УДК 336.743
DOI: 10.31673/2409-7292.2020.032228

Костюк П.П.

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Технологія блокчейн стає однією із головних рушійних сил інновацій в глобальній економіці. Її впровадження матиме величезний вплив на те як діють підприємства та уряди і на те як люди організовують своє повсякденне життя. Індустрія фінансових послуг на даний момент зазнає найбільшого впливу блокчейн-революції, а фінансові інституції є одними з найперших користувачів технології. У той же час, сфера морських перевезень, як доволі традиційна індустрія, поки що не має багато прикладів застосування блокчейну, але ця технологія здатна суттєво змінити цю галузь.

Ключові слова: захист персональних даних, блокчейн, блокчейн-технології як захист інформації.

Вступ

Якщо ви стежили за банківською діяльністю, інвестуванням або криптовалютою протягом останніх десяти років, ви можете бути знайомі з «blockchain», технологією ведення рекорду за bitcoin. І є хороший шанс, що він має лише такий сенс. Намагаючись дізнатися більше про блокчейн, ви, мабуть, зіткнулися з таким визначенням: «blockchain - це розподілена, децентралізована, громадська книга».

Що таке Blockchain? Якщо ця технологія настільки складна, чому її називають «блокчейн»? На самому базовому рівні блокчейн буквально є лише ланцюжком блоків, але не в традиційному розумінні цих слів. Коли ми говоримо в цьому контексті слова «блок» і «ланцюжок», ми фактично говоримо про цифрову інформацію («блок»), що зберігається в публічній базі даних («ланцюжок»).

«Блоки» на блок-ланцюзі складаються з цифрової інформації. Зокрема, вони складаються з трьох частин:

1. Блоки зберігають інформацію про транзакції, скажімо дату, час і суму долара вашої останньої покупки від Amazon.
2. Блоки зберігають інформацію про те, хто бере участь у транзакціях. Блок для вашої покупки з компанією Amazon запише Ваше ім'я разом з Amazon.com, Inc.
3. Блоки зберігають інформацію, що відрізняє їх від інших блоків. Як і ви, і я маю імена, щоб відрізняти нас один від одного, кожен блок зберігає унікальний код, який називається «хеш», що дозволяє нам розрізняти його від кожного іншого блоку.

Скажімо, ви зробили свою покупку на Amazon, але в той час, як це відбувається, ви вирішите, що ви просто не можете протистояти і вам потрібен другий. Навіть якщо деталі нової транзакції виглядають майже ідентично вашій попередній покупці, ми все одно можемо розрізняти блоки через їх унікальні коди.

Хоча блок у наведеному вище прикладі використовується для зберігання однієї покупки з Amazon, реальність дещо інша. Один блок на блокчейн може фактично зберігати до 1 Мб даних. Залежно від розміру операцій, це означає, що один блок може розмістити кілька тисяч угод під одним дахом.

Аналіз останніх досліджень і публікацій

Компанія IBM провела дослідження технології «блокчейн», та опублікувала певні недоліки даної технології [1].

Незважаючи на значні погіршення ситуації з блокчейн, існують також значні труднощі з її прийняттям. Перешкоди до застосування технології blockchain сьогодні не просто технічні. Реальні виклики полягають у політичній та регуляторній, здебільшого, не кажучи вже про тисячі годин (читання: гроші) про індивідуальне проектування програмного забезпечення та зворотному програмуванні, необхідному для інтеграції blockchain до поточних бізнес-мереж. Ось деякі з проблем, що стоять на шляху широкого поширення блокчейн:

Вартість

Хоча блокчейн може заощадити користувачам гроші на транзакційних зборах, технологія далека від безкоштовної. Наприклад, система «докази роботи», яку використовує Bitcoin для перевірки транзакцій, споживає великі обсяги обчислювальної потужності. У реальному світі влада від мільйонів комп'ютерів у мережі Bitcoin близька до того, що споживає Данія щорічно. Вся ця енергія коштує грошей, і згідно з недавнім дослідженням дослідницької компанії Elite Fixtures, вартість видобутку одного біткоїну різко змінюється за місцем розташування - від $ 531 до приголомшливих $ 26,170. Виходячи зі середніх витрат на комунальні послуги в США, цей показник ближче до $ 4 758. Незважаючи на витрати на видобуток біткоїну, користувачі продовжують збільшувати свої рахунки за електроенергію для перевірки операцій на блокчейн. Це відбувається тому, що, коли шахтарі додають блок для блочного ланцюга Bitcoin, вони отримують достатню кількість біткоїну, щоб зробити свій час і енергію корисними. Однак, коли мова йде про блокхенах, які не використовують криптовалюту, шахтарі потрібно буде платити або іншим чином стимулювати перевірку транзакцій [2].

