DOI: 10.35681/1560-9189.2022.24.1.263077

УДК 004.738

Т. О. Охріменко[1], О. І. Макаренко[1], А. В. Бредніков[1], А. В. Толбатов[1], І. О. Бондаренко[2]
[1]Національний авіаційний університет
Проспект Любомира Гузара, 1, 03058 Київ, Україна
[2]Вінницький національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

Проблеми анонімності та централізації фінансових систем і їхнє вирішення за допомогою технології Blockchain

Наразі централізована фінансова система має істотні недоліки. Персональні дані концентруються у централізованих базах даних і підлягають достатньому ризику бути скомпрометованими. Існує проблема захисту персональних даних користувачів. Крім того існує проблема анонімності сторін транзакції. Також проблемою централізованого фінансового світу є так званий «Ефект Метью». У статті наведено статистику витоків персональних даних. Розглянуто рішення Blockchain, яке засноване на протоколі Monero, що дає змогу вирішити окреслені проблеми. Для забезпечення анонімності та високої продуктивності представлено технології: Ring Signature, одноразової адреси (Stealth Address), Ring Confidential Transactions (RingCTs).

Ключові слова: *децентралізовані фінанси, технологія розподіленого реєстру Blockchain, безпека персональних даних, DeFi.*

Вступ

Сервіси інтернет-додатків, засновані на централізованій архітектурі (включаючи фінансові послуги), постійно збирають персональну інформацію про користувачів з різних причин для розвитку бізнесу, проте не приділяється достатньої уваги захисту конфіденційності користувачів, який має бути основою, навіть якщо і не може стимулювати зростання прибутку. Однак, як тільки інформація користувачів проникне через подібні програми, існує ймовірність загрози того, що сотні мільйонів користувачів будуть скомпрометовані. Витік інформації, якщо нею зловживають хакери, призводить до непередбачуваних катастроф для користувачів, наприклад, шахрайства з грошима або особистими даними. На даний час суспільство гостро потребує заходів захисту приватного життя, які керуються технологіями і не залежать від волі людини, оскільки конфіденційність є основним правом людини.

Вісімдесят відсотків світового багатства перебуває в руках двадцяти відсотків людей. Це соціальне явище має назву «розщепленням на дві вісімки» або «ефектом Метью». Ефект Метью [1] відображає поляризацію нашого суспільства, коли багаті стають багатшими, а бідні — біднішими. Ефект Метью особливо помітний у фінансовому світі. У централізованому фінансовому світі влада фінансів сконцентрована саме у цих двадцяти відсотків. Замкнений фінансовий світ — це та проблема, яка заважає подальшому розвитку економіки, оскільки правила захищають інтереси невеликої кількості людей, а інші виключають більшість.

Мета роботи

Метою роботи є розробка покращеної (удосконаленої) моделі на основі існуючих протоколів технології Blockchain для вирішення проблем централізованої фінансової системи, а саме проблеми забезпечення безпеки персональних даних та анонімності.

Проблеми централізованої фінансової системи

Централізована фінансова система має певні недоліки. Висока концентрація влади дозволяє централізованим фінансовим установам маркувати, відслідковувати та навіть блокувати особисті активи людей, а також мати контроль над їхніми персональними даними. Банки є інструментом централізованих фінансових інститутів. Коли звичайні люди передають контроль над своїми активами банкам або трастовим компаніям, ці фінансові посередники можуть з легкістю використовувати гроші на ринку для інвестицій, і в разі високого прибутку, вони передають обумовлену частину своїм клієнтам.

Фінансові кризи низькоякісних іпотечних кредитів часто відбувалися протягом усієї історії. Централізованим фінансовим інститутам було неможливо передбачити ці ризики, і вони були ще більше схильні до помилок. Ці ризики завдають великої шкоди централізованій системі. У централізованому фінансовому світі є порогові значення для участі у фінансових подіях. Наприклад, приватний капітал, венчурний капітал і фінансові злиття та поглинання пов’язані з приватними фондами або деякими великими фігурами на фінансовому ринку, і звичайні інвестори ніколи не зможуть подолати розрив у капіталі. Тому більшість якісних проектних можливостей контролюються найвищим класом.

