin Unlimited' Hopes to Save Bitcoin from Itself, Motherboard, Vice Media LLC (14 October 2016).
6. URL: https://www.blockchain.com/ru/charts/miners-revenue.
7. URL: https://www.blockchain.com/ru/charts/blocks-size.
8. URL: https://www.blockchain.com/ru/charts/difficulty.
9. URL: https://www.blockchain.com/ru/charts/market-price.
10. URL: https://www.blockchain.com/ru/charts/cost-per-transaction-percent.
11. URL: https://www.blockchain.com/ru/pools.
12. URL:https://bitcoinmagazine.com/articles/understanding-the-lightning-network-part-building-a-bidirectional-payment-channel-1464710791/.
13. URL: https://blockstream.com/2018/01/23/musig-key-aggregation-schnorr signatures.html.

В.Г. Станиславский. Эффективность управления транзакциями в условиях децентрализации и масштабируемости сети bitcoin. – Статья.

Аннотация. *В статье будут рассмотрены проблемы масштабируемости сети классического блокчейна в условиях увеличения нагрузки на сеть и популяризации технологии при использовании в децентрализованной платежной системе bitcoin. Автор попытается связать экономическую целесообразность, масштабируемость сети и децентрализацию как пути повышения эффективности и гибкости управления транзакциями биткоина.*

Ключевые слова: *bitcoin, blockchain, SegWit, Lightning Network, децентрализация, масштабируемость, управление, транзакции биткоина.*

V. Stanislavskyi. Management efficiency of transactions in conditions of decentralization and scalability of the bitcoin network. – Article.

Summary. *The article will consider the problems of the scalability of the classical blockchain network in conditions of increasing the network capacity and popularizing the technology in a decentralized payment system of bitcoin. The author will try to link economic expediency, network scalability and decentralization as ways to increase the efficiency and flexibility of managing Bitcoin transactions.*

Key words: *bitcoin, blockchain, SegWit, Lightning Network, decentralization, scalability, management, bitcoin transactions.*