Неефективність

Bitcoin - ідеальний приклад для можливої неефективності blockchain. Система «підтвердження роботи» Bitcoin займає близько десяти хвилин, щоб додати новий блок в блокчейн. За такої швидкості, за оцінками, мережа blockchain може керувати лише 7 транзакціями в секунду (TPS). Хоча інші криптовалюти, такі як Ethereum (20 TPS) і Bitcoin Cash (60 TPS) працюють краще, ніж Bitcoin, вони все ще обмежені blockchain. Спадковий бренд Visa, для контексту, може обробляти 24000 TPS.

Конфіденційність

Хоча конфіденційність у мережі blockchain захищає користувачів від хакі та зберігає конфіденційність, вона також дозволяє незаконну торгівлю та діяльність на мережі blockchain. Найбільш цитованим прикладом блокейна, що використовується для незаконних операцій, є, мабуть, Шовковий шлях, онлайн-ринок “темних веб-сайтів”, що діє з лютого 2011 року до жовтня 2013 року, коли його було закрито ФБР. Веб-сайт дозволив користувачам переглядати веб-сайт, не відслідковуючись і здійснюючи незаконні покупки в біткоїнах. Поточне регулювання в США забороняє користувачам онлайн-обмінів, як, наприклад, тих, які побудовані на блокчейн, повністю анонімність. У Сполучених Штатах Інтернет-біржі повинні отримувати інформацію про своїх клієнтів, коли вони відкривають рахунок, перевіряють ідентичність кожного клієнта і підтверджують, що клієнти не з'являються в жодному списку відомих або підозрюваних терористичних організацій [3].

Безпека

Кілька центральних банків, включаючи Федеральний резерв, Банк Канади та Банк Англії, розпочали розслідування цифрових валют. Згідно з звітом Банку Англії за лютий 2015 р., «Подальші дослідження також потребуватимуть розробки системи, яка могла б використовувати розподілену головну технологію, не порушуючи здатності центрального банку контролювати свою валюту і захищати систему від системного нападу».

Сприйнятливість

Нові криптовалюти та мережі блочного ланцюга піддаються атакам на 51%. Ці напади надзвичайно важко виконати через обчислювальну потужність, необхідну для того, щоб отримати контроль над мережею блокчейн, але дослідник інформатики Нью-Йорка Джозеф Бонно сказав, що це може змінитися. У минулому році Бонно опублікував звіт про те, що 51% атак, швидше за все, збільшиться, оскільки зараз хакери можуть просто орендувати обчислювальну потужність, а не купувати все обладнання.

Постановка проблеми.

2017 рік став переломним для технології блокчейн і біткоін. Спираючись на суху статистику, можна сказати, що динаміка зростання ціни на валюту за рік зросла у понад 10 разів. Грунтуючись на даних сайту Coinspot, можна побачити, що світова спільнота готова до переходу на нову сходинку валютних операцій в інтернеті.

Проте за умов широкого використання новітніх технологій, основною проблемою пересічних користувачів інтернету залишається неосвіченість у цьому питанні, а також недовіра до технології.

Блокчейн впроваджується не лише в економічному руслі, а й може стати плацдармом для формування «розумних» контрактів у будь-якій сфері діяльності. Як і всі технології, блокчейн не є досконалою на 100%, тому на неї можуть здійснюватися атаки, про які повинні знати користувачі.

Основна частина.

На самому базовому рівні блокчейн буквально є лише ланцюжком блоків, але не в традиційному розумінні цих слів. Коли ми говоримо в цьому контексті слова «блок» і «ланцюжок», ми фактично говоримо про цифрову інформацію («блок»), що зберігається в публічній базі даних («ланцюжок»). «Блоки» на блок-ланцюзі складаються з цифрової інформації. Зокрема, вони складаються з трьох частин:

1. Блоки зберігають інформацію про транзакції, скажімо дату, час і суму долара вашої останньої покупки від Amazon.
2. Блоки зберігають інформацію про те, хто бере участь у транзакціях. Блок для вашої покупки з компанією Amazon запише Ваше ім'я разом з Amazon.com, Inc.
3. Блоки зберігають інформацію, що відрізняє їх від інших блоків. Як і ви, і я маю імена, щоб відрізняти нас один від одного, кожен блок зберігає унікальний код, який називається «хеш», що дозволяє нам розрізняти його від кожного іншого блоку.

