УДК 004.056.5 **DOI:10.30837/rt.2020.1.200.11**

І.Д. ГОРБЕНКО, д-р техн. наук, О.О. КУЗНЕЦОВ, д-р техн. наук,
М.О. ПОЛУЯНЕНКО, канд. техн. наук, А.С. КІЯН, К.Є. ЛИСИЦЬКИЙ, С.О. КАНДІЙ

ПРОТОТИПУВАННЯ ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ ЕЛЕКТРОННОГО БЛОКЧЕЙН-ГОЛОСУВАННЯ

Вступ

Для забезпечення захищеності інформаційних ресурсів, надійності їх розподіленого зберігання, розгортання децентралізованих систем управляння та різних за функціональним призначенням інформаційних сервісів та послуг застосовуються блокчейн-мережі [1 – 3].

Зазвичай технологія блокчейн застосовується у різних додатках [1]: для створення криптовалют та запрограмованих юридичних зобов'язань (смарт-контрактів); при побудові децентралізованих сховищ (електронні реєстри, кадастри, тощо) та систем електронних довірчих послуг (ідентифікація, голосування, інфраструктура відкритих ключів – ІВК, тощо). На сьогодні в світі вже існує понад 1100 видів цифрових грошей із загальною капіталізацією 133 мільярди доларів (за даними CoinMarketCap – Forbes). В Україні понад 100 приватних компаній та окремих проектів задіяно в індустрії блокчейну (за даними Асоціації Блокчейн України), 37 % з них – від українських інвесторів, 63 % – від іноземних інвесторів. За технологією блокчейн створено державний майданчик для онлайн аукціонів України OpenMarket (СЕТАМ), де Міністерство юстиції України продає арештоване і конфісковане майно [4].

Слід відзначити, що використання нової та неперевіреної часом технології зазвичай несе додаткові ризики та загрози. Зокрема, необхідно проводити експертні випробування з наступних питань:

- безпека технології блокчейн (правильність формування блоків, транзакцій та їх взаємодії);
- безпека транспортного рівня мережі блокчейн (правильність формування повідомлень при комунікації між вузлами мережі);
- безпека вузлів мережі блокчейн (правильність комунікації вузлів та коректність обробки помилок, що можуть виникати);
- безпека консенсусу (правильність роботи протоколів консенсусу та їх захищеність від існуючих та потенційних атак);
- безпека криптографічних модулей (правильність реалізації криптографічних перетворень).

Зазначені проблемні питання ускладняються через переважне застосування інформаційних технологій іноземного виробництва, експертні дослідження щодо яких не проводилися через їх складність та дороговизну.

Окремо слід зазначити можливість застосування найближчим часом квантових методів обчислення для реалізації існуючих та потенційних атак на різні компоненти блокчейн-систем. Зокрема, за прогнозами Національного інституту стандартів і технологій США в найближчі 5 – 10 років стануть доступними універсальні квантові обчислювачі, здатні проводити криптоаналіз практично всіх алгоритмів асиметричного шифрування, інкапсуляції ключів, електронного підпису, тощо [5 – 7].

Отже дослідження технології блокчейн, вивчення її складових, зокрема оцінка інформаційної та функціональної безпеки, прототипування децентралізованих систем, побудованих за цією технологією є безумовно важливим та актуальним завданням.

ПАТ «ІІТ» під керівництвом Департаменту захисту інформації Державної служби спеціального зв'язку та захисту інформації України проведено низку заходів щодо пошукових досліджень технології блокчейн, а також можливостей і напрямків її імплементацій у державній сфері. Досліджено можливість застосування блокчейн-систем при проведенні публічних опитувань, голосувань, референдумів, виборів; створення національної системи електронних

грошей (національної криптовалюти); використання запрограмованих юридичних зобов'язань (смарт-контрактів); відмовостійкого електронного документообігу, електронних реєстрів, кадастрів, тощо. У ході досліджень запропоновано ряд концепцій з використанням переваг блокчейн-технології щодо створення децентралізованих системи електронних довірчих послуг (ідентифікація, інфраструктури відкритих ключів, голосувань). Розроблено апаратно-програмний комплекс для досліджень функціонування реально діючих блокчейн-систем та на його базі розгорнуто прототип системи електронного голосування.

Мета статті – викладення окремих результатів з прототипування децентралізованої системи електронного блокчейн-голосування, дослідження інформаційної та функціональної безпеки, обґрунтування рекомендацій щодо подальшого впровадження в Україні.

Структура децентралізованої системи електронного блокчейн-голосування

Технологія блокчейн призначена для створення захищених цифрових реєстрів, стійких до несанкціонованого доступу. Інформація зберігається розподіленим способом (тобто без центрального сховища) та без центрального органу (наприклад, банку, компанії, або органу влади), при цьому унеможливлюються зміни в уже внесених в реєстр даних [1 – 3].

До безумовних переваги такої технології слід віднести наступні [1]:

– Блокчейн забезпечує історично стійке зберігання інформації. Окремі записи (блоки) зв'язується криптографічними перетвореннями, які унеможливлюють зміну жодного біту в уже внесених в реєстр даних;
– Децентралізація забезпечує надійність збереження інформації. Навіть за умови блокування, виходу із ладу або втрати керування над значною часткою вузлів мережі блокчейн цифрові реєстри не можуть бути змінені або втрачені;
– Криптографічні перетворення забезпечують безпеку інформації (цілісність, неспростовність, доступність та конфіденційність).

Отже, практичне впровадження технології блокчейн підвищує довіру до інформаційних ресурсів та сервісів (що є особливо актуальним для державних установ); зменшує час та накладні витрати; унеможливлює втручання центрального органу та відповідні корупційні дії; підвищує надійність збереження інформації та якість наданих послуг.

Для прототипування основних складових системи електронного голосування запропонована дворівнева архітектура, спрощена схема якої наведена на рис. 1.

Рис. 1. Спрощена архітектура децентралізованої системи електронного голосування

Децентралізована інфраструктура ідентифікації виборців (ДІ eID) має забезпечувати процедуру надійної ідентифікації користувачів та формування списків легітимних виборців. Вона складається із провайдерів послуг ідентифікації громадян (далі- IdP, провайдери). Необхідно забезпечити реалізацію процедури ідентифікації за допомогою:

- засобів BankID;
- засобів MobileID;
- електронного паспорта громадянина;
- цифрового (електронного) підпису:
- програмний носій цифрового підпису;
- апаратний носій цифрового підпису.

Відповідно до висунутих вимог, в ролі *IdP* можуть виступати:

- банківські установи;
- мобільні оператори;
- центри міграційної служби (центри надання адміністративних послуг – ЦНАП);
- центри сертифікації ключів національної системи ЕЦП.

Регламенти функціонування провайдерів встановлюються Законом України "Про електронні довірчі послуги" [8], імплементованим Регламентом ЄС [9] та іншими міжнародними та національними нормативними документами [10 – 12].

Вимоги та процедури ідентифікації залежать від конкретного провайдера.

Мережа провайдерів ідентифікації сформована поза межами децентралізованої системи електронного голосування. Кожен IdP має попередньо сформовану локальну базу даних своїх користувачів, яка містить їхні ідентифікаційні дані та, можливо, локальні ідентифікатори. Відповідальність за надійне збереження та коректне використання локальних баз даних покладається на IdP.

Для організації інфраструктури ідентифікації в рамках децентралізованої системи електронного голосування, IdP об'єднуються в окрему приватну мережу блокчейн (private permissioned Blockchain). В даній мережі кожен із IdP виступає вузлом-валідатором. Необхідно зазначити, що для такої мережі немає необхідності застосовувати складні та енергоємні протоколи консенсусу, оскільки мережа поєднує довірені («чесні») вузли.

Децентралізована інфраструктура для здійснення дистанційного волевиявлення та підрахунку голосів має забезпечувати процес дистанційного волевиявлення зареєстрованих (авторизованих) легітимних виборців та процес підрахунку голосів. Додатково в даній інфраструктурі повинні бути організовані процеси реєстрації кандидатів. Довіреними вузлами в даному випадку будуть виступати аналоги територіальних виборчих громад, проте завдяки децентралізованому підходу та технології blockchain наявність головного органу (центральної виборчої комісії) не потрібне. Така організація значно зменшує ризики, пов'язані із людським фактором, включаючи можливості підкупу членів центральної виборчої комісії.