Згідно з дослідженням [2] витоків конфіденційної інформації з організацій централізованого фінансового сегмента в табл. 1 наведено наступні результати.

Таблиця 1 Статистичні дані витоків інформації

Опис	**Значення (кількість або відношення)**
Загальна кількість витоків даних із організацій фінансового сегмента зафіксована у світі в 2019 році	218
Порівняно з минулим роком	+ 7,9 %

Опис	Значення (кількість або відношення)
На витоки із централізованого фінансового сегмента від усіх витоків, зафіксованих у світі	8,7 %
У результаті витоків із організацій централізованого фінансового сегмента було скомпрометовано записів, що відносяться до типу даних користувачів (персональні дані та платіжна інформація)	Більше 1,04 млрд.
У порівнянні з минулим роком	У 27 разів більше
Частка зафіксованих випадків компрометації інформації із організацій централізованого фінансового сегмента, серед яких був витік персональних даних	64,5 %
На частку співробітників припадає відсоток усіх витоків із організацій фінансового сегмента	46,7 %
Частка витоків із організацій фінансового сегмента, що були зв'язані з використанням мережевого каналу передачі інформації	83,2 %

Децентралізована система фінансів (DeFi)

Концепції «децентралізованих фінансів, розподілених фінансів і програмованих фінансів», які набувають поширеності з кожним роком, можуть мати однакову цінність для DeFi, яка має кілька важливих особливостей:

— заснована на Blockchain-технологіях;

— активи контролюються фізичними особами;

— кліринг і розрахунки здійснюються в режимі реального часу і є криптографічно захищеними.

Децентралізовані фінанси (DeFi) — це технологія з відкритим вихідним кодом, яка спрямована на усунення посередників шляхом введення децентралізованого реєстру для того, щоб поліпшити поточну фінансову систему у всіх аспектах.

Основна частина

Block-DAG

Розглянемо базову структурну декомпозицію основного модуля Blockchain-рішення, яка показана на рис. 1. Безперервна робота системи та постійно виникаючі бізнес-вимоги зможуть просувати вперед безперервну ітерацію системи Blockchain-технології. Крім того, в ітерації відбуватимуться феноменальні зміни, зумовлені технологічним прогресом (наприклад, квантові обчислення, апаратні прориви тощо). Проте технологічні оновлення не змінять структуру технології Blockchain. Це дозволить оптимізувати лише основні модулі в рамках фреймворку. Тому структура анонімного, високопродуктивного та розширюваного Blockchain-децентралізованого фінансового рішення, розгорнутого в рамках Blockchain-системи, є досить стабільною.

