УДК 621.395.7 (043.2)

В. В. Гуменюк
К. В. Безпалий

ЗАБЕЗПЕЧЕННЯ ДОСТОВІРНОСТІ КОНФІДЕНЦІЙНОГО ГОЛОСУВАННЯ НА ОСНОВІ СМАРТ-КОНТРАКТІВ У МЕРЕЖІ БЛОКЧЕЙН

Вінницький національний технічний університет

Анотація

Робота представляє результати досліджень, заснованих на зібраних даних про методи побудови децентралізованих мереж та розробки додатків із використанням анклавів. Проаналізовано основні принципи створення децентралізованих мереж, а також описано функціонування технології blockchain. Визначено вимоги до систем голосування та застосування мережі blockchain. Розглянуто питання пов'язані з розробкою децентралізованих додатків. Проведено аналіз платформ blockchain.

Ключові слова: інформаційна безпека, кіберзагрози, децентралізовані мережі, анклави, blockchain, системи голосування.

Abstract

The paper presents research findings based on collected data on methods for building decentralized networks and developing applications using enclaves. The fundamental principles of creating decentralized networks are analyzed, and the operation of blockchain technology is described. Requirements for voting systems and the application of blockchain networks are established. The work addresses issues related to the development of decentralized applications, conducts an analysis of blockchain platforms, and designs, develops, improves, and tests a decentralized application for internet voting.

Keywords: *information security, cyber threats, decentralized networks, enclaves, blockchain, voting systems.*

Вступ

Інформаційні технології поступово стають невід'ємною частиною людського життя. Перехід від реального світу до цифрового простору приносить численні переваги. Голосування є основою успішної демократії, тому воно повинно бути доступним та безпечним для усіх громадян. На сьогодні паперові системи голосування є доступними і недорогими, але мають два основні недоліки. Багато експертів вважають, що такі системи не масштабуються належним чином, що призводить до проблем з точністю. Крім того, вони вимагають довіри до організаторів, які повинні правильно і чесно проводити процедуру [1]. Регулярно з'являються повідомлення про злами інформаційних систем, які надають зловмисникам несанкціонований доступ до конфіденційних даних [2]. Метою роботи є можливість мінімізації таких ризиків завдяки швидкому розвитку криптографії, зокрема технології blockchain. Blockchain може запропонувати масштабоване рішення для сучасних і застарілих виборчих систем, забезпечуючи безпечне і захищене від фальсифікацій цифрове голосування. Розглянемо питання розробки децентралізованих додатків з використанням технології blockchain, а також проведемо порівняння різних blockchain платформ.

Забезпечення достовірності конфіденційного голосування на основі смарт-контрактів

Голосування відіграє важливу роль у функціонуванні демократичного суспільства. Традиційне голосування вимагає присутності виборців на виборчих дільницях, що зазвичай пов'язано з витратами часу та значними фінансовими витратами на організацію процесу. Електронне голосування є процесом

прийняття рішень шляхом використання спеціальних електронних засобів для голосування та технічних засобів для підрахунку голосів і оголошення результатів. Одним із різновидів такої процедури є вибори через Інтернет. Ця технологія дозволяє значно скоротити час, необхідний для підрахунку голосів, а також спрощує процедуру голосування для виборців, яким не потрібно фізично з'являтися на виборчі дільниці.

Електронне голосування, засноване на криптографічних методах, забезпечує повнофункціональне онлайн-голосування на будь-яких пристроях з автоматичним і анонімним підрахунком голосів. Це економічніша, прозоріша та неупереджена система порівняно з традиційними методами. Проте, безпекові ризики, такі як можливість злому системи або маніпуляції з результатами, залишаються значним викликом. Для мінімізації цих ризиків використовуються різні протоколи, зокрема гомоморфне шифрування, "кільцевий підпис", Mix networks, "сліпий підпис" та докази з нульовим розголошенням. Попри ці заходи, ризики фальсифікацій і компрометації результатів електронного голосування можуть бути навіть вищими, ніж у традиційних систем.

Аналізуючи критику існуючих систем електронного голосування, можна виділити кілька основних недоліків, які потребують покращення: недостатня прозорість процесу голосування, низька стійкість до відмов системи, а також вразливість до зламів і крадіжок конфіденційних даних. Виходячи з цих загальних вимог безпеки та відмовостійкості, все частіше пропонується використовувати протокол на основі технології блокчейн, який може суттєво покращити зазначені аспекти.

Позитивні властивості блокчейну та біткоїну можна проілюструвати на прикладі угод з нерухомістю. Власник може бути визначений як особа, яка останньою продала будинок, але право власності можна підтвердити лише через повне паперове дослідження усіх пов'язаних транзакцій. Ця "паперова доріжка" зазвичай зберігається та перевіряється титульними компаніями. Хоча система не повністю запобігає шахрайським транзакціям, таким як продаж будинку, яким людина не володіє, або продаж одного й того ж майна декільком сторонам, шахрайство зрештою виявляється, і реальне право власності встановлюється. Подібна перевірка необхідна для фінансових транзакцій, включаючи продаж криптовалют та інших фінансових інструментів. Зазвичай проблема вирішується шляхом запису усіх транзакцій в одному централізованому реєстрі, але такий підхід не завжди є практичним через масштабування та необхідність довіри до зберігача реєстру. Для усунення цих проблем блокчейн надає механізм розподіленої довіри: кілька сторін зберігають записи транзакцій, і кожна з них може перевірити, чи не було змінено порядок та часові позначки транзакцій.