Скажімо, ви зробили свою покупку на Amazon, але в той час, як це відбувається, ви вирішите, що ви просто не можете протистояти і вам потрібен другий. Навіть якщо деталі нової транзакції виглядають майже ідентично вашій попередній покупці, ми все одно можемо розрізняти блоки через їх унікальні коди.

Хоча блок у наведеному вище прикладі використовується для зберігання однієї покупки з Amazon, реальність дещо інша. Один блок на блокчейн може фактично зберігати до 1 Мб даних. Залежно від розміру операцій, це означає, що один блок може розмістити кілька тисяч угод під одним дахом [4].

Коли блок зберігає нові дані, він додається до блокчейна. Blockchain, як випливає з назви, складається з декількох блоків, зв'язаних разом. Для того, щоб блок був доданий до blockchain, однак, чотири речі повинні відбутися:

1. Необхідно здійснити транзакцію. Давайте продовжимо приклад вашої привабливої покупки Amazon. Після поспішного натискання декількох підказок, ви йдете проти свого кращого судження і зробіть покупку.
2. Ця транзакція повинна бути перевірена. Після здійснення цієї покупки необхідно підтвердити транзакцію. З іншими публічними записами інформації, такими як Комісія з цінних паперів, Вікіпедія або Ваша місцева бібліотека, хтось відповідає за перевірку нових записів даних. Проте, за допомогою блокчейна ця робота залишається до мережі комп'ютерів. Ці мережі часто складаються з тисяч (або у випадку Bitcoin, близько 5 мільйонів) комп'ютерів, поширених по всьому світу. Коли ви робите покупку від Amazon, ця мережа комп'ютерів поспішає перевірити, що ваша транзакція відбулася так, як ви сказали. Тобто, вони підтверджують деталі покупки, включаючи час угоди, суму долара та учасників. (Докладніше про те, як це відбувається за секунду.)
3. Ця транзакція повинна зберігатися в блоці. Після того, як ваша транзакція перевірена як точна, вона отримує зелене світло. Сума долара транзакції, цифровий підпис і цифровий підпис Amazon зберігаються в блоці. Там транзакція, швидше за все, приєднається до сотень, чи тисяч інших.
4. Цей блок повинен мати хеш. Не на відміну від ангела, який отримує свої крила, як тільки всі транзакції блоку були перевірені, йому слід надати унікальний ідентифікаційний код, який називається хешем. Блоку також дається хеш останнього блоку, доданого до блокчейна. Після того як хеш, блок може бути доданий до blockchain.

Коли цей новий блок буде додано до блокчейна, він стане загальнодоступним для всіх, хто бажає його переглянути - навіть ви. Якщо ви подивитеся на блокчейн Bitcoin, ви побачите, що у вас є доступ до даних транзакцій, разом з інформацією про те, коли ("Час"), де ("Висота"), і хто ("Пересланий") блок додано в блокчейн.

Чи є Blockchain приватним?

Будь-хто може переглядати вміст блочного ланцюга, але користувачі також можуть підключати свої комп'ютери до мережі blockchain. При цьому їх комп'ютер отримує копію блокчейна, яка автоматично оновлюється, коли додається новий блок, подібно до Facebook News Feed, який оновлюється при кожному новому статусі.

Кожен комп'ютер в мережі blockchain має свою власну копію блокчейна, що означає, що є тисячі, або у випадку Bitcoin, мільйони копій того ж блокчейна. Хоча кожна копія блокчейна ідентична, поширення цієї інформації по мережі комп'ютерів ускладнює маніпулювання інформацією. За допомогою blockchain немає єдиного, остаточного розрахунку подій, якими можна керувати. Натомість хакеру потрібно було б маніпулювати кожною копією блочного ланцюга в мережі.

Проглядаючи блоккейн Bitcoin, однак, ви помітите, що у вас немає доступу до інформації про користувачів, які здійснюють транзакції. Хоча транзакції на blockchain не є повністю анонімними, особиста інформація про користувачів обмежується їх цифровим підписом або ім'ям користувача.