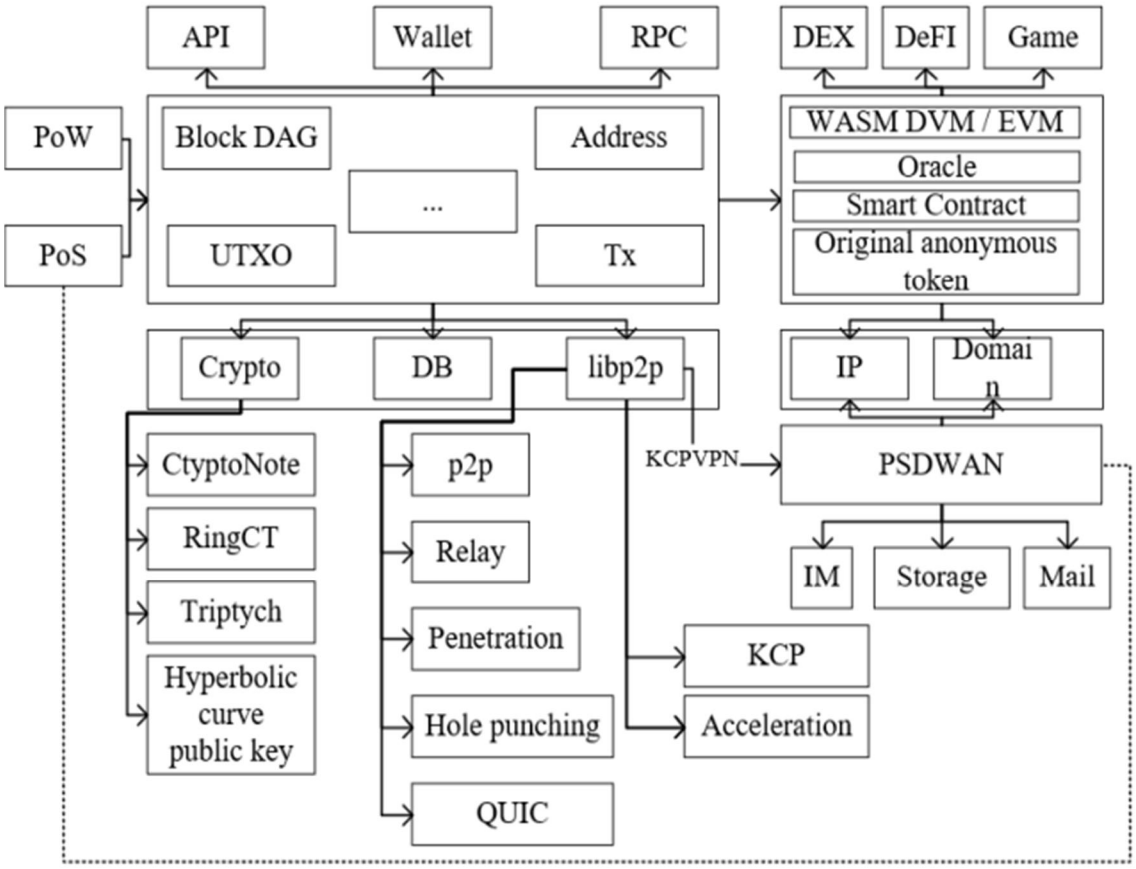

Рис. 1. Системна схема запропонованої моделі

Blockchain, по суті, подібний до бухгалтерської книги. Він містить інформацію про угоди між усіма зацікавленими сторонами, як будь-яка інша база даних. Однак якщо є необхідність, щоби база даних була стійкою від атак і найголовніше — підтримувала один і той же стан на різних пристроях, а саме: анонімне, високопродуктивне, децентралізоване фінансове рішення, що розширюється, з Blockchain одночасно це буде непросто. Традиційні фінансові платіжні системи можуть опрацьовувати від тисяч до десятків тисяч транзакцій кожну секунду. На відміну від цього, продуктивність обробки транзакцій Bitcoin [3] відрізняється на кілька порядків. Продуктивність обробки транзакцій різних відомих Blockchain-проектів показана в табл. 2 нижче.

Bitcoin використовує ланцюгову структуру для організації блоків [3, 4], таким чином кількість транзакцій, які може містити кожен блок, обмежено. Коли є кілька майнерів, що працюють над блоком, і кілька блоків знайдені одночасно, майнерам потрібно вибрати «кращий ланцюжок», заснований на принципі найдовшого ланцюга, і тимчасово відкинути інші блоки. Причина, через яку він є «тимчасовим», полягає в тому, що відкинутий блок буде продовжувати розширюватися та відповідати принципу найдовшого ланцюга, а потім займе місце колишнього кращого ланцюга. У верхній частині Blockchain постійний процес «відбору, відкидання та

конвергенції» називається «вибором кращого ланцюжка». Наприклад, є 10 майнерів, які видобули 10 блоків на одному рівні і в один і той же час, і в кожному блоці є 100 транзакцій, тоді лише один блок буде продовжено за кращим ланцюжком, а решту 9 блоків буде відкинуто. Таким чином, 900 відкинутих транзакцій будуть упаковані та підтверджені у наступних блоках. Отже, якщо всі десять блоків можуть бути підтверджені одночасно, продуктивність обробки буде збільшена в 10 разів.

Таблиця 2. Продуктивність обробки транзакцій різних Blockchain-проектів

Name	**TPS**	**Block time**
BTC	7	10 min
BCH	24	10 min
LTC	7~28	2,5 min
ETH	20~40	15 s

Вибір кращого ланцюжка також спричинить ще одну важливу проблему безпеки — 51-відсоткову атаку з хеш-швидкістю. Як згадувалося раніше, майнери, які контролюють хешрейт, можуть фактично маніпулювати вибором «кращого ланцюжка» та перезаписувати попередній блок своїми спеціально підібраними створеними блоками. Так що, як запобігти 51-відсотковій атаці хешрейту та підвищити безпеку Blockchain, стало гарячою темою в Bitcoin (проілюстровано на рис. 2).