Основний принцип децентралізованих мереж базується на розподіленому реєстрі. Подібно до бухгалтерської книги, в яку записуються всі грошові перекази та нарахування, блокчейн зберігає записи про всі проведені операції. Ці записи можуть включати грошові трансакції та укладені контракти. Копії реєстру з повною історією зберігаються у всіх учасників мережі. Блокчейн є одноранговою мережею, де ресурси використовуються для підтвердження та схвалення кожної транзакції. У такій мережі відсутнє центральне управління, і немає можливості змінювати або підробляти реєстр. Усі учасники мають однакову інформацію, і будь-яка зміна у мережі відбивається на кожному вузлі. Це унеможливлює підробку даних, оскільки будь-які помилкові дані на одному з вузлів не будуть збігатися з даними інших вузлів, що робить їх недостовірними.

Кожна нова транзакція перевіряється учасниками, отримує схвалення та зберігається у блоці. Блоки формуються майнерами, які вирішують складні математичні завдання. Майнинг полягає у виконанні серії обчислень для знаходження хешу із заданими властивостями, що потребує значних операційних витрат. Блок складається із заголовка, хеша заголовка попереднього блоку та певної кількості транзакцій. Блоки об'єднуються в ланцюг (chain), звідси й назва «blockchain». Кожен блок дійсний лише тоді, коли він зв'язаний з попереднім, що виключає можливість зміни реєстру. Для зміни одного блоку необхідно переписати усю його історію в блокчейні. Щоб контролювати всю мережу, потрібно більше 50% обчислювальної потужності, що в масштабах великої системи практично неможливо. Атака 51% у мережі біткоїн потребує зламу 150 000 серверів одночасно, що робить її малоймовірною.

Першим типом є публічний блокчейн. Це відкрита база даних, у якій кожен учасник має можливість читати та записувати дані. Така система не підходить для організацій, що працюють з конфіденційною інформацією, оскільки всі вузли в мережі рівноправні, і дані не можуть бути змінені після внесення. Крім того, всі транзакції у такій базі є загальнодоступними, що забезпечує прозорість, але не гарантує

конфіденційності необхідної для обробки приватних даних. Основною перевагою публічного блокчейну є децентралізація, що виключає потребу в посередниках, таких як банки. Наприклад, передача біткойнів фіксується у блокчейні без можливості зміни або скасування.

Другим типом є приватний блокчейн. Він має обмеження для читання та запису даних і використовується приватними організаціями. Доступ до такої мережі можливий лише за запрошенням, а учасники повинні мати відповідні дозволи. Інформація шифрується для забезпечення конфіденційності. Приватний блокчейн швидший за публічний та дозволяє визначати пріоритетні вузли. Особливим видом приватного блокчейну є консорціум, де транзакції обробляються групою заздалегідь визначених компаній.

Основні принципи побудови децентралізованих мереж включають розподіл, публічність і безпеку. Блокчейн працює на комп'ютерах добровольців по всьому світу, забезпечуючи стійкість до зламу. Будь-який користувач може переглядати блокчейн у будь-який момент, що гарантує прозорість. Високі обчислювальні витрати роблять «атаку 51%» практично неможливою, а система шифрування захищає дані. При побудові децентралізованих мереж важливо враховувати ці принципи, а також забезпечити правильну роботу протоколів та налаштування компонентів мережі, що є завданням розробників.

Оскільки велика кількість сторін бере участь у верифікації кожної транзакції, а копії даних зберігаються у багатьох учасників, система блокчейн забезпечує високий рівень прозорості. Ця властивість дозволяє переконатися, що реєстр не редагувався несанкціонованим шляхом. Кожна транзакція здійснюється з використанням унікального цифрового підпису, що підтверджує факт її виконання певним користувачем відповідно до правил системи.

Структура блоку в технології блокчейн складається зі списку транзакцій (тіла) та заголовка, який містить ключі транзакцій. Тіло блоку включає список усіх попередніх транзакцій, а заголовок зберігає результат виконання хеш-функції поточних і попередніх транзакцій. Хеш ідентифікаторів обчислюється з хешів транзакцій поточного блоку та ідентифікатора попереднього блоку. Це забезпечує зв'язок кожного блоку з попереднім і наступним, зберігаючи надійність системи. Зашифрована у заголовках інформація про дані з попередніх блоків дозволяє відстежувати усі коригування даних, оскільки зміни в одному блоці вплинуть на ідентифікатори всіх наступних блоків.