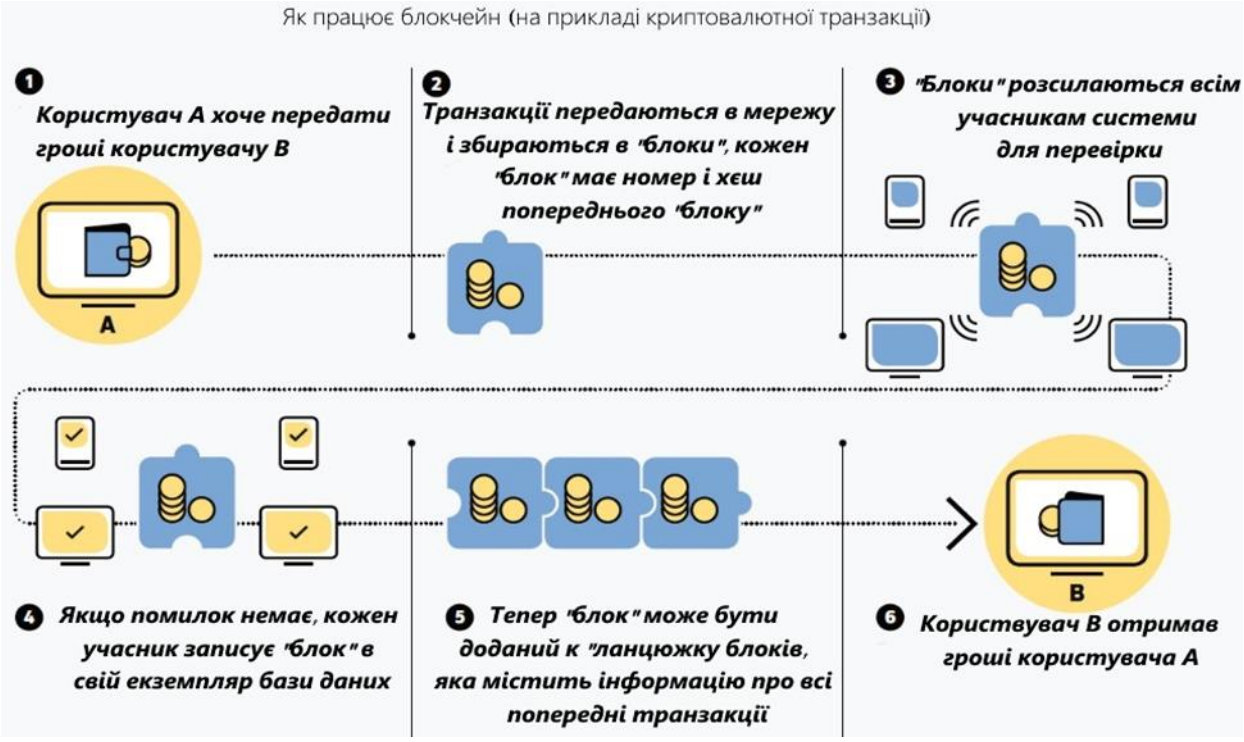

Рис. 1. Схема транзакцій за участі технології блокчейн

Розрахунки та практичні рекомендації:

Зараз розглянемо простий випадок - біткойн-адреса, що представляє відкритий ключ, за яким він згенерований. Біткойн-адреса генерується на основі відкритого ключа з використанням односторонньої функції криптографічного хешування. Алгоритм хешування, або просто хеш-алгоритм (hash algorithm), являє собою односторонню (односпрямовану) функцію, яка обчислює цифровий відбиток (fingerprint) або хеш-значення (hash) вхідних даних довільного розміру. Криптографічні хеш-функції активно використовуються в біткойнсістеме: в біткойн-адресах, в адресах скриптів і в процесі Майнінг за алгоритмом докази виконання роботи (Proof-of-Work). До алгоритмів, що застосовуються для генерації біткойн-адреси по відкритому ключу, відносяться Secure Hash Algorithm (SHA) і RACE

Integrity Primitives Evaluation Message Digest (RIPEMD), зокрема версії SHA256 і RIPEMD160. Маючи відкритий ключ К, ми обчислюємо хеш-значення за алгоритмом SHA256, а до отриманого результату застосовуємо алгоритм RIPEMD160, отримуючи в результаті 160-бітове (20-байтовое) число:

A = RIPEMD160 (SHA256 (K)),

де,
К - відкритий ключ,
А - обчислюється біткойн-адреса.