Для організації інфраструктури дистанційного волевиявлення в рамках децентралізованої системи електронного голосування представництва відповідальних за проведення виборчого процесу, наприклад територіальні виборчі громади, (A1, A2,...,An), подібно до провайдерів ідентифікації, об'єднуються в окрему приватну мережу блокчейн (private permissioned Blockchain), в якій кожен із Ai виступає вузлом-валідатором – в сукупності вони являють собою децентралізоване Агентство (A). Аналогічно до верхньої мережі Blockchain, у нижній також немає необхідності застосовувати складні та енергоємні протоколи консенсусу, оскільки мережа поєднує довірені («чесні») вузли. Вузли-валідатори формують гаманці для легітимних виборців та проводять процедуру автентифікації виборців. Також вони відповідають за процес формування гаманців для альтернатив (кандидатів).

На рис. 1 наведено також відповідальні міністерства та відомства із зазначенням основних завдань та функцій при розгортанні децентралізованої системи електронного голосування.

Обрис прототипу системи електронного голосування

На сьогодні існує низка програмних рішень, що надають інструменти для розробки, розгортання та підтримки систем, заснованих на використанні технології блокчейн. Серед існуючих альтернатив для реалізації прототипу системи електронного голосування було обрано платформу Exonum [13, 14] з декількох причин.

По-перше, Exonum спроектовано таким чином, що система працює виключно на обчислюваних потужностях вузлів-валідаторів, які зацікавлені у її надійному функціонуванні. Такими вузлами-валідаторами у випадку електронного голосування є представники децентралізованого агентства. Кожний з них зберігає у себе копію стану бази даних, усі атомарні операції щодо якої, оформлені в блоки та формують Blockchain. Окрім того, система, побудована на Exonum, продовжує коректно функціонувати навіть у випадку компрометації чи відключення 2/3 вузлів-валідаторів системи, та унеможливлює підробку даних блокчейна шляхом змови вузлів за рахунок наявності процедури «Біткоінг-анкорінг», що регулярно відправляє зліпки стану системи в публічний блокчейн Біткоіна. Такий підхід дозволяє унеможливити наявність неправомірних дій зі сторони вузлів-валідаторів та попередити атаки на них.

По-друге, платформа Exonum надає високу продуктивність, що в сотні разів перевищує показники швидкодії її альтернатив, а саме забезпечується виконання до 5000 транзакцій в секунду із затримкою в 0,5 с. Така продуктивність є важливою характеристикою під час розробки системи електронного голосування, коли протягом одного дня усі громадяни мають здійснити доступ та волевиявлення у системі. Додатковою перевагою, що забезпечується Exonum, є тонкий клієнт, за рахунок якого кінцеві користувачі(виборці або спостерігачі) можуть перевірити наявність та коректність транзакцій.

По-третє, нині вже функціонують успішні проекти, реалізовані з використанням Exonum, не тільки у комерційному секторі, але і на державному рівні. Одним з таких прикладів є система реєстрації земельних ділянок у Грузії, реалізована сумісно компанією Bitfury та Національним агентством публічного реєстру Грузії. Використання Exonum у цьому випадку дозволило не тільки запобігти неправомірному оскарженню прав власності за рахунок видачі власникам цифрових сертифікатів їх активів, підкріплених криптографічними підтвердженнями (геш-значеннями), що публікуються у Blockchain та не можуть бути у подальшому змінені, але і значно зменшити часові та матеріальні затрати під час процесу реєстрації земельних ділянок.

Децентралізована процедура проведення виборчого процесу та підрахунку голосів є верхньою мережею розробленої дворівневої архітектури електронного голосування. Протокол голосування у подібній системі з функціональної точки зору складається з наступних етапів:

1. Формування списків легітимних виборців, тобто виборців, що мають право здійснювати волевиявлення у межах конкретного виборчого процесу.
2. Генерація гаманців легітимних виборців у системі голосування, що є необхідною умовою для подальшого їх доступу до системи.
3. Реєстрація кандидатів у децентралізованій системі голосування, інформація про яких попередньо пройшла перевірку спеціальними органами.
4. Автентифікація виборців при першому доступі до системи голосування системи, що полягає у зарахуванні на рахунок виборця одного голосу, який він зможе віддати на користь того чи іншого кандидата.
5. Здійснення волевиявлення у системі, після якого виборець вже не може змінити свій вибір.
6. Підрахунок голосів у системі голосування, що значно полегшує сучасний процес з точки зору використовуваного часу, матеріальних та людських ресурсів

Перший етап реалізується нижньою мережею архітектури, інші функціонують у верхній мережі, прототип якої було практично реалізовано. Таким чином у прототипі передбачено, що виборці пройшли попередню ідентифікацію у певного провайдера та володіють ключовою парою, відкритий ключ якої поступив до верхньої мережі і є деперсоналізованим іден-

тифікатором користувача у системі голосування. Загалом схему голосування можна уявити наступним чином (рис. 2).

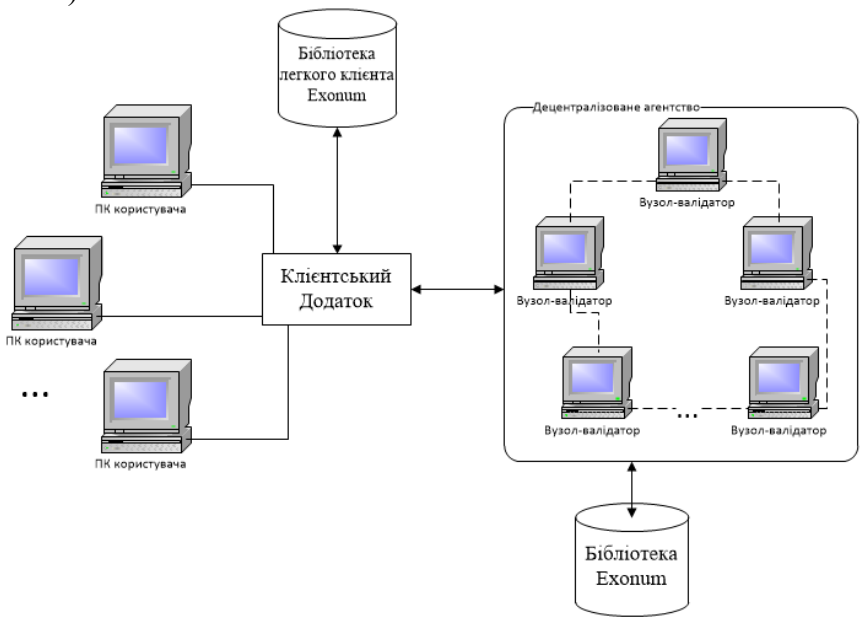

Рис. 2. Структурна схема прототипу електронного голосування

Логіка роботи системи реалізується за рахунок комплексного функціонування її чотирьох складових частин:

- клієнтського додатку;
- децентралізованого агентства;
- бібліотеки Exonum;
- бібліотеки легкого клієнта Exonum.

Бібліотеки Exonum та легкого клієнта Exonum зазначені на структурній схемі системи, оскільки мають принципове значення для реалізації функціонування програмного забезпечення. Бібліотека Exonum у складі системи забезпечує створення приватного Blockchain, вузлами якого є представництва децентралізованого агентства, чіткий регламент обробки транзакцій, який незалежно від кількості вузлів, не може бути змінено, забезпечення прозорості обробки транзакцій, що може бути продемонстрована третім сторонам, підписання транзакцій та інше.

Етап 2 – 6 описаного вище протоколу у прототипі представляє собою конкретний вид транзакції у системі, інформація про яку записується до Blockchain та не може бути у подальшому змінена. Відповідно, всього у системі наявні 4 типи транзакцій: реєстрація кандидата, реєстрація виборців, зарахування голосу на рахунок виборця при його першому вході до системи і перерахування голосу з рахунку виборця на рахунок кандидата під час здійснення волевиявлення. У свою чергу легкий клієнт Exonum надає інструменти формування та відправлення транзакцій до мережі Blockchain Exonum, що представлена децентралізованим агентством, та формування запитів до вузлів та перевірку їх відповідей.