Маючи ланцюг блоків, що містять хеші попередніх блоків, можна перевірити оригінальність ланцюга, коректність даних у кожному блоці та виявити підроблені блоки. Для досягнення угоди між учасниками щодо внесення змін до блокчейну використовуються алгоритми консенсусу, такі як proof-of-work (доказ виконання роботи) та proof-of-stake (доказ частки володіння). Доказ виконання роботи (PoW) захищає мережеві системи від зловживань, вимагаючи вирішення складних математичних завдань, які потребують обчислювальних ресурсів і часу, що забезпечує сильний захист від фальсифікацій. Хеш ідентифікатора блоку повинен задовольняти певну умову складності обчислень. Доказ частки володіння (PoS) є альтернативою PoW і заснований на доказі засобів, що шукаються, де блок із більшою ймовірністю записується обліковим записом з більшим балансом токенів.

В останні роки активно розвиваються децентралізовані цифрові валюти, основними перевагами яких є захищеність від втручання третіх осіб у фінансові системи та прозорість. Деякі дослідники шукали спосіб голосування та підрахунку голосів за допомогою технології блокчейн. У 2015 році Дж. С. Чеплач з IT Університету Копенгагена представив доповідь про сфери використання блокчейна, зокрема зазначаючи його можливості для електронного голосування. Того ж року З. Жао та Т. Чан запропонували метод голосування з використанням технологій блокчейн та zk-SNARK, який забезпечував конфіденційність, перевіряльність та незмінюваність. У 2016 році було запропоновано протокол з використанням Zerocoin для забезпечення більшості вимог електронного голосування. Також П. С. Джейсон та К. Ючі розробили протокол із застосуванням сліпого підпису та карт Біткоїн.

Недоліками системи голосування на базі Bitcoin є низька швидкість транзакцій через недостатню пропускну здатність мережі. Надмірна популярність криптовалюти призводить до накопичення черг транзакцій, що збільшує час їх обробки та вартість комісій. Ці проблеми ускладнюють ефективну реалізацію системи голосування на основі блокчейн. Технологія блокчейн, завдяки децентралізованості, реплікації бази даних між учасниками, незмінності даних та збереженню усіх транзакцій у вигляді ланцюжка блоків, має потенціал для використання в електронних системах голосування, усуваючи недоліки традиційних систем.

Висновки

Технологія блокчейн, завдяки децентралізованості, реплікації бази даних між учасниками, незмінності даних та збереженню всіх транзакцій у вигляді ланцюжка блоків, має потенціал для усунення недоліків електронного голосування. Проаналізовано різницю між паперовим та електронним голосуванням, основні принципи побудови децентралізованих мереж і технології блокчейн, а також вимоги до голосування із застосуванням блокчейн. За результатам аналізу розглянуто можливість підвищення достовірності системи електронного голосування у мережі блокчейн із захистом конфіденційності на основі смарт-контрактів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Block The Vote: Could Blockchain Technology Cybersecure Elections? [Електронний ресурс]. – Режим доступу: http://www.forbes.com/sites/realspin/2016/08/30/block-the-votecouldblockchain-technology-cybersecure-elections.

2. California: The Top to Bottom Review [Електронний ресурс]. – Режим доступу: http://www.votetrustusa.org/index.php?option=com_content&task=view&id =2554&Itemid=113.

3. IGS Votomatic Prototype Goes to the Smithsonian [Електронний ресурс]. – Режим доступу: https://web.archive.org/web/20070713201451/http://www.igs.berkeley.edu/publicatios/par/winter2001/votomatic.htm.

4. Kiwi. Bitcoin testnet sandbox. [Електронний ресурс]. – Режим доступу: https://testnet.manu.backend.hamburg/faucet.

5. NSW election result could be challenged over iVote security flaw [Електронний ресурс]. – Режим доступу: https://www.theguardian.com/australia-news/2015/mar/23/nsw-electionresult-could-be-challenged-over-ivote-security-flaw.

6. Peer-to-peer [Електронний ресурс]. – Режим доступу: https://bitcoin.org/bitcoin.pdf.

7. Slim. Middeware-slim. [Електронний ресурс]. – Режим доступу: https://www.slimframework.com/docs/v3/concepts/middleware.html.

8. State bans electronic balloting in 4 counties / Touch-screen firm accused of 'reprehensible,' illegal conduct [Електронний ресурс]. – Режим доступу: https://www.sfgate.com/politics/article/State-bans-electronic-balloting-in-4- counties-2784975.php.

9. Voting Machine Company Submits to Inquiry [Електронний ресурс]. – Режим доступу: https://www.nytimes.com/2006/10/31/us/politics/31vote.html?_r=1&oref=sl ogin.

10. Why machines are bad at counting votes [Електронний ресурс]. – Режим доступу: https://www.theguardian.com/technology/2009/apr/30/e-votingelectronic-polling-systems.

Гуменюк В'ячеслав Володимирович – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: hvv@vntu.edu.ua

Безпалий Кирило Валерійович – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: kyrylo.bezpalyi@vntu.edu.ua

Humeniuk Vyacheslav Volodymyrovych – associate assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: hvv@vntu.edu.ua

Bezpalyi Kyrylo Valeriovitch – associate assistant of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: kyrylo.bezpalyi@vntu.edu.ua