Біткойн-адреси майже завжди кодуються в форматі, який використовує 58 символів (система числення Base59) і контрольну суму для підвищення зручності читання людиною, для усунення неоднозначності і для захисту від помилок у записі адреси і його введення. Крім того, формат Base58Check використовується багатьма іншими способами в біткойн-системі, там, де необхідно, щоб користувач без труднощів прочитав і правильно записав числове значення, наприклад біткойн-адреса, секретний ключ, зашифрований ключ або хеш скрипта. У наступному розділі ми докладно розглянемо механізм кодування і декодування Base58Check, а також представлення результатів його роботи.

Транзакції - що всередині Насправді внутрішній вміст транзакції значно відрізняється від візуального представлення транзакції, сформованого типовим провідником по блокам. Фактично більшість конструкцій високого рівня, які ми спостерігаємо в різних версіях призначеного для користувача інтерфейсу біткойн-додатків, насправді не існує в біткойн-системі. Ми можемо скористатися інтерфейсом командного рядка Bitcoin Core (getrawtransacti.on і decoderawtransacti.on) для вилучення транзакції Аліси в сьогоденні, «сирому» вигляді, декодувати її і подивитися, що вона містить.

Результат буде таким:

{
"versi.on": 1, "lockti.l'le": 0, "vin11 : [{ "txi.d": "7957a35fe64f80d234d76d83a2a8fla0d8149a41d81de548f0a65a8a999f6f18", "vout": 0, "scri.ptSi.g" : "3045022100884d142d86652a3f47ba4746ec719bbfbd040a570bldeccbb6498c75c4ae24cb02204 b9f039ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813[ALL] 0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789dl 72787ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf", "sequence" : 4294967295
], "vout":"value": 0.01500000, "scri.ptPubKey": "OP _OUP OP _HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG" }, { "value": 0.08450000, "scri.ptPubKey": "OP_DUP OP_HASH160 7f9Ыa7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG", }]
}

Захищеність Blockchain

Технологія Blockchain пояснює питання безпеки і довіри кількома способами. По-перше, нові блоки завжди зберігаються лінійно і хронологічно. Тобто, вони завжди додаються до «кінця» блокчейна. Якщо ви подивитеся на блокчейн Bitcoin, ви побачите, що кожен блок має позицію на ланцюжку, що називається «висотою». Станом на лютий 2020, висота блоку перевищила 562,000.

Після того, як блок був доданий до кінця блокчейна, дуже важко повернутися і змінити вміст блоку. Це тому, що кожен блок містить свій власний хеш, а також хеш блоку перед ним. Хеш-коди створюються математичною функцією, яка перетворює цифрову інформацію в рядок чисел і букв. Якщо ця інформація редагується будь-яким чином, змінюється також хеш-код.

Ось чому це важливо для безпеки. Скажімо, хакери намагаються відредагувати вашу транзакцію від Amazon, так що вам доведеться платити за покупку двічі. Як тільки вони змінять суму долара вашої транзакції, хеш блоку буде змінено. Наступний блок у ланцюзі все ще буде містити старий хеш, і хакеру потрібно буде оновити цей блок, щоб покрити свої доріжки. Однак, це може змінити хеш блоку. І наступний, і так далі.

Для того, щоб змінити один блок, то хакеру потрібно буде змінити кожний блок після нього на блокчейн. Перерахування всіх цих хешей потребує величезної та неймовірної кількості обчислювальної потужності. Іншими словами, після додавання блоку в блокчейн дуже важко редагувати і неможливо видалити.

Для вирішення питання про довіру, мережі blockchain реалізували тести для комп'ютерів, які хочуть приєднатися і додати блоки до ланцюга. Тести, які називаються «моделями консенсусу», вимагають, щоб користувачі «доводили» себе, перш ніж вони могли брати участь у мережі blockchain. Один з найпоширеніших прикладів, використаних Bitcoin, називається «доказом роботи».

У системі доказування роботи комп'ютери повинні «довести», що вони зробили «роботу», вирішуючи складну обчислювальну математичну задачу. Якщо комп'ютер вирішує одну з цих проблем, вони мають право додати блок в блокчейн. Але процес додавання блоків в блокчейн, що криптовалютний світ називає «видобуванням», нелегкий.

Доказ роботи не робить неможливими атаки хакерів, але це робить їх непридатними. Якщо хакер хотів координувати атаку на блокчейн, їм потрібно було б вирішувати складні обчислювальні математичні завдання на рівні 1 в 5,8 трлн. Витрати на організацію такого нападу майже напевно перевищуватимуть переваги.

Мета blockchain полягає в тому, щоб дозволити записати та розповсюдити цифрову інформацію, але не редагувати. Ця концепція може бути важкою для того, щоб обернути голову навколо, не бачачи технології в дії, так що давайте подивимося, як найперша застосування технології blockchain дійсно працює.