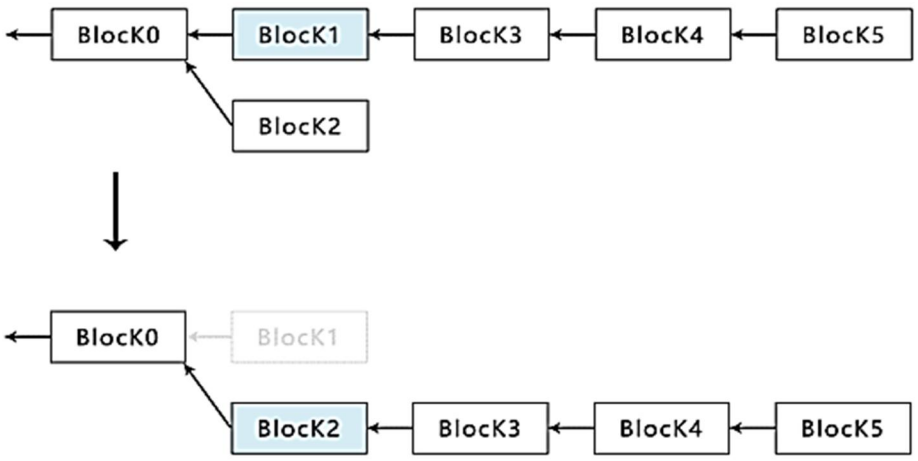

Рис. 2. Вибір кращого ланцюга Bitcoin

Концепція Block-DAG

Block-DAG використовує Орієнтований Ациклічний Граф (DAG) [5] для організації блоків. DAG відноситься до орієнтованого графа без петель. У неорієнтованому ациклічному графі, якщо лінія йде з точки A в точку B через C, а потім знову в точку A, то утворюється петля. Після зміни напрямку ребер з B на C, він

знову повертається в направлений ациклічний граф. Іншими словами, Block-DAG використовує «граф» замість «ланцюга» для організації блоків, і таким чином вирішує проблему продуктивності та безпеки «кращого вибору ланцюга» Bitcoin. Іншими словами, різновид між Block-DAG і традиційним ланцюгом Bitcoin полягає в тому, що обробка блоків Bitcoin є аналогією однопотокової обробки, в той час, як BlockDAG є багатоядерною і багатопотоковою (рис. 3).

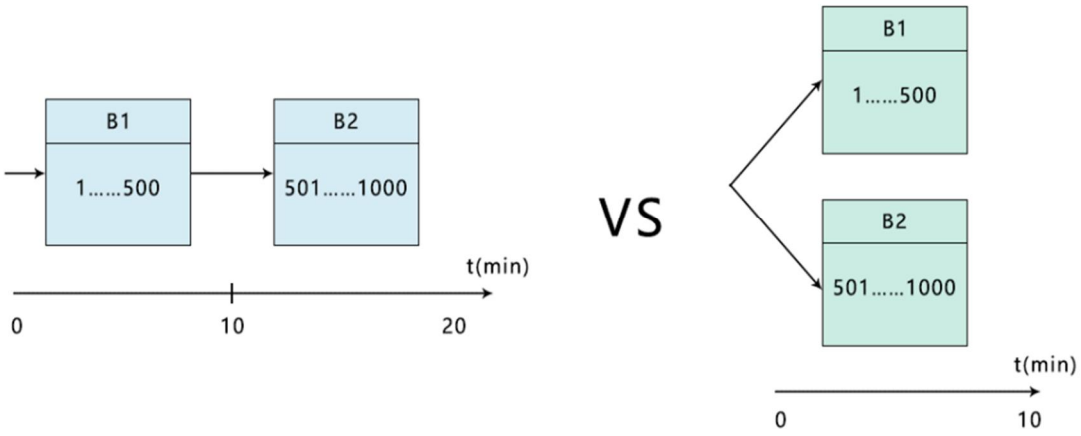

Рис. 3. Паралельна обробка транзакцій

Blockchain, що базується на Block-DAG, більше не є єдиною ланцюговою структурою. Весь Blockchain утворює мережу, як показано на рис. 4.

