DOI: 10.35681/1560-9189.2023.25.1.287172

УДК 519.816; 004.056

М. М. Савченко
Інститут проблем реєстрації інформації НАН України
вул. М. Шпака, 2, 03113 Київ, Україна

Безпека систем підтримки прийняття рішень на основі децентралізованих платформ даних

Розглянуто підходи до