Інформаційні технології

УДК 004.852

Сидоренко Захар Андрійович

бакалавр комп'ютерних наук

Національного технічного університету України

«Київський політехнічний інститут імені Ігоря Сікорського»

Сидоренко Захар Андреевич

бакалавр компьютерных наук

Национального технического университета Украины

«Киевский политехнический институт имени Игоря Сикорского»

Sydorenko Zakhar

bachelor of computer science of

The National Technical University of Ukraine

«Kyiv Polytechnic Institute»

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ BLOCKCHAIN

ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ BLOCKCHAIN

STUDY OF BLOCKCHAIN TECHNOLOGY

Анотація: Проведено аналіз основних плюсів та мінусів технології, а також досліджено основні принципи її побудови.

Ключові слова: Blockchain, блок, ланцюжок блоків, хеш.

Аннотация: Проведен анализ основных плюсов и минусов технологии, а также исследованы основные принципы ее построения.

Ключевые слова: Blockchain, блок, цепочка блоков, хэш.

Annotation: The analysis of the main advantages and disadvantages of technology has been carried out, and the basic principles of its construction have been investigated.

Keywords: Blockchain, block, hash.

Blockchain - це принципово нова надійна технологія зберігання записів, яка може кардинально змінити підхід до формування і зберігання баз даних.

Технологія Blockchain має величезний потенціал з точки зору спрощення та підвищення ефективності за рахунок створення принципово нової інфраструктури фінансових сервісів. Ця технологія може успішно використовуватися банками для проведення внутрішніх взаєморозрахунків і здійснення міжбанківських операцій, а також при проведенні мікроплатежів між фізичними особами [1].

При цьому вона може значно спростити відстеження підозрілих транзакцій і в цілому підвищити прозорість угод. По суті це технологія розподіленого підтвердження транзакцій, яка представляє собою величезну розподілену базу даних [2]. При цьому перевіркою достовірності транзакцій займаються самі учасники, вони ж підтверджують їх коректність та формують нові блоки.

Такий підхід цікавий перш за все тим, що із його використанням відпадає необхідність у посередниках, що здійснюють обробку транзакцій і, як наслідок, підвищується швидкість обробки операцій і знижується вартість для кінцевого споживача [3].

За деякими оцінками, використання Blockchain дозволить банкам заощаджувати близько 20 мільярдів доларів за рахунок відмови від послуг посередників при здійсненні транзакцій. Blockchain може стати реальною альтернативою системі SWIFT, яка на даний момент є не дуже гнучкою і досить дорогою.

Але перехід на нову технологію займає деякий час. На це є кілька причин і перш за все - невизначеність у правовій та регуляторній області.

Крім того, широкомасштабне впровадження цієї технології передбачає значних змін в області стандартизації.

Blockchain - це технологія, яка набрала популярності завдяки її використанню при побудові криптовалюти Bitcoin (Рис 1.1).

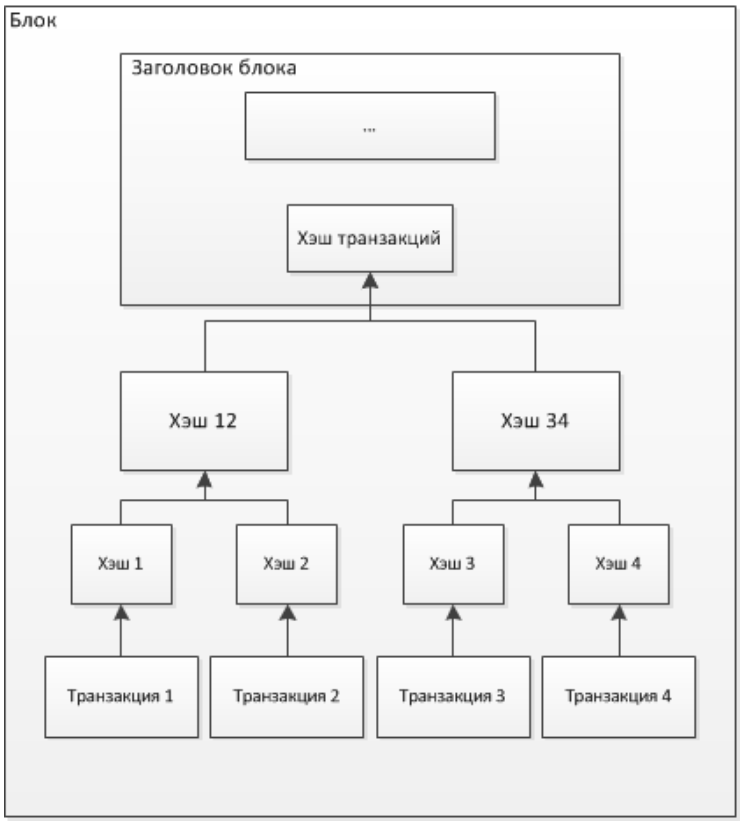

Рис 1 – Схема отримання хешу транзакцій [10]

Основа технології blockchain - в розподіленому зберіганні інформації. Це дозволяє зберігати важливу інформацію одночасно на багатьох серверах (у всіх учасників мережі), при цьому зберігати відкрито і безпечно [1]. Наприклад, на базі цієї технології можна зберігати як історію банківських транзакцій клієнтів, так і базу контрактів, результати голосувань, відбитків пальців або історій хвороб. Інформацію, яка одночасно зберігається у багатьох місцях неможливо підробити, неможливо вкрасти, тому що оригінальні записи відразу можуть бути відновлені з сусідніх джерел.