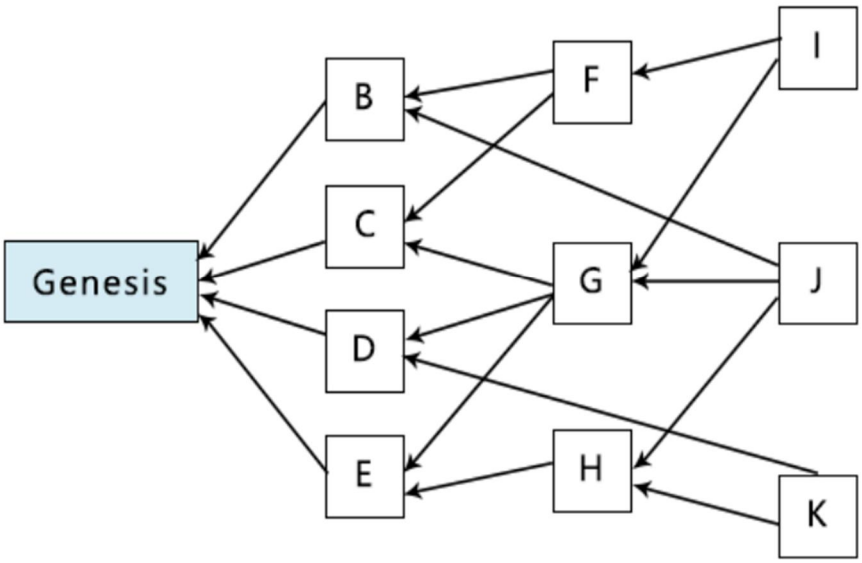

Рис. 4. Організація блоків Block-DAG

Як відомо, у Blockchain блоки постійно розширюються до більш вищого рівня. У Block-DAG, якщо блок не має нового блоку, пов’язаного з ним, це означає, що блок знаходиться у верхньому положенні, і такі блоки називаються «наконечниками». Починаючи з кожної вершини, генезис-блоки можна простежити тільки

в одному напрямку. На наконечник посилатиметься новий блок, а в свою чергу новий блок може посилатися на кілька наконечників одночасно. За допомогою наведеного рис. 4 розглянемо, як блок Block-DAG розширюється сам собою.

На самому початку весь Blockchain має лише один блок — генезис-блок, що означає, що є лише 1 наконечник. Якщо припустити, що одночасно працюють 4 майнери, то 4 блоки {B, C, D, E} будуть розширені на тому самому наконечнику.

Припустимо, що через швидкість видобутку та передачі мережею майнер A та майнер B отримали {B, C}, майнер C отримав {C, D, E}, а майнер D отримав тільки {E}, який він видобув сам. Таким чином, вони продовжують видобуток на основі наконечника {B, C}, {C, D, E} та {E}. Їм не потрібно продовжувати чекати, поки всі блоки вузлів будуть верифіковані, або вибирати найкращий ланцюжок {B, C, D, E}.

Розділимо наконечник {B, C, D, E} на три групи: {B, C}, {C, D, E}, {E}, який виготовляє нові блоки {F, H, I}, майнери використовують їх як наконечник і продовжують добувати, а решту можна зробити тим же способом.

У блоці Block-DAG, після того, як наконечник використовується наступним блоком, він називається «батьківською стороною», що аналогічно концепції «батьківського блоку» в Bitcoin. «Сторона» — це концепція алгоритму DAG, яка більш докладно була розглянута у [6]. Як бачимо, через різні непередбачувані фактори не кожен наконечник може бути «батьківською стороною» і може продовжувати розширюватися. Цей вид блоку буде відкинутий як «сирітський блок» у DMCH [7].

Розглядаючи крайній випадок, якщо новому блоку дозволено посилатися на всі наконечники, які йому доступні, це означає, що буде більше паралельних блоків на однаковій висоті, що призведе до більшої продуктивності обробки транзакцій, але побічні ефекти також дуже очевидні. Якщо майнерів буде достатньо, блок розширюватиметься без обмежень. Тому ми маємо знайти баланс для максимальної кількості наконечників, на які можуть посилатися нові блоки. Максимальна кількість наконечників, на які дозволено посилатися новим блокам у розглянутій моделі, становить 3. Це значення може бути динамічно скориговано, і після інтеграції із сегментами транзакцій воно дозволить збільшення в TPS [8].

