УДК 002.55 DOI: 10.31673/2518-7678.2019.044448

Ткаленко О.М., к.т.н.; **Мельник М. В.**

АНАЛІЗ ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН З МЕТОЮ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БАНКІВСЬКИХ ОПЕРАЦІЙ

Tkalenko O.M., Melnyk M.V. Analysis of the use of blockchain technology to ensure the security of banking operations.

Blockchain is one of the most promising technological sectors (along with Big Data, Machine learning, artificial intelligence), comparable in scale, degree of influence and distribution in the future with the effect that the Internet once produced. The features of the distributed registry technology allow its use in various fields - from file transfer systems to more reliable copyright protection, for example, in art and science. This article analyzes the features and effectiveness of using blockchain technology to ensure the safety of banking operations. The analysis of means ensuring the safety of the use of this technology is carried out. The basic principles that are useful when using blockchain technology in banking operations, as well as possible vulnerabilities of this technology are described.

Keywords: blockchain, hashing, hash functions, electronic signature, collisions, public key, phishing, token, integration, identification, security, SWIFT.

Ткаленко О.М., Мельник М.В. Аналіз застосування технології блокчейн з метою забезпечення безпеки банківських операцій.

Блокчейн - одна з найперспективніших технологічних галузей (поряд з Big Data, Machine learning, штучним інтелектом), яка порівнюється за масштабом, мірою впливу і поширенням у майбутньому з тим ефектом, що справила на світ мережа Інтернет. Особливості технології розподіленого реєстру дозволяють використовувати її у різних галузях - від систем передавання й до більш надійного захисту авторських прав, наприклад, у мистецтві, науці. У даній статті проведений аналіз особливостей і ефективності застосування технології блокчейн для забезпечення безпеки банківських операцій. Проведено аналіз засобів, що забезпечують безпеку застосування даної технології. Описано основні принципи, корисні при використанні технології блокчейн при проведенні банківських операцій, а також можливі вразливості даної технології.

Ключові слова: блокчейн, хеш-функції, електронний підпис, колізії, відкритий ключ, фішинг, токен, інтеграція, ідентифікація, безпека, SWIFT.

Ткаленко О.М., Мельник Н.В. Анализ применения технологии блокчейн с целью обеспечения безопасности банковских операций.

Блокчейн - одна из самых перспективных технологических отраслей (наряду с Big Data, Machine learning, искусственным интеллектом), сравнимая по масштабу, степени влияния и распространением в будущем с тем эффектом, который в свое время произвел Интернет. Особенности технологии распределенного реестра позволяют использовать ее в различных областях - от систем передачи файлов и к более надежной защиты авторских прав, например, в искусстве, науке. В данной статье проведен анализ особенностей и эффективности применения технологии блокчейн для обеспечения безопасности банковских операций. Проведен анализ средств, обеспечивающих безопасность применения данной технологии. Описаны основные принципы, полезные при использовании технологии блокчейн при проведении банковских операций, а также возможные уязвимости данной технологии.

Ключевые слова: блокчейн, хеширование, хеш-функции, электронная подпись, коллизии, открытый ключ, фишинг, токен, интеграция, идентификация, безопасность, SWIFT.

Вступ

Зниження витрат, підвищення рівня безпеки та більш висока прозорість транзакцій - три основні сильні сторони блокчейну. У зв'язку з потребою банків, бізнесу і суспільства в цих трьох аспектах, будь-яка теоретична робота або розробка в цій області стає досить актуальною. Основна задача - це визначити, наскільки застосування технології блокчейн забезпечує безпеку банківських операцій у порівнянні з рівнем безпеки при поточних способах проведення банківських операцій.

Виклад основного матеріалу дослідження

Двома основними елементами блокчейну, що забезпечують його безпеку, є хеш-функції і електронний підпис.

Хешування - це процес перетворення масиву вхідних даних довільної довжини у бітовий ряд фіксованої довжини, яка подається на вихід. Правильно складена хеш-функція забезпечує захист від колізій - неможливість отримати два однакових хеша при різних початкових даних - і має ефект лавини, коли будь-яка зміна в масиві вхідних даних тягне за собою зміни, що з'являються на виході бітового рядку.