Для коректного функціонування прототипу системи голосування через клієнтський додаток з системою взаємодіють три типи користувачів, яким надано конкретні повноваження:

1. Виборець: здійснює вхід до системи голосування; здійснює передачу голосу обраному кандидату; переглядає особисту інформацію кандидата.
2. Адміністратор: здійснює вхід до системи голосування; додає особисту інформацію кандидата до системи, створюючи йому особистий гаманець; отримує доступ до поточних результатів голосування; переглядає особисту інформацію кандидата; володіє інструментами для перевірки коректності транзакції у Blockchain.

3. Кандидат: не здійснює вхід до системи, оскільки його особистий ключ невідомий; отримує голоси від виборців.

Кожен користувач в системі має зареєстрований гаманець, ідентифікатором якого є його відкритий ключ. На етапі авторизації користувач у клієнтському додатку вводить свою ключову пару, і якщо гаманець з відповідним відкритим ключем наявний у системі, а секретний ключ відповідає відкритому (при цьому секретний ключ відомий лише користувачу, а його коректність перевіряється шляхом підписання контрольної фрази), отримує доступ до системи. При цьому, як було зазначено, ключова пара кандидата невідома ні одній зі сторін виборчого процесу, тому здійснити вхід до системи від його обличчя неможливо.

Після отримання доступу користувачем-виборцем системою здійснюється перевірка, чи брав він участь у виборчому процесі. Якщо виборець вже віддав голос за одного з кандидатів, його дії у системі обмежуються переглядом інформації про зареєстрованих кандидатів, у випадку якщо на його рахунку ще наявний голос, виборець може віддати його за обраного кандидата, ініціювавши при цьому транзакцію голосування, яка буде підписана його ключем і внесена до Blockchain.

У свою чергу користувач-адміністратор після отримання доступу до системи має право зареєструвати кандидата, заповнивши усю інформацію про нього та підписавши транзакцію про створення кандидата своїм ключем, переглянути кількість голосів відданих за кандидата, що відбувається шляхом отримання інформації про стан гаманця кандидата, переглянути реєстр Blockchain, а саме дані транзакцій, що записані до нього, їх статус, та ключ того, ким було ініційовано певну транзакцію.

Отже, клієнтський додаток забезпечує інтерфейс для взаємодії користувача та безпосередньо логіки функціонування системи. Він є проміжним елементом взаємодії децентралізованого агентства, діяльність якого побудована на використанні фреймворку Exonum та легкого клієнта Exonum. З цієї точки зору функціями клієнтського додатку є:

- ініціювання створення транзакції;
- ініціювання запиту на отримання даних.

Функціональна взаємодія клієнтського додатку, вузлів-валідаторів та легкого клієнта з метою створення транзакції продемонстрована на рис. 3.

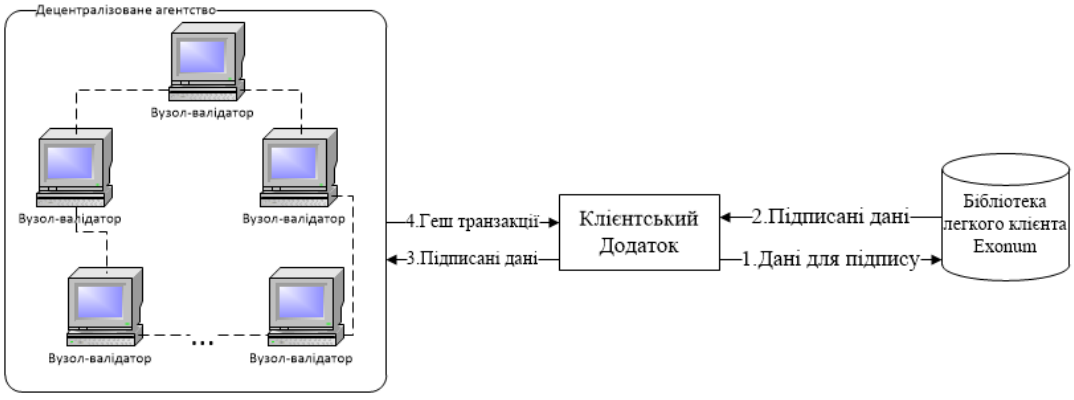

Рис. 3. Схема взаємодії складових системи в межах формування транзакції

Ініціювання створення транзакцій забезпечує виконання загальних функцій системи таких, як реєстрація виборця, голосування та реєстрація кандидатів у децентралізованій системі волевиявлення.

Відповідно ініціювання запиту на отримання даних підтримує авторизацію користувача у системі та підрахунок голосів, відданих на користь конкретного кандидата. Схема взаємодії клієнтського додатку, вузлів-валідаторів та легкого клієнта під час запиту даних продемонстрована на рис. 4.

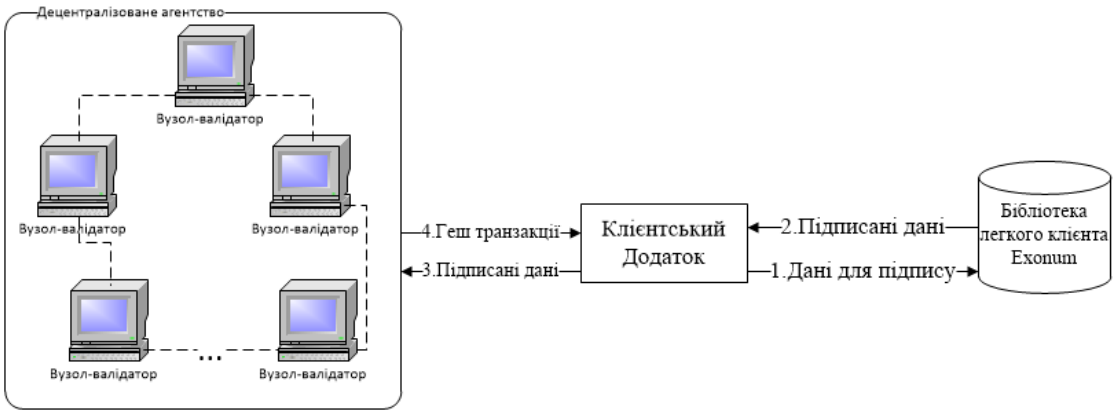

Рис. 4. Схема взаємодії складових системи в межах запиту даних

Таким чином, прототип уособлює основні процеси, які необхідні для організації виборчого процесу. При цьому кожна дія, що змінює стан Blockchain реєструється і не може бути спростована. Цей факт забезпечує гарантію незмінності вибору, єдиноразовість здійснення волевиявлення одним виборцем, а також зарахування голосів на рахунок кандидатів тільки від легітимних виборців.

Обґрунтування механізмів та протоколів безпеки технології блокчейн

Ключовим аспектом технології блокчейна є визначення того, хто з користувачів публікує наступний блок. Це вирішується шляхом реалізації однієї з багатьох можливих моделей консенсусу. В інклюзивних блокчейн-мережах зазвичай існує безліч вузлів публікації, що конкурують одночасно за публікацію наступного блоку. Вони зазвичай роблять це, щоб отримати винагороду за формування блоку та/або підтвердження транзакцій. Як правило, вони не довіряють користувачам, які можуть знати один одного тільки за їх публічними адресами. Кожен, хто публікує блок, швидше за все, мотивований прагненням до фінансової вигоди, а не добробутом інших вузлів публікацій або навіть самої мережі [1].

У такій ситуації навіщо користувачеві поширювати блок, який інший користувач намагається опублікувати? Крім того, хто вирішує конфлікти, коли кілька вузлів публікують блок приблизно в один і той же час? Щоб вирішувати ці протиріччя, технологія блокчейн використовує консенсусні моделі, щоб дозволити групі користувачів, які не мають взаємної довіри один до одного, працювати разом.

Консенсус є процедурою прийняття рішення. Його мета – забезпечити те, щоб всі учасники мережі погодили свій поточний стан після додавання нової інформації, блоку даних або пакета транзакцій. Іншими словами, консенсус-протокол гарантує те, що ланцюг вірний, і дає стимул учасникам залишатися чесними (тобто дотримуватися процедур визначених у системі). Це є важливим процесом, який запобігає ситуації, коли хтось контролює всю систему, і процедура консенсусу гарантує те, що всі учасники системи дотримуються правил мережі.