Блок транзакцій - спеціальна структура для запису групи транзакцій в системі біткоін і аналогічних їй.

Щоб транзакція вважалася достовірною («підтвердженої»), її формат і підписи повинні перевірити, а потім групу транзакцій записати в спеціальну структуру - блок. Інформацію в блоках можна швидко перевірити ще раз. Кожен блок завжди містить інформацію про попередній блок. Усі блоки можна вишикувати в один ланцюжок, який містить інформацію про всі операції в цій базі. Найперший блок в ланцюжку - первинний блок (англ. Genesis block) - розглядається як окремий випадок, оскільки у нього відсутній батьківський блок.

Блок складається із заголовка і списку транзакцій. Початок блоку включає в себе свій хеш, хеш попереднього блоку, хеші транзакцій і додаткову службову інформацію. В біткоін системі першою транзакцією в блоці завжди вказується отримання комісії, яка стане нагородою користувачеві за створений блок [4].

Далі йдуть всі або деякі з останніх транзакцій, які ще не були записані в попередні блоки. Для транзакцій в блоці використовується деревоподібне хешування, аналогічне формування хеш-суми для файлу в протоколі BitTorrent. Транзакції, крім нарахування комісії за створення блоку, містять всередині атрибуту input посилання на транзакцію з попереднім станом даних (в системі біткойнів, наприклад, дається посилання на ту транзакцію, за якою були отримані біткоіни, які зараз витрачаються). Комісійні транзакції можуть містити в атрибуті будь-яку інформацію (для них це поле зветься англ. Coinbase parameter), оскільки у них немає батьківських транзакцій [5].

Створений блок буде прийнятий іншими користувачами, якщо числове значення хешу заголовка дорівнює або нижче певного числа, величина якого періодично коригується. Так як результат хешування (функції SHA-256) є незворотним, немає алгоритму отримання бажаного

результату, крім випадкового перебору. Якщо хеш не задовольняє умові, то в заголовку змінюється параметр nonce і хеш перераховується. Зазвичай потрібна велика кількість перерахунків. Коли правильний варіант знайдений, вузол розсилає отриманий блок іншим підключеним користувачам, які перевіряють блок. Якщо помилок немає, то блок вважається доданим в ланцюжок і наступний блок повинен включити в себе його хеш.

Величина цільового числа, з яким порівнюється хеш, в системі біткоінів коригується через кожні 2016 блоків. Заплановано, що вся мережа системи біткоінів повинна витрачати на генерацію одного блоку приблизно 10 хвилин, на 2016 блоків - близько двох тижнів. Якщо 2016 блоків сформовані швидше, то шуканий параметр трохи зменшується і досягти його стає важче, в іншому випадку він збільшується. Зміна складності обчислень не впливає на надійність мережі і потрібна лише для того, щоб система генерувала блоки майже з постійною швидкістю, яка не залежить від обчислювальної потужності учасників мережі [6].

Блоки одночасно формуються безліччю майнерів. Блоки, які задовольняють критерії, відправляються в мережу, включаючись в розподілену базу блоків. Постійно виникають ситуації, коли кілька нових блоків в різних частинах розподіленої мережі вказують на один і той самий попередній блок, тобто ланцюжок блоків може розмежовуватися. У цьому випадку можливе паралельне нарощування різних гілок. Спеціально або випадково можна обмежити трансляцію інформації про нові блоки (наприклад, один із ланцюгів може розвиватися в межах локальної мережі). В цьому випадку можливе одночасне паралельне нарощування різних гілок. У кожному з нових блоків можуть зустрічатися як однакові транзакції, так і різні, що увійшли тільки в один з них. Коли ретрансляція блоків відновлюється, майнери починають вважати головний ланцюжок той у якого найбільший рівень складності хешу і найбільша довжина. У разі

рівного розподілу складності і довжини перевага віддається тому ланцюжку, кінцевий блок якого з'явився раніше [7]. Транзакції, що увійшли тільки у відхилену гілку (в тому числі по виплаті винагороди), втрачають статус підтверджених. Якщо це транзакція з передачі біткоінів, то вона буде поставлена в чергу, а потім включена в черговий блок. Транзакції отримання винагороди за створення відсічених блоків не дублюються в іншій гілці, тобто «зайві» біткоіни, виплачені за формування відсічених блоків, не отримують подальших підтверджень і «втрачаються».

Таким чином, ланцюжок блоків містить історію володіння, з якою можна ознайомитися, наприклад, на спеціалізованих сайтах.