Хеш-функції гарантують незмінність блоків транзакцій - неможливо внести зміну в окремий блок, не змінивши весь ланцюжок. Це відбувається через те, що кожен новий блок посилається на хеш попереднього в реєстрі. Індивідуальний хеш блоку залежить від усіх його транзакцій, але замість того, щоб послідовно передавати транзакції хеш-функції, вони збираються воєдино хеш-значення за допомогою двійкового дерева Меркле. Таким чином, хеші використовуються як заміна вказівникам у звичайних структурах даних: пов'язаних списках і двійкових деревах.

За рахунок використання хешів загальний стан блокчейну можна висловити одним-єдиним числом: хешем самого нового блоку. Тому властивість незмінності хешу одного блоку гарантує незмінність всього блокчейну (рис. 1).

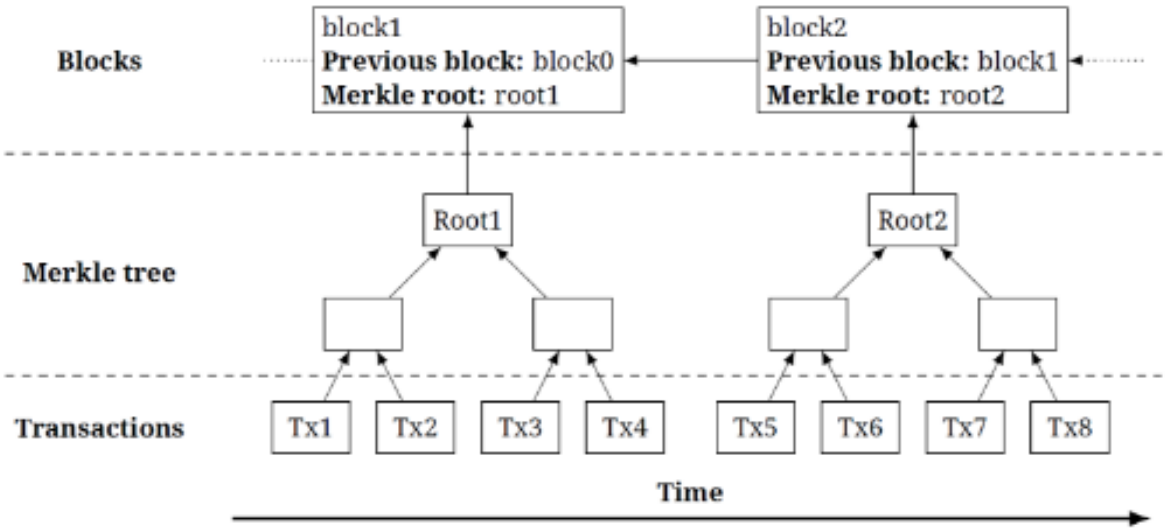

Рис. 1. Процес формування хешу

У цифрових підписах у блокчейнах використовуються два ключа - закритий і відкритий [1]. Перший використовується для формування цифрового підпису та є засекреченим. Другий - для перевірки справжності підпису. Відкритий ключ можна обчислити на підставі закритого, а ось зворотна дія на практиці не реалізовується через занадто великий обсяг обчислень (рис. 2).

Визначимо, яким чином блокчейн може підвищити безпеку банківських операцій. Блокчейн не захищає від самого поширеного зараз методу шахрайства - фішингу, - коли зловмисники не атакують систему безпосередньо, а за рахунок вірусів крадуть паролі від рахунків. У випадку з блокчейном – це буде електронний підпис/токен/ключ і т. д.

Виконуючи дослідження, визначено, що не менш серйозним, особливо в Україні, є шахрайство співробітників банків стосовно рахунків і кредитних ліній клієнтів - і це як раз

те, з чим впровадження блокчейну може боротися. Ключова відмінність блокчейну від звичайних децентралізованих баз у формуванні блоків, які практично неможливо скомпрометувати, і заміна централізованої бази даних в окремому банку на приватний блокчейн з певними обмеженнями на читання і редагування пішов би на користь всім - самим клієнтам, регуляторам і самому банку.

Зараз при використанні централізованих баз, недобросовісні співробітники можуть без відома клієнта, наприклад, змінювати умови по кредиту (підвищувати процентну ставку). У разі відсутності закріпленого на папері підтвердження умов, вся інформація про кредити зберігається в електронному вигляді - і банкір, що знаходиться у змові з працівником ІТ-відділу може без відома клієнта від його імені погодитися на зміни умов, і при цьому зачистити або «скинути» логи, щоб договір у базі виглядав таким чином, ніби він так укладений з самого початку.