Коли користувач приєднується до блокчейн-мережі, він погоджується з початковим станом системи. Це записано в єдиному попередньо сконфігурованому блоці – генезис блоці. Кожна блокчейн-мережа має опублікований генезис блок, і кожен блок повинен бути доданий в блокчейн після нього на основі узгодженої моделі консенсусу.

Концептуально безпека блокчейн-технології ґрунтується на наступних властивостях:

- Узгоджений початковий стан системи. Це є єдиний попередньо сконфігурований блок – генезис блок.
- Користувачі погоджуються з консенсусною моделлю, на основі якої блоки додаються в систему та оновлюється її поточний стан.
- Кожен блок пов’язаний з попереднім блоком шляхом включення криптографічного геш-значення попереднього заголовку блока (за винятком першого генезис-блоку, який не має попереднього блоку).

- Об’єктивність. Для визначення поточного стану системи не потрібна довіра авторитетним джерелам – корінь довіри знаходиться в самому блокчейні та у використанні криптографічно надійних функцій – користувачі можуть перевірити кожен блок самостійно.

Незалежно від моделі консенсусу, кожен блок повинен бути дійсним і, отже, може бути перевірений незалежно кожним користувачем блокчейн-мережі. Використовуючи початковий стан та можливість перевірки кожного блоку, користувачі можуть незалежно та самостійно узгодити поточний стан блокчейн-системи.

У табл. 1 наведено основних виділені ідей [2], які можуть / повинні (в залежності від поставлених завдань та вибраних шляхів реалізації) бути закладені в механізми консенсусу.

Таблиця 1

Основні чинники механізмів консенсусу у блокчейн-системах

Послуги / показники	**Визначення**
Децентралізоване управління	Єдиний центральний орган не може забезпечити завершеність транзакції.
Структурованість взаємовідносин	Вузли обмінюються повідомленнями заздалегідь визначеними способами, які можуть включати етапи або рівні.
Автентифікація	Процес надає засоби для перевірки особи учасників.
Цілісність	Забезпечення перевірки цілісності транзакції (наприклад, математично за допомогою криптографічних геш-функції).
Неспростовність	Надаються засоби для перевірки того, що передбачуваний відправник дійсно відправив повідомлення
Конфіденційність	Конфіденційність гарантує, що тільки визначений одержувач може прочитати повідомлення.
Відмовостійкість	Мережа працює ефективно і швидко, навіть якщо деякі вузли, сервери або інші компоненти мережі виходять з ладу або працюють неналежним чином.
Продуктивність	Враховує пропускну здатність, життєздатність, масштабованість та затримку.

В межах цих ідей існують значні відмінності між різними механізмами консенсусу. Ряд перерахованих вище параметрів реалізується за допомогою основних методів криптографії, які використовують математичні функції для забезпечення безпеки і конфіденційності. Ці методи включають симетричне і не симетричне шифрування і геш-функції.

Ключовою особливістю блокчейн-технології є те, що немає необхідності в тому, щоб довірена третя сторона надавала стан системи – кожен користувач у системі має все необхідне, щоб власноруч, з деякого доступного набора станів визначитися з поточним станом та перевірити цілісність системи.

Щоб додати новий блок в блокчейн-систему, всі вузли з часом повинні прийти до спільної згоди, проте деякі тимчасові розбіжності можливі.

В блокчейн-мережах модель консенсусу повинна працювати навіть у присутності, можливо, недобросовісних користувачів (тобто таких, які навмисно або ненавмисно недотримуються визначених у системі процедур), оскільки ці користувачі можуть спробувати порушити або спотворити ланцюжок блоків.

Звернемо увагу на те, що технологія блокчейн не є механізмом, який безумовно гарантує цілісність та справжність даних у блокчейн-мережі, технологія блокчейн лише надає механізм для виявлення таких маніпуляцій з даними у системі.

У деяких блокчейн-мережах може існувати деякий рівень довіри між вузлами публікації. В залежності від рівня цієї довіри може знадобитися узгоджена модель ресурсномістких процесів (час обчислень, інвестиції тощо) щоб визначити який учасник додає наступний блок до ланцюжка. Як правило, в міру підвищення рівня довіри зменшується потреба у використ-

танні ресурсів в якості міри формування довіри. Для деяких ексклюзивних блокчейн реалізацій уявлення про консенсус виходить за рамки забезпечення достовірності блоків, але охоплює всі системи перевірок від пропозиції транзакції до її остаточного включення в блок.

Варто відзначити, що завдання розподіленого консенсусу не специфічна для блокчейн систем і має добре перевірені рішення для багатьох інших розподілених систем. Навіть завдання консенсусу, в якому вузли можуть бути недобросовісними, – завдання візантійського консенсусу – вперше була сформульовано в 80-х роках минулого століття, а методи його вирішення з'явилися в кінці 90-х.

Як і всі розподілені системи, реалізація блокчейна пов'язана з низкою проблем – затримка в мережі, помилки при передачі, помилки в програмному забезпеченні, лазівки в системі безпеки та хакерські погрози, що впливає на її масштабованість, ефективність і безпеку. Більш того, децентралізований характер технології передбачає, що жодному з учасників системи не можна довіряти. Можуть з'явитися шкідливі вузли, а також різниця в даних через суперечливість інтересів. Для протидії вказаним проблемам існують кілька базових моделей консенсусу. Умовно всі моделі консенсусу можна розділити на декілька основних типів зображених на рис. 5.

Пошук методу досягнення консенсусу, без довіри між учасниками в розподіленому середовищі, який може масштабуватися необмеженим лінійним способом та був би надійним, триває і досі.

Консенсуси, засновані на доказах, працюють з тим припущенням, що учасники мережі будуть витрачати фінансові ресурси, щоб отримати прийняття рішення про вибір наступного блоку. Унікальність цих алгоритмів в тому, що вони економічно стимулюють вузли до певної фінансової участі для отримання можливості отримати винагороду за блоки. Ці моделі консенсусу роблять протоколи стійким за своєю природою до атак Сивіли. При цьому відпадає необхідність в Інфраструктурі Відкритих Ключів або інших схемах автентифікації.

Будь-яка з децентралізованих систем повинна мати стимул для підтримки свого існування учасниками цієї системи. Як правило, в ролі стимулу виступає матеріальна зацікавленість, що характерно для інклюзивних систем і для ексклюзивних систем, спрямованих на фінансову сферу. Як «стимул» участі може бути адміністративний ресурс, який зобов'язує учасників підтримувати функціонування блокчейн-систем. І якщо в другому випадку кількість учасників і їх можливості в підтримці роботи блокчейн-мережі визначаються і обмежуються обсягом фінансування, то в першому визначаються їх вигодою, що тягне за собою ризики пов'язані з монополізації децентралізованої системи.

Крім того, з ростом розміру блокчейна зростають вимоги до сховища, пропускної здатності та обчислювальної потужності, що застосовуються до повноправних вузлів мережі. У певний момент система стає досить громіздкою, у якої повноправно функціонувати можуть лише деякі вузли, які можуть дозволити собі ресурси для обробки блоків – що призводить до ризику централізації.

Розглядаючи більш детально життєві цикли блокчейн-систем, що мають фінансову стимуляцію підтримки свого існування, бачимо, що нарощування вливання в блокчейн систему її учасника призводить до збільшення прибутку цього учасника, що стимулює його до максимального нарощування частки своєї участі в блокчейн-системі. Для блокчейн-систем, побудованих на механізмах консенсусу, в основі яких лежить виконання трудомісткого завдання, це виражається в закупівлі та побудові дорогих ферм на спеціалізованому високопродуктивному обладнанні; якщо розглядати механізми консенсусу, засновані на частці володіння, – виражається в прямому вливанні фінансових ресурсів; при використанні BFT протоколів консенсусу – створення додаткової кількості учасників (які, як правило, вимагають певного фінансування); інші алгоритми консенсусу, також засновані на матеріальному або нематеріальному фінансовому забезпеченні, що при проектуванні блокчейн-мереж повинно обмежувати участь окремого представника і залучати якомога більше незалежних учасників. Однак постійне експоненціальне збільшенням фінансових вливань призводить до експоненціально-

го збільшення складності (вартості) участі в підтримці консенсусу, що призводить до витіснення з системи «слабких» учасників або стимулює їх до об'єднання в великі пули (з втратою можливості самостійного контролю блокчейн-мережі).