Розподілена база даних Blockchain формується як безперервно зростаючий ланцюжок блоків із записами про всі транзакції. Копія бази або її частини одночасно зберігається на безлічі комп'ютерів і синхронізуються відповідно до формальних правил побудови ланцюжка блоків. Інформація в блок не шифрується і доступна у відкритому вигляді, але захищена від змін криптографічно через хеш-ланцюжок [8].

База публічно зберігає в незашифрованому вигляді інформацію про всі транзакції, що підписуються за допомогою асиметричного шифрування. Для запобігання багаторазової витрати однієї і тієї ж суми використовуються мітки часу, реалізовані шляхом розбиття БД на ланцюжок спеціальних блоків, кожен з яких, в числі іншого, містить в собі хеш попереднього блоку і свій порядковий номер. Кожен новий блок здійснює підтвердження транзакцій, інформацію про яких містить і додаткове підтвердження транзакцій у всіх попередніх блоках ланцюжка. Змінювати інформацію в блоці, який вже знаходиться в ланцюзі, не можливо, так як в такому випадку довелося б редагувати інформацію в усіх наступних блоках. Завдяки цьому успішна double-spending атака (повторна трата раніше витрачених коштів) на практиці вкрай малоймовірна [9].

Найчастіше навмисна зміна інформації в будь-яку з копій бази або навіть в досить великій кількості копій не буде визнана істинною, тому що не буде відповідати правилам. Деякі зміни можуть бути прийняті, якщо будуть внесені в усі копії бази (наприклад, видалення декількох останніх блоків через помилки в їх формуванні).

Для більш наочного пояснення механізму роботи платіжної системи Сатоси Накамото ввів поняття «цифрова монета», визначивши його як ланцюжок цифрових підписів. На відміну від стандартизованих номіналів звичайних монет, кожна «цифрова монета» має свій власний номінал. Кожній біткойн-адресі може зіставлятися будь-яка кількість «цифрових монет». За допомогою транзакцій їх можна ділити й об'єднувати, при цьому зберігається загальна сума їх номіналів за вирахуванням комісії [10].

Дані поділяються на маленькі частини - блоки, які індивідуально хешуються за допомогою Leaf Tiger Hash, потім з кожної пари хешів черзі обчислюється Internal Tiger Hash. Якщо хешу немає пари, то він переноситься в нову ланцюжок без змін. Далі в ланцюжку для кожної пари знову обчислюється Internal Tiger Hash. Ця процедура повторюється до тих пір, поки не залишиться один хеш. Цей єдиний хеш, що залишився після Internal Tiger Hash називають Tiger Tree Root. Саме його використовують для однозначної ідентифікації файлу і вказують в різних P2P посиланнях.

У цій статті було проведено загальний огляд, що таке технологія Blockchain. Також було визначено основні компоненти технології, наведено сфери її застосування.

Проведено аналіз алгоритмів, які використовуються для отримання хешів нових блоків. В результаті дослідження було виявлено, що технологія Blockchain також може використовуватися при створенні платформи для смарт-контрактів. Нагадаємо, що смарт-контракт – це електронний алгоритм, що описує набір умов, виконання яких тягне за собою деякі події в реальному світі або цифрових системах. Для реалізації розумних

контрактів потрібне децентралізоване середовище, яке повністю виключає людський фактор, а для можливості використання в розумному контракті передачі вартості необхідна криптовалюта (наприклад Bitcoin).

Література:

1. Antonopoulos Andreas Mastering Bitcoin: Unlocking Digital Cryptocurrencies / Antonopoulos Andreas – K. : NGITS, 2014. – C. 150 – 290
2. Tapscott Don, Tapscott Alex Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World / Tapscott Don, Tapscott Alex – K. : Information Systems, 2016 – C. 100 – 150.
3. Vigna Paul, Casey Michael The Age of Cryptocurrency: How Bitcoin and the Blockchain Are Challenging the Global Economic Order / Vigna Paul, Casey Michael – K. : Economic, 2015 – C. 200 – 210.
4. Skinner Chris Value Web / Skinner Chris – K. : Information technologies, 2016 – C. 150 – 175.
5. Wattenhofer Roger The Science of the Blockchain / Wattenhofer Roger – K. : Information technologies, 2016 – C. 94 – 120.
6. Duggal Pavan Blockchain Contracts and Cyberlaw / Duggal Pavan – K. : Information Systems, 2015 – C. 15 – 39.
7. William Jacob Blockchain: The Simple Guide To Everything You Need To Know / William Jacob – K. : Information technologies, 2016 – C. 40 – 50.
8. Harris Tim Bitcoin: Mastering Bitcoin & Cyptocurrency for Beginners — Bitcoin Basics, Bitcoin Stories, Dogecoin, Reinventing Money & Other Digital Currencies / Harris Tim – K. : Economic, 2016 – C. 30 – 47.
9. Sammons Eric Bitcoin Basics: 101 Questions and Answers / Sammons Eric – K. : Information Systems, 2015 – C. 93 – 100.
10. Boyen Xavier, Carr Christopher, Haines Thomas – Blockchain-Free Cryptocurrencies. A Rational Framework for Truly Decentralised Fast

Transactions / Boyen Xavier, Carr Christopher, Haines Thomas K. : Information Systems, 2015 – C. 45 – 90.