Анонімність

Розглянута модель базується на Blockchain-протоколі Monero, який, у свою чергу, походить з протоколу CryptoNote [4]. Оригінальний Whitepaper CryptoNote був опублікований у 2012 році. Автор оригінального Whitepaper використав псевдонім Ніколас Ван Саберхаген. Менш ніж через рік, після того, як друге видання Whitepaper було опубліковано під тим самим псевдонімом, особистість автора, як і раніше, залишається невідомою. Протокол CryptoNote в основному вирішує дві проблеми:

1) невідстежуваність — це означає, що для всіх транзакцій, що входять, всі можливі відправники можуть бути джерелом, але невідомо, хто їх відправив;

2) непов'язаність — це означає, що неможливо довести, що будь-які дві вихідні транзакції відправлені від однієї й тієї ж людини.

Кільцевий підпис

Функція невідстежуваності використовує технологію кільцевого підпису. Ця технологія може вирішити проблему анонімності відправника транзакції. Технологія кільцевого підпису заснована на концепції групового підпису, запропонованого Девідом Чаумом та Е. Ван Хейстом [10]. Кільцевий підпис використовує кілька публічних підписів, які змішуються разом, щоб приховати реальний підпис транзакції, що не вплине на можливість перевірки дійсності транзакції. І слід зазначити, що пізніше було доведено, що технологія кільцевого підпису може бути простежена за певних обставин [11]. Пізніше це питання вирішили в компанії Monero Ring Confidential Transactions (RingCTs) [12].

Одноразовий ключ

Функція непов'язаності, використовує технологію одноразового ключа, яка може вирішити проблему анонімності одержувача транзакції. Оскільки відкритий ключ необхідний під час зміни підпису, всі вхідні транзакції адреси відкритого ключа можна спостерігати на Blockchain, тому легко викрити всі сторони, що пов'язані з транзакцією. Таким чином, удосконалена технологія обміну ключами Діффі-Хеллмана [13, 14] дозволяє генерувати одноразовий ключ для захисту всіх сторін. Загальний принцип полягає в тому, що відправник транзакції використовує власні дані для хешування відкритого ключа одержувача і таким чином створює унікальний одноразовий ключ для транзакції, тому тільки одержувач може генерувати закриту частину транзакції [9].

Досягнення анонімності

У процесі досягнення анонімності окремий користувач має два закриті та два відкриті ключі для завершення всього процесу шифрування. Технологія Ring Signature гарантує анонімність відправника транзакції, технологія одноразової адреси (Stealth Address) гарантує анонімність одержувача транзакції, а технологія Ring Confidential Transactions (RingCTs) гарантує анонімність вмісту транзакції.

Механізм верифікації

Механізм верифікації можна поділити на класичний розподілений механізм верифікації і Blockchain-механізм верифікації. Початок досліджень механізму верифікації можна простежити з 1975 року, коли в комп'ютерній області було піднято «проблему двох армій». Західні вчені досліджували «проблему візантійських генералів», яка зосереджена на тому, як небездоганні вузли можуть досягти верифікації з будь-якими конкретними даними, коли можуть бути несправні вузли або шкідливі атаки. Дослідження механізму верифікації грунтується на цій проблемі. 2008 року, коли Сатоші Накамото запропонував Bitcoin, механізм верифікації відкрив еру верифікації Blockchain. На даний час механізм верифікації Blockchain можна розділити на дві категорії: один є авторизованим механізмом верифікації, а інший — несанкціонованим механізмом верифікації. Авторизований механізм верифікації вимагає від користувача повної аутентифікації особи перед участю в наступному механізмі угоди, у той час як при несанкціонованому механізмі верифікації, який