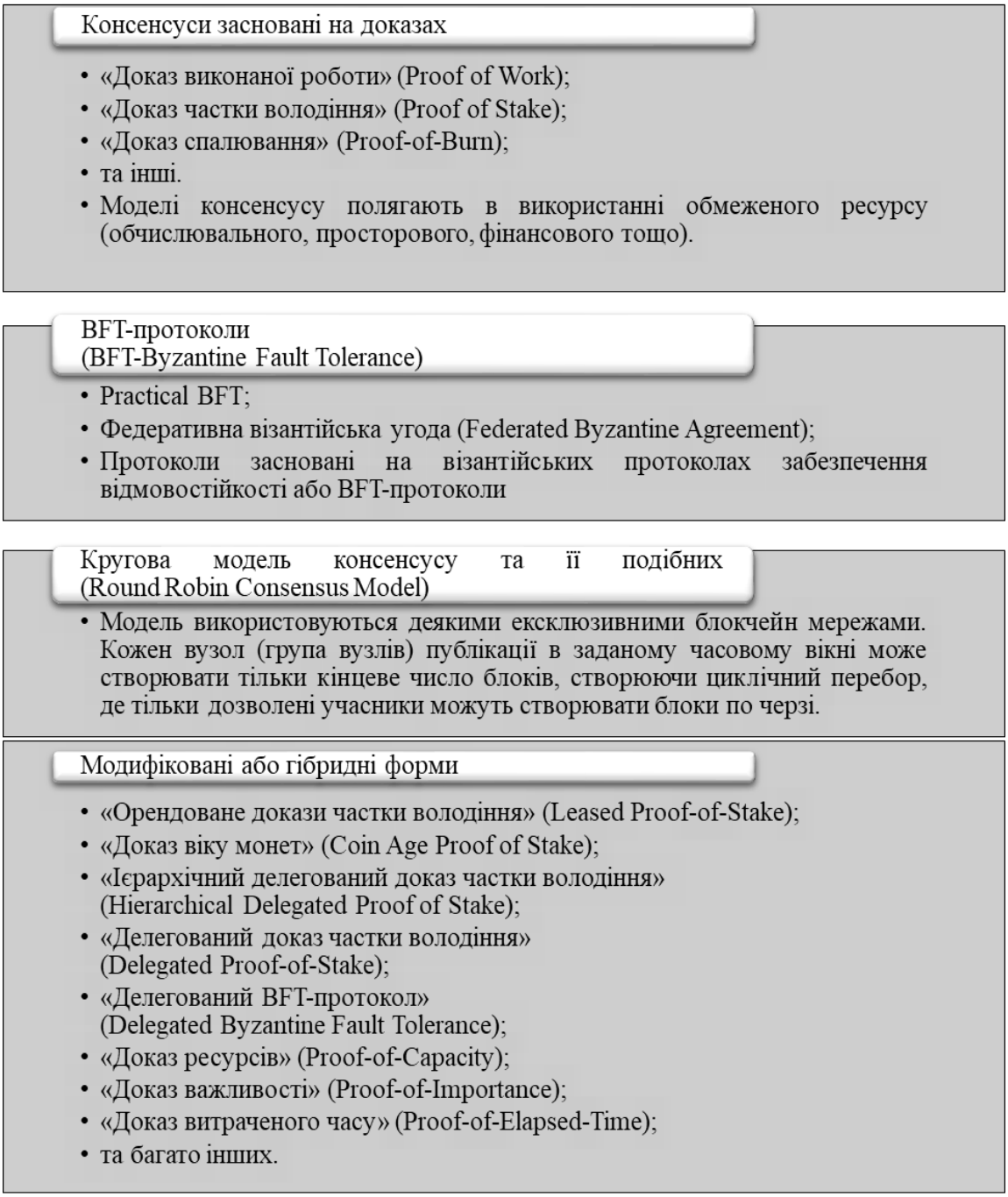

Рис. 5. Найпоширеніші моделі консенсусу

Таким чином, замість децентралізованої блокчейн-мережі з досить великою кількістю незалежних учасників (змова між якими практично виключена) в мережі починають домінувати кілька великих пулів або монополій, кількість яких складають одиниці. У даних умовах об'єднання великих гравців стає простим завданням, а з огляду на їх загальний інтерес в фінансову вигоду – практично неминучі.

Якщо ж об'єднання учасників блокчейн-системи не відбувається, але при цьому складність (вартість) участі в ній стає дедалі більше – система починає втрачати учасників, яким стає не вигідно підтримувати її функціонування. В результаті в системі залишається обмеже-

не вузьке коло, що має інші причини крім фінансових в підтримці роботи алгоритмів консенсусу, або блокчейн-система «гине».

В обох випадках, блокчейн-системи, побудовані за принципом фінансової зацікавленості учасників в підтримки роботи її механізмів консенсусу, схильні до високого ризику централізації її управління, що неминуче призводить до втрати довіри до блокчейн-системи як до незалежного та децентралізованого механізму.

На відміну від інклюзивних мереж ексклюзивні блокчейн-мережі дозволяють адміністративним шляхом впливати на саму можливість брати участь в підтриманні функціонування системи або впливати на фінансову вигоду кожного з учасника і тим самим забезпечувати необхідну кількість учасників гарантуючи малу ймовірність їх взаємної змови. Але при цьому необхідні достатні фінансові витрати адміністратора мережі – на фінансову зацікавленість участі сторонніх учасників у підтримці консенсусу мережі або на забезпечення призначених учасників всім необхідним для виконання своїх функцій.

У таких ексклюзивних блокчейн-мережах адміністратор має всі можливості прямо або побічно впливати на прийняття рішення цієї «децентралізованої» системи. У зв'язку з чим не рекомендується участь в блокчейн-системах сторонніх організацій для ведення та документування своїх будь-яких операцій, без повної довіри до цієї третьої сторони.

З іншого боку, такі ексклюзивні блокчейн-системи ідеально підходять для ведення та контролю операцій всередині певного кола суб'єктів взаємодії, де є недовіра між собою або необхідна можливість повного аудиту проведених операцій. У таких випадках в реєстрі блокчейн-системи заносяться всі операції і дані, необхідні для його аудиту, та по принципам побудови блокчейн-ланцюга заносяться до реєстру за участю всіх зацікавлених суб'єктів взаємодії включаючи сторони, які беруть участь в аудиті.

Резюмуючи наведене, враховуючи необхідність організації публічної колективної демократії, з дотриманням всіх вимог безпеки її проведення, необхідно застосовувати ексклюзивні блокчейн-системи з використанням BFT-протоколів консенсусу. Причому до вузлів публікації повинна бути залучена необхідна, але обмежена, кількість незалежних учасників (спостерігачів, незалежних громадських об'єднань). Їх кількість обмежується принципами неможливості вплинути на процеси формування реєстру блокчейн-мережі, але при цьому залишає факт фіксації їх участі в перевірці та підтвердженні кожного сформованого блоку, що надалі виключить будь-яку можливість маніпулювання з блокчейн-реєстром власником системи.

Доступ до реєстру повинен бути організований з дотриманням публічності та прозорості, що надасть можливість реалізувати основну перевагу блокчейн-технології – кожен користувач зможе особисто провести підрахунок голосів та переконатися у легітимності результатів голосування.

Обґрунтування механізмів та протоколів криптографічного захисту інформації

Криптографія як наука з'явилася, перш за все, для забезпечення конфіденційності інформації. З розвитком технологій стало зрозуміло, що криптографічні методи можуть бути застосовані для надання інших послуг, таких як забезпечення цілісності пакетів, неспростовності отримання інформації, автентифікації користувачів, тощо. Більш того, сучасний світ важко уявити без електронних цифрових підписів, направленого шифрування та кодів автентифікації повідомлень, на базі яких будуються численні криптографічні протоколи, що становлять основу для інформаційно-комунікаційних систем. Задача побудови надійної системи електронного голосування є гарним прикладом проблеми, що стимулює розвиток нових криптопримітивів для синтезу відповідних протоколів. Розглянемо основні вимоги до протоколів електронного голосування:

- Анонімність. Ніхто не має зв'язувати волевиявлення виборця з його особистістю.
- Валідація виборчих бюлетенів. Система повинна відрізняти валідні бюлетені від зіпсованих. Наприклад, коли виборець віддав свій голос за декількох кандидатів.