Технологія Blockchain була вперше викладена в 1991 році Стюартом Хабером і В. Скотнеттом, двома дослідниками, які хотіли впровадити систему, в якій мітки документів не могли бути змінені. Але майже два десятиліття по тому, з запуском Bitcoin у січні 2009 року, блокчейн мав своє перше реальне застосування.

Протокол Bitcoin побудований на блокчейн. У дослідницькій роботі, що представляє цифрову валюту, творець псевдонімів Bitcoin, Сатоші Накамото, назвав його «новою електронною грошовою системою, що є повністю рівноправною, без довірених третіх осіб».

Ось як це працює. У вас є всі ці люди, у всьому світі, які мають Bitcoin. За даними дослідження, проведеного Кембриджським центром альтернативних фінансів на 2017 рік, їх кількість може становити 5,9 млн. Чоловік. Скажімо, один з тих 5,9 мільйонів людей хоче витратити свій Bitcoin на продукти. Тут приходить блокчейн. Коли справа доходить до друкованих грошей, використання друкованої валюти регулюється та перевіряється центральним органом, як правило, банком або урядом, - але Bitcoin не контролюється ніким. Натомість транзакції, зроблені в Bitcoin, перевіряються мережею комп'ютерів.

Коли одна людина платить іншу за товари, що використовують Bitcoin, комп'ютери на ралі мережі Bitcoin для перевірки транзакції. Щоб зробити це, користувачі запускають програму на своїх комп'ютерах і намагаються вирішити складну математичну задачу, яку називають «хешем». Коли комп'ютер вирішує проблему «хешуванням» блоку, його алгоритмічна робота також перевірить блок транзакцій. Завершена транзакція публічно реєструється і зберігається як блок на блокчейн, після чого вона стає незмінною. У випадку з Bitcoin, і більшість інших блокчейн, комп'ютери, які успішно перевіряють блоки, винагороджуються за свою роботу за допомогою криптовалют. (Докладніше пояснення верифікації див. У розділі Що таке Bitcoin Mining?)

Хоча транзакції публічно записані на блокчейн, дані користувача не є або, принаймні, не повністю. Для проведення транзакцій у мережі Bitcoin учасники повинні запускати програму, яка називається «гаманцем». Кожен гаманець складається з двох унікальних і

окремих криптографічних ключів: відкритого ключа і закритого ключа. Відкритий ключ - це місце, де трансакції депоновані та вилучені. Це також ключ, який відображається на обліковому записі blockchain як цифровий підпис користувача.

Навіть якщо користувач отримує платіж у Bitcoins до свого відкритого ключа, вони не зможуть вилучити їх з приватним партнером. Відкритий ключ користувача - це скорочена версія приватного ключа, створена за допомогою складного математичного алгоритму. Однак через складність цього рівняння практично неможливо змінити процес і створити приватний ключ з відкритого ключа. З цієї причини технологія blockchain вважається конфіденційною.

Висновки.

Було розглянуто особливості технології блокчейн у інформаційному просторі. Хоча блокчейн повністю приватний але в той самий час усі транзакції відкриті і кожен може їх відстежити. Прозорість це головне у цій децентралізованій системі, але усі транзакції без імені власника, транзакції містять в собі адресу гаманця відправника, адресу одержувача, час коли було відправлено, кількість переведеної валюти та комісія за переведення. Велика перевага криптовалюти в тому що її можна розділяти до дуже малих частин і все одно будуть проходити транзакції через те що ціна на криптовалюту може дуже зрости сума транзакціїї буде сменшуватися, це є перевага над звичайними грошами.

Перелік посилань

1. [Електронний ресурс] – Проблема захисту персональних даних в мережі інтернет https://cyberleninka.ru/article/v/problemy-zaschity-personalnyh-dannyh-v- seti-internet
2. [Електронний ресурс] – Інформаційна безпека https://vuzlit.ru/1024552/informatsionnaya_bezopasnost_kak_snizit_bankov skie_riski_v_rf
3. [Електронний ресурс] – Блокчейн технології для кожногоhttps://xakep.ru/2017/11/09/blockchain-bitcoin-conference/
4. [Електронний ресурс] – Блокчейн. Перспективи розвитку http://nbuv.gov.ua/j-pdf/Chac_2017_26_10.pdf

Надійшла: 25.06.2020 Рецензент: д.т.н., професор Савченко В.А.