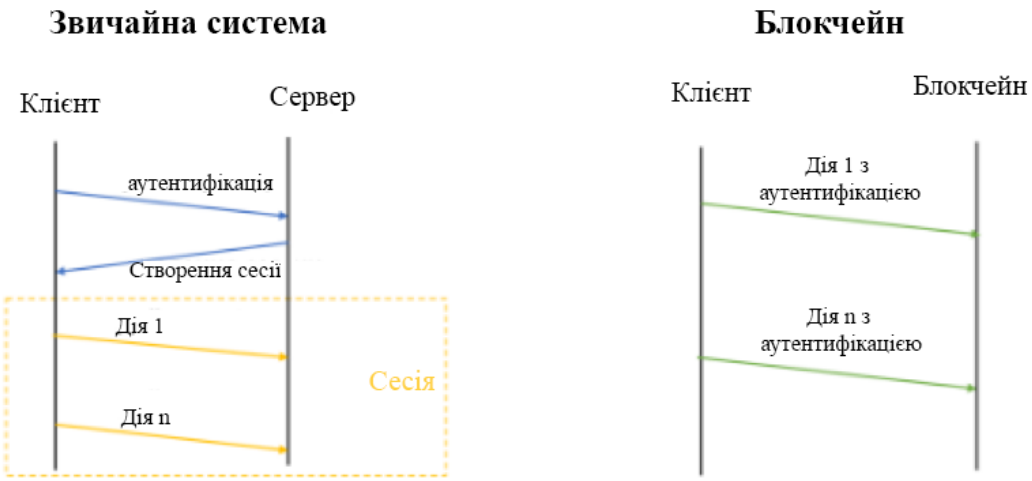

Рис. 2. Різниця у зверненні до системи через електронний підпис у блокчейні у звичайних випадках

Дослідження показали, що застосування блокчейну дозволить уникнути цієї проблеми з кількох причин. По-перше, ніякі зміни у стані рахунку будуть неможливі без підтвердження унікальним електронним підписом клієнта, який зберігається у нього.

По-друге, початкові умови за договором вже будуть представляти із себе блок, який не можна буде змінити - будь-які зміни будуть розглядатися вже в рамках нового блоку, який буде містити хеш попереднього. По-третє, у кожного клієнта у розпорядженні буде копія бази з банку (наприклад, з обмеженим правом редагування і з правом читання всіх), яка буде синхронізуватися в певний проміжок часу (наприклад, раз на добу).

З інтеграцією блокчейну стане неможлива ситуація, що відбувалася у 2011-2016 роках в американському банку Wells Fargo, коли співробітники банку (з санкції топ-менеджменту, який виборює бонуси) відкривали тисячі неузгоджених з клієнтами кредитних ліній, що призвело до найбільшого з 2008 року скандалу в банківському секторі США і мільярдних втрат клієнтів [2]. Ще одна проблема, яка могла б вирішитися використанням свого приватного блокчейну у кожному банку - ведення депозитів. Проблема для будь-якого банку полягає в тому, що будь-який депозит необхідно забезпечувати резервами в Центральному банку, а резерви - це непрацюючі гроші.

Тому, існує досить поширена схема, коли знову ж без згоди клієнта гроші з його депозитного рахунку переводяться на інвестиційний (управитель) рахунок - банк отримує можливість не виділяти кошти під резерви і при цьому ще грати на біржах на гроші клієнта.

В результаті, якщо банк «лопається», то клієнт не може розраховувати не тільки на свої відсотки, але і на початковий внесок, оскільки керуючі рахунки не забезпечуються страховкою з резервів ЦБ.

Інтеграція блокчейну дозволить отримати всі ті ж переваги в плані безпеки для клієнта, що й описані вище для кредиту - неможливість змінювати умови і процентні ставки без його відома, неможливість для банку приховувати результати своїх махінацій від клієнтів і регуляторів. Для взаємин вже між банками - власні міжбанківські розрахунки, розрахунки по клірингу, перекази між клієнтами різних банків, ейкварінг і так далі - необхідний приватний блокчейн з уже більш широкими повноваженнями з читання, який би охоплював би кілька банків - поки ця стадія далека від реалізації. Ключова перевага в плані безпеки в даному випадку в порівнянні з тим, що забезпечує зараз SWIFT, можливість зробити «відкат» блокчейну до стану «передатаки» (оскільки були вкрадені тільки цифрові активи), якщо більше 50% учасників мережі погодяться. В даному випадку присутня певна конфронтація з самою філософією блокчейну, що вже завершені блоки будуть збережені. Однак саме такий підхід був застосований, коли зловмисник вкрав ефірів у блокчейні «Ефіріум» на суму понад 50 млн. доларів.