- Ідентифікація виборців. Система повинна запобігати спробам проголосувати декілька разів або спробам проголосувати за іншого виборця.
- Відкритість. Незалежні аудитори повинні мати змогу перевірити коректність даних.

На перший погляд вимоги суперечать одне одному, але це не так. Для реалізації послуги забезпечення анонімності зручно використати механізми гомоморфного шифрування. Гомоморфне шифрування є криптографічним примітивом, який дозволяє виконувати обчислення над шифротекстами таким чином, щоб після розшифрування результат співпадав з аналогічними обчисленнями над відкритими текстами. Припустимо, що є два відкритих тексти в форматі цілих чисел – m_1 і m_2. Тоді схема вважатиметься гомоморфною по відношенню до операції додавання, якщо сума шифротекстів $Enc(m_1)$ і $Enc(m_2)$ буде дорівнювати сумі відкритих текстів після розшифрування, тобто виконуватиметься рівність

$$Dec(Enc(m_1)+Enc(m_2))=m_1+m_2\ . \tag{1}$$

Тобто, виборець може зашифрувати свій голос та відправити до виборчої дільниці, на якій з застосуванням операції гомоморфного складання відбудеться підрахунок голосів. При цьому, зміст голосу не буде відомий дільниці, оскільки він зашифрований. Як буде показано далі, для забезпечення інших послуг, на схему гомоморфного шифрування накладаються більш складні вимоги, ніж підтримка операції гомоморфного складання. У загальному випадку потрібна можливість обчислювати досить велику кількість різноманітних математичних операцій над шифротекстами.

Криптосистеми, які можуть обчислювати над шифротекстами будь-які операції, називаються повністю гомоморфними. Тривалий час не вдавалося побудувати такі системи, проте у 2009 році американським криптологом G. Gentry була розроблена перша така система. З тих пір напрямок гомоморфного шифрування отримав поштовх для розвитку. Цікавим є те, що математичні перетворення, які застосовуються у найкращих сучасних повністю гомоморфних системах, належать до класу криптографії на гратках (lattice-based cryptography), яка при певному виборі загальносистемних параметрів є стійкою до атак на квантових комп'ютерах. Нещодавно прийнятий стандарт направленого шифрування та інкапсуляції ключів ДСТУ 8961:2019 також базується на стійкості проблем в теорії граток та може бути адаптований для випадку повністю гомоморфного шифрування.

Для валідації бюлетенів можливо застосувати докази з нульовим розголошенням. Доказ з нульовим розголошенням є протоколом, у якому одна сторона доводить іншій певне твердження, при цьому не розголошуючи інформації про це твердження. Наприклад, виборець хоче довести дільниці, що його гомоморфно зашифрований голос є валідним, при цьому не надаючи жодної інформації про вміст шифротекста. Для простоти викладення представимо, що голос є набором з N чисел, що належать множині $\{0,1\}$, де всі числа є нулями, а i-те число є одиницею та відповідно позначає номер кандидата, за якого проголосував виборець. Тобто валідними голосами будуть всі набори вигляду

$$\begin{aligned}&(1,0,0,...,0,0)\\&(0,1,0,...,0,0)\\&(0,0,1,....,0,0)\\&...\\&(0,0,0,...,1,0)\\&(0,0,0,...,0,1)\end{aligned} \tag{2}$$

Шляхом нескладних математичних обчислень можливо довести, що голос, представлений набором цілих чисел $a=(a_1,a_2,...,a_N)$, належить до множини голосів (2), якщо виконується рівність

$$f(a) = \sum_{i=1}^{N} (a_i^2 - a_i)^2 + (\sum_{i=1}^{N} a_i)^2 = 1 \qquad (3)$$

Якщо гомоморфно провести всі обчислення, то задача доказу валідності голоса зводиться до доказу того, що у отриманому шифротексті після обчислення $f(a)$ буде одиниця. Для вирішення цієї задачі існують різні протоколи. Для сучасних схем гомоморфного шифрування є перспективним підходи на основі схеми Фіата – Шаміра з перериваннями (Fiat – Shamir With Aborts), але детальний їх розгляд виходить за межі цієї статті.

Однією з послуг, що надається електронним цифровим підписом є ідентифікація користувача, або групи користувачів, яка володіє секретним ключем, на якому було вироблено підпис. Цей принцип можливо використати для забезпечення вимоги ідентифікації виборців. Якщо кожен виборець має свій секретний ключ, то до голосу і доказу валідності можливо додати підпис, який однозначно ідентифікує користувача.

В Україні розгорнута інфраструктура відкритих ключів, активно розвиваються такі технології, як MobileID та SmartID. Для організації виборів доцільно використовувати ресурси цих, вже існуючих систем. Узагальнена модель голосу виборця наведена на рис. 6.

Рис. 6. Узагальнена модель бюлетеня для системи електронного голосування

Оскільки всі голоси є гомоморфно зашифрованими, то незалежні аудитори можуть провести всі обчислення незалежно від ЦВК і після завершення виборів перевірити результати, чим забезпечується відкритість голосування. В залежності від інших вимог у модель бюлетеня можуть вноситися зміни, наприклад, для збору статистики по окремим регіонам.

Окрім цього, в зв'язку зі збільшенням кількості кібератак в світі виникає потреба в побудові надійної інфраструктури, яка буде зберігати та оброблювати данні виборців. Технологія блокчейн дозволяє будувати надійні розподілені інформаційні системи, функціонування яких можливе навіть якщо 49 % інфраструктури пошкоджено зловмисниками. Такі властивості забезпечуються за допомогою великої кількості криптографічних примітивів, які узгодженим чином формують надійні протоколи.

Сам блокчейн є спеціально сформованою базою даних, яка зберігає транзакції. До кожної транзакції, спрощено кажучи, додається електронний цифровий підпис. Наприклад, у випадку електронного голосування це може бути підпис на закритому ключі виборчої дільниці, до якої надійшов голос. Це унеможливлює "вкидування голосів" від третіх сторін. Транзакції групуються у блоки. Кожен блок містить геш-значення від усіх транзакції у ньому, сформований за допомогою дерева Меркла. Це забезпечує цілісність блока. На рис. 7 схематично наведена структура блоків.

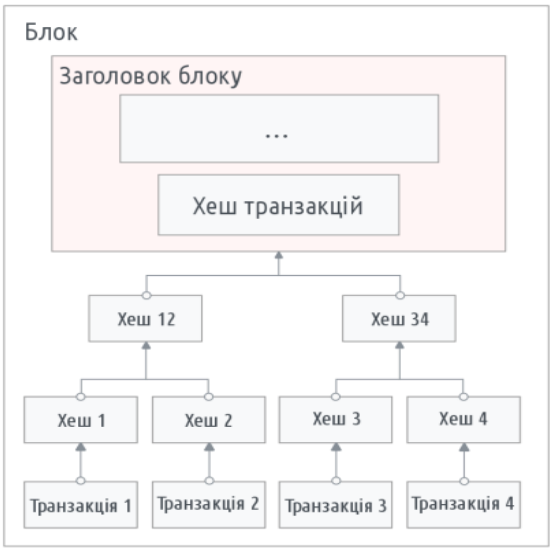

Рис. 7. Узагальнена структура блока в блокчейні

Окрім цього, до блока додається геш-значення від попереднього блока, тим самим створюється ланцюг блоків. Зрозуміло, що змінити данні, що зберігаються в якомусь блоці, дуже важко, оскільки доведеться коригувати усі блоки.

Блокчейн є децентралізованою структурою. Кожен з вузлів містить повні або часткові копії даних, що зберігаються на інших вузлах. Для забезпечення безпечної комунікації між окремими вузлами використовуються складні протоколи, розгляд яких виходить за межі цієї статті. Зазначимо лише, що для реалізації цих протоколів, окрім згаданих вище, в більшості випадків вимагається наявність блочних та/або поточних шифрів. Тож, виникає задача вибору криптопримітивів для функціонування блокчейн-системи.