представлений Bitcoin, вузли можуть входити та виходити з Blockchain у будь-який час, а кількість вузлів схильна до динамічної і непередбачуваної зміни, а процеси вибору виробника блоків, генерації блоків, верифікації вузлів та оновлення Blockchain здійснюються за допомогою певних алгоритмів. Безумовно, найбільш успішним механізмом верифікації, як і раніше, є proof-of-work (PoW), а саме майнінг. Загалом значна кількість Blockchain у галузі використовує механізм верифікації PoW. Однією з причин цього явища є те, що для формування верифікації потрібен час. Друга причина полягає в тому, що PoW ефективно вирішили проблему візантійських генералів за допомогою методів шифрування та економічних стимулів. Тим не менш, за десять років, що минули з моменту створення Bitcoin, можна визнати, що в механізмі PoW виникли деякі похідні проблеми. Механізм верифікації Blockchain в основному оцінюється за шістьома аспектами: безпека, пропускна спроможність транзакцій, масштабованість, час підтвердження транзакцій, децентралізація та зайняття ресурсів. Розглянемо покращений механізм верифікації, що формується через три етапи — PoW, PoW+ pure-proof-of-stake (PPoS) та PPoS. Його схема трансформації повторює схему ETH. Крім того, оскільки розглянуте рішення базується на протоколі Monero, його безпека, пропускна здатність транзакцій, масштабованість і час підтвердження транзакцій успадкували здатність Monero. Додатково, за допомогою технології BlockDAG та технології шифрування була покращена безпека (анти-51-відсоткова подвійна атака), пропускна здатність (TPS збільшена до 70) та час підтвердження транзакцій (близько 2 хвилин).

Висновки

Розглянуто проблеми централізованих фінансових систем. Виділено ключові ризики для користувачів і представлено статистику витоку персональних даних. Як вирішення проблеми розглянуто модель Blockchain протоколу, що базується на протоколі Monero, а також Blockchain-концепцію Block-DAG.

Проаналізовано технологію Ring Signature, що гарантує анонімність відправника транзакції і технологію одноразової адреси (Stealth Address), що в свою чергу гарантує анонімність одержувача транзакції. Також розглянуто технологію Ring Confidential Transactions (RingCTs), що гарантує анонімність відправника транзакції і суми, що відправляється. Проведено порівняння з існуючими Blockchain-протоколами, виділено покращений алгоритм верифікації.

1. Frost Jon, Gambacorta Leonardo, and Gambacorta Romina. The Matthew Effect and Modern Finance. *On the Nexus between Wealth Inequality, Financial Development and Financial Technology,* 2020, SSRN: https://ssrn.com/abstract=3666377

2. Статистика витоків конфіденційної інформації. URL: https://www.infowatch.ru/

3. Bitcoin Whitepaper. URL: https://bitcoin.org/bitcoin.pdf

4. CryptoNote Standards. URL: https://cryptonote.org/standards/

5. Liou J., Palis M.A. An Efficient Clustering Heuristic for Scheduling DAGs on Multiprocessors. *Proc. Symp. Parallel and Distributed Processing,* 1996.

6. Bouali L., Oukfif Karima, Bouzefrane S., Oulebsir F. A Hybrid Algorithm for DAG Application Scheduling on Computational Grids. *International Conference on Mobile, Secure and Programmable Networking,* 2015. P. 63–77.

7. Darma Cash. URL: https://www.darmacash.com/

8. Sydorenko V., Gnatyuk S., Fesenko A., Yevchenko Y., Tolbatov A., Sotnichenko Y. Experimental FMECA-based assessing of the critical information infrastructure importance in aviation. *CEUR Workshop Proceedings.* 2020. Vol. 2732. P. 136–156.

9. Application Layer Protocol. URL: https://cryptonote.org/inside

10. David Cham. Group Signatures. EUROCRYPT '91. 1991. P. 257–265.

11. Fujisaki E., Suzuki K. Traceable Ring Signature. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*. 2007. P. 181–200.

12. Monero Ring Confidential Transactions. URL: https://www.getmonero.org/resources/moneropedia/ringCT.html

13. Rebecca N. Wright. Encyclopedia of Physical Science and Technology. Third Edition, 2003.

14. Iavich M., Iashvili G., Gnatyuk S., Tolbatov A., Mirtskhulava L. Efficient and Secure Digital Signature Scheme for Post Quantum Epoch. *Communications in Computer and Information Science.* 2021. Vol. 1486. P. 185–193.

Надійшла до редакції 10.05.2022