Взаємини між компаніями складніші, оскільки, якщо один агент переводить гроші і отримує за це послугу, то в корпоративному секторі ланцюжок довший: як мінімум одна компанія представляє іншій зобов'язання заплатити, друга надає якусь послугу, і перша потім здійснює платіж. Проблема полягає в тому, що в поточних умовах жодна платформа не забезпечує такого функціоналу. Для забезпечення взаємовідносин всередині корпоративного сектору для банків являються важливими - смарт-контракти, які можна запрограмувати під кожен з можливих сценаріїв розвитку подій. Важлива проблема цього напрямку полягає в тому, що на даний момент відсутні регулятивні заходи щодо смарт-контрактів. Отже, якщо стався збій в контракті, або контрагент не виконав своїх зобов'язань. На даному етапі смарт-контракти розумно впроваджувати саме для скорочення витрат, але не як засіб підвищення безпеки, оскільки в їх кодуванні досі залишаються серйозні прогалини.

Висновки

Застосування технології блокчейн забезпечить підвищення рівня безпеки банківських операцій, особливо у сфері ведення рахунків, обслуговування депозитів та кредитних ліній - і це найлегше реалізувати на практиці, оскільки банку необхідний для цього тільки свій приватний блокчейн без взаємозв'язку з іншими банками і ЦБ. Для корпоративного сектору однозначної відповіді немає, в першу чергу, через відсутність регулювання смарт-контрактів і проблеми в їх програмному коді.

Відповідно до сучасних стандартів, в рамках інформаційних систем повинні реалізовуватися щонайменше наступні механізми безпеки: ідентифікація і перевірка справжності користувача; управління доступом; протоколювання і аудит; криптографія; екранування (засіб розмежування доступу); забезпечення високої доступності.

Відповідно порівнюється блокчейн за цими критеріями з поточними інструментами виконання банківських операцій - реляційними централізованими базами даних (для зберігання інформації по депозитах і кредитах) і SWIFT для переказів.

Дослідження показали, що блокчейн дає результати, що перевершують інші по забезпеченню безпеки: по-перше, за рахунок електронного підпису однозначно проводиться ідентифікація користувача - скомпрометувати її можна, тільки вкравши ключ; по-друге, управління доступом і екранування у блокчейні теж на високому рівні - технологія дозволяє розділяти ролі в системі (оператор, аудитор, пересічний користувач) таким чином, щоб не дозволяти всім брати участь, наприклад, в підтвердженні транзакцій; по-третє, у блокчейну

високий рівень криптографічного захисту, оскільки блоки складаються з хеш-сум, а по хеш-сумі не можна однозначно визначити предмет транзакції та інші вхідні дані; в четвертих, перевага блокчейну найважливіша у порівнянні із звичайними базами даних і SWIFT - транзакції формуються у блоки, які практично неможливо змінити. Це дозволяє забезпечити близьке до ідеального протоколювання, оскільки без санкціонованих дій ніхто не зможе видалити транзакції, що забезпечує високий рівень прозорості та значно полегшує аудит, оскільки нічого не можна заховати.

Список використаної літератури

1. Воронцова Е.А., Мелешенко Е.Г. Блокчейн: панацея или угроза для хранения и передачи информации // Синергия наук. 2016. № 5. − С. 93 – 101.

2. Jay J.Wylie, Michael W., Bigrigg, John D. Strunk Survivable Information Storage Systems // Computer. 2000. Volume 33, Issue 8, p. 61-68.

3. Экранирование, анализ защищенности [Електронний ресурс] // – Режим доступу: http://www.intuit.ru/studies/courses/10/10/lecture/318.

Автори статті

Ткаленко Оксана Миколаївна – кандидат технічних наук, доцент, доцент кафедри Інформаційних систем та технологій, Державний університет телекомунікацій, Київ, Україна.

Мельник Микола Віталійович – магістр, кафедра Інформаційних систем та технологій, Державний університет телекомунікацій, Київ, Україна.

Authors of article

Tkalenko Oksana Mykolayivna – candidate of Science (technic), associate professor, associate professor of Information systems and technologies Department, State University of Telecommunications, Kyiv, Ukraine.

Melnyk Mykola Vitaliyovych – student, Information systems and technologies Department, State University of Telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію: 28.10.2019 р. Рецензент: д.т.н., доцент К.П. Сторчак