В Україні запроваджено ряд стандартів у галузі криптографічної діяльності. Розглянемо деякі з них.

ДСТУ 4145-2002 є стандартом електронного цифрового підпису. Він ґрунтується на перетвореннях у групі точок еліптичних кривих над полями Галуа $GF(2^m)$. Схема підпису схожа на ECDSA (міжнародний стандарт підпису), проте не потребує операції взяття зворотного елемента в полі, що дозволяє швидше виробляти та перевіряти підпис. Стандарт дозволяє проводити обчислення як в поліноміальному базисі, так і у оптимальному нормальному базисі. ДСТУ 4145-2002 є основним видом підпису для державної інфраструктури відкритих ключів та навіть застосовується в системах, у яких циркулює інформація з обмеженим доступом, що становить державну таємницю. Надійність та ефективність ДСТУ 4145-2002 підтверджена численними дослідженнями як українських, так і зарубіжних криптологів.

ДСТУ 7624-2014 є стандартом симетричного блочного шифрування. Визначає rijndael-подібний блочний шифр “Калина”. Калина забезпечує нормальний, високий і надвисокий рівні стійкості, із довжинами блока і ключа 128, 256 і 512 бітів. Стійкість rijndael-подібних шифрів підтверджена часом. До того ж, у Калині значно покращені показники безпеки. Лінійний та диференційний криптоаналіз є неефективним вже при п’яти ітераціях. В рамках консервативного і прозорого підходу до проектування блокового шифру, шар нелінійного перетворення циклової функції реалізований на базі S-блоків. Розмір S-блоку був обраний виходячи з можливості ефективної реалізації на процесорах загального призначення. Шифр, на відміну від міжнародного стандарту AES, орієнтований на 64-бітні системи, що дозволяє отримати кращі результати на сучасних платформах. Обчислення гарно розпаралелюються за допомогою AVX2, NEON та інших наборів SIMD інструкцій. Стандарт підтримує 10 режимів роботи, які дозволяють гнучко використовувати шифр для різних призначень, серед яких є унікальні режими, характерні тільки для Калини.

ДСТУ 7564-2014 є стандартом гешування. Визначає ітеративну криптографічну геш-функцію “Купина”. Купина за структурою є SPN-мережею. Результатом роботи геш-функції є бітова послідовність від 8 до 512 біт. Така гнучкість є особливістю стандарту. Основними режимами роботи, рекомендованими до застосування, є «Купина-256», «Купина-384» і «Купина-512». Геш-функція, як і блочний шифр Калина, мають високі показники стійкості до лінійного та диференційного криптоаналізу, оскільки при розробці особлива увага приділяється криптостійкості.

ДСТУ 8845-2019 є новим стандартом потокового шифрування. Шифр має високу пропускну здатність до 17 Гб/с. Дизайн шифру схожий на міжнародний потоковий шифр SNOW-2, але значно покращений. Криптосистема орієнтована на 64-бітні системи. Також збільшені довжини ключа та вектору ініціалізації, що дозволяє захиститися від атак на квантовому комп’ютері, таких як алгоритм Гровера. Окрім того, шифр забезпечує зв’язок між окремими елементами шифропослідовностей, що значно підвищує стійкість до нав’язування помилкових символів та режимів роботи.

Тож, Україна має всі необхідні криптографічні стандарти для побудови надійних блокчейн-систем для електронного голосування.

Обґрунтування механізмів та протоколів безпеки комп’ютерних мереж, вузлів та інфраструктури

Обґрунтування безпеки комп’ютерних мереж, вузлів та інфраструктури системи електронного голосування на основі Blockchain базується на основі оцінки захищеності (вразливостей) стосовно існуючих та потенційних атак, спрямованих на порушення безпеки

Вимоги захищеності зазвичай обґрунтовуються через забезпечення цілісності та неспростовності (авторства) інформації стосовно існуючих та потенційних атак, спрямованих на порушення безпеки. Неповний перелік вимог до механізмів та протоколів безпеки комп’ютерних мереж, вузлів та інфраструктури представлено в табл. 2. При цьому розглядалася модель блокчейн-системи, яка функціонує із застосуванням технології Exonum, що вже є впровадженою в Україні. В таблиці наведено загальний опис вразливостей, мета та спосіб моделювання існуючих та потенційних атак (або перевірки на відповідність реалізації).

Таблиця 2

Перелік вимог, вразливостей та способів їх моделювання

Вимоги	Реалізація вимоги	Перевірка вимогам
BFT-протокол забезпечує надійну роботу навіть в ненадійних мережах за умови, що більше 2/3 вузлів облікової системи є чесними. При зменшенні цієї частки блокчейн-система втрачає працездатність.	Встановлення найменшої кількості (або частки) діючих вузлів валідаторів, за якої система буде забезпечувати надійну роботу. Встановити, як система реагує на «злочинні» дії вузлів-валідаторів, тобто такі дії, за яких вузол повідомляє хибну інформацію.	Шляхом навмисного зменшення кількості діючих вузлів-валідаторів моделюється умова, за якою частка працездатних (чесних) вузлів облікової системи менша за 2/3.
BFT протокол консенсусу є ефективним у системах з низькою затримкою, але дуже чутливий до кількості вузлів і пропускної здатності, так як одне повідомлення генерує безліч інших запитів і перевірок. Якщо використовувати велику кількість вузлів, то відбувається стрімке зростання кількості повідомлень і дуже велике зростання навантаження на мережу. В останньому	Встановлення залежності між пропускною здатністю системи та кількістю вузлів-валідаторів. Встановити поріг сталого функціонування системи Exonum при збільшені вузлів валідаторів.	Шляхом масштабування (зміни кількості) вузлів-валідаторів моделюється робота блокчейн-мережі у різних режимах.
	Встановлення залежності між ненадійністю у роботі каналів зв’язку та працездатністю блокчейн-системи. Необхідно встановити поріг сталого функціонування системи Exonum	Шляхом зміни затримок у каналі зв’язку (через короткотермінову зупинку окремих вузлів) моделюється зменшення загальної пропускної здатності системи.

Вимоги	Реалізація вимоги	Перевірка вимогам
випадку протокол працює неефективно.	при збільшені часу обміну між вузлами валідаторів (загублення пакетів даних, низька пропускна спроможність каналу зв'язку, збільшення часу обміну даними між вузлами).	
В базовому варіанті Practical BFT протоколу передбачається наявність лідера, що може стати точкою DoS-атаки для зупинки роботи облікової системи зловмисником. Оскільки є «лідер», що відправляє всім транзакції для підтвердження. Вимога стійкість системи до DoS-атак.	Встановлення максимальної кількості, повідомлень при яких вузол-валідатор зберігає своє стале функціонування.	Максимальна кількість повідомлень, при яких вузол-валідатор зберігає своє стале функціонування, виходить за межі обчислювальних ресурсів, якими володіє комплекс. Отже моделювання цієї вразливості в комплексі не реалізоване.
Стійкість розподілених систем Exonum до віддалених атак, оскільки їх компоненти використовують відкриті канали передачі даних.	Виконання основних вимог через перевірку неможливості проведення ефективних віддалених атак	Встановлення умов, які потрібні для здійснення атак. Перевірка через аудит початкових кодів (реалізовані протоколи передачі даних забезпечують захист від віддалених атак).
Відсутність помилок в реалізації протоколу BFT блокчейн-мережа які допускають порушення безпеки.	Відповідність реалізації протоколу BFT наданої документації.	Перевірка через виконання тестів внутрішніх програмних компонентів (ВПК) Exonum та аудиту початкових кодів (реалізований протокол BFT повинен відповідати наданій документації).
Зберігання особистих ключів від компрометації та / або модифікації конфігураційних файлів вузлів-валідаторів.	Встановлення наявних механізмів захисту особистих ключів та конфігураційних файлів вузлів-валідаторів від несанкціонованого доступу.	Перевірка через виконання тестів ВПК Exonum та аудиту початкових кодів (реалізовані механізми захисту особистих ключів та конфігураційних файлів вузлів-валідаторів повинні виключати можливість несанкціонованого доступу).

Проведення випробувань щодо рівня захисту від актуальних атак на Blockchain-платформи включає встановлення:

1. надійності роботи у ненадійних мережах;
2. надійності системи при масштабуванні кількості вузлів-валідаторів;
3. надійності системи при ненадійній роботі каналів зв'язку;
4. можливості захисту системи від віддалених атак;
5. відповідності реалізації протоколу BFT;
6. можливості віддаленого несанкціонованого доступу (компрометація особистих ключів) та / або модифікації конфігураційних файлів вузлів-валідаторів.

Розглянемо ці випробування більш докладно.

Встановлення надійності роботи у ненадійних мережах. Дослідження безпеки здійснюється шляхом моделювання блокчейн-мережі із порушеннями в роботі окремих вузлів. Зокрема моделюються випадки, коли доля ненадійних вузлів перевищує частку, достатню для правильної роботи системи.

Встановлення надійності системи при масштабуванні кількості вузлів-валідаторів. В мережі з великим числом вузлів в каналі зв'язку превалюють повідомлення із неприйняттям консенсусом або повторною спробою. Завдяки зростаючим затримкам та переповненості каналу зв'язку більшість вузлів очікують або виводять повідомлення про те, що власна висота блока нижче ніж висота блока більшості вузлів. Робота мережі характеризується нерівномірною швидкістю прийняття блоків. Середня швидкість знижується на 30 – 40 % відсотків. При відключенні вузлів кількістю від 1/3 від загальної значно збільшується кількість повідомлень про відмову з'єднання. Це погіршує швидкодію, загострюються відрив між вузлами по висоті блока, збільшуються перерви на очікування вузлів, що відстали.

Встановлення надійності системи при ненадійній роботі каналів зв'язку. Моделюється система із оцінкою швидкості прийняття блоків у залежності від загальної кількості валідаторів, збільшуючи процент зупинених вузлів. Встановлюються кількісні показники співвідношення між працюючими та зупиненими вузлами.

Встановлення відповідності реалізації протоколу BFT. BFT-протокол забезпечує надійну роботу навіть в ненадійних мережах за умови, що більше 2/3 вузлів системи є чесними, тобто діють за протоколом. Для прийняття консенсусу на одному раунді відбувається попереднє голосування, поріг для прийняття консенсусу – це отримання щонайменше +2/3 попередніх голосів щодо визначеного раунду та геша, щодо яких встановлюється консенсус.

Встановлення можливості віддаленого несанкціонованого доступу (компрометація особистих ключів) та / або модифікації конфігураційних файлів вузлів-валідаторів. У ситуації, коли вузол симулює неправильні адресу або порт при підписанні транзакцій на неправильному ключі, виникає помилка, консенсус не досягнуто, система не приймає підписані транзакції на неправильному ключі. При моделюванні спроб неправильної конфігурації ключів не вдалося запустити мережу, тобто обійти встановлений протоколом захист. При зміні адреси іншого вузла не вийде досягнути з'єднання. Це запобігає довільному приєднанню чужих вузлів. Також команда запуску ноди потребує знання паролю pass, який ніде не зберігається у відкритому вигляді. Таким чином, команда має захист від несанкціонованого запуску вузла, навіть якщо приватним ключем володіє неуповноважений користувач.

Висновки та рекомендації

У ході пошукових досліджень розроблено апаратно-програмний комплекс для перевірки функціонування реально діючих блокчейн-систем та на його базі розгорнуто прототип системи електронного голосування. Головною перевагою розробленого прототипу є імплементація вітчизняних криптографічних стандартів які є стійкими і в умовах постквантового періоду. Проведено дослідження безпеки блокчейн-систем стосовно децентралізованих атак та атак, направлених на вибрані алгоритми консенсусу. Сформовано основні засади щодо розробки моделей загроз та моделей порушника відносно децентралізованих облікових систем, які дозволять проводити обґрунтовані оцінки стану безпеки децентралізованих систем та технологій.

Практичне впровадження технології блокчейн підвищує довіру до інформаційних ресурсів та сервісів (що є особливо актуальним для державних установ), зменшує час та накладні витрати, унеможливлює втручання центральних органів та відповідні корупційні дії, підвищує надійність збереження інформації та якість наданих послуг. З метою реалізації вироблених концепцій, сприяння розвитку та продуктивного використання інформаційних технологій в державі доцільною є розробка «Дорожньої карти з впровадження технології блокчейн в Україні», яка повинна включати:

- перелік додатків, щодо яких є доцільним застосування технології блокчейн в Україні;
- визначення рекомендованих компонентів технології блокчейн для різних практичних застосувань в Україні;
- перелік «базових» блокчейн-систем із рекомендованими компонентами для різних практичних застосувань в Україні;

– низка програм та методик проведення експертних досліджень «базових» блокчейн-систем для практичних застосувань в Україні;
– результати експертних досліджень «базових» блокчейн-систем із наданням рекомендацій щодо практичних застосувань в Україні;
– положення концепції та програми впровадження технології блокчейн в Україні.

Доцільним є також розгортання найближчим часом елементів децентралізованої інфраструктури електронного голосування із застосуванням технології блокчейн. Це надасть змогу у якості експерименту вже восени цього року провести перші в Україні місцеві вибори із застосуванням новітніх блокчейн-технологій, які унеможливлюють адміністративне втручання, підробку або викривлення результатів волевиявлення населення, забезпечують автоматичний підрахунок голосів та захищене документування результатів. До експерименту слід залучити окремі райони із переважно молодим та прогресивно думаючим населенням (студентські містечка, гуртожитки, університетські кампуси, тощо). Вибори необхідно провести із залученням нових комп'ютерних технологій, блокчейн-систем, смарт-контрактів, тощо, і це повністю відповідає загальній стратегії Президента України із розгортання новітніх технологій та систем державного управляння, зокрема є елементом державної стратегії з надання *е*-послуг «Держава у смартфоні».

Заплановані заходи спрямовані на підвищення ефективності державного управляння загалом та, зокрема, надання державних інформаційних послуг, усунення адміністративних бар'єрів та виключення умов виникнення корупції, підвищення довіри громадян України до національної влади, органів самоврядування, держави загалом.

Список літератури:

1. NISTIR 8202 Blockchain Technology Overview https://doi.org/10.6028/NIST.IR.8202
2. Consensus – Immutable agreement for the Internet of value https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf
3. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, 2009. 9 p.
4. СЕТАМ. https://setam.net.ua/
5. Vlad Gheorghiu, Michele Mosca. Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes,URL: https://arxiv.org/pdf/1902.02332.pdf
6. Perlner R. A., Cooper D.A. "Quantum Resistant Public Key Cryptography: A Survey", IDtrust '09, April 14- 16, 2009, Gaithersburg, MD. P. 85-93. URL: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id= 901595
7. Lily Chen, Stephen Jordan, Yi-Kai Liu, Dustin Moody, Rene Peralta, Ray Perlner and Daniel Smith-Tone. "NISTIR 8105. Report on Post-Quantum Cryptography" / National Institute of Standards and Technology. Internal Report 8105, April 2016. 10 p.
8. Закон України "Про вибори президента України".
9. Закон України "Про електронні довірчі послуги".
10. Регламент (ЄС) № 910/2014 Європейського Парламенту та Ради від 23 липня 2014 року «Про електронну ідентифікацію та довірчі послуги для електронних транзакцій у межах внутрішнього ринку та про скасування Директиви 1999/93/ЄС» (1) (COM (2012) 0238-C7-0133/2012 – 2012/0146 (COD)).
11. Горбенко І.Д., Кузнецов О.О., Потій О.В., Горбенко Ю.І., Полуяненко М.О. Технологія блокчейн: огляд, сучасні проблеми та перспективи впровадження в Україні // ІІ міжнар. наук.-практ. конф. "Проблеми кібербезпеки інформаційно-телекомунікаційних систем" (PCSITS), 11-12 квітня 2019 р., м. Київ, 2019. С. 217-220.
12. Isirova K. and Potii O. Decentralized public key infrastructure development principles // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). Kiev, 2018. P. 305-310.
13. Exonum documentation //URL: https://exonum.com/doc/version/0.12/
14. Bitfury Exonum //URL: https://exonum.com/ru/index

Харківський національний
університет імені В. Н. Каразіна;
АТ «Інститут інформаційних технологій»

Надійшла до редколегії 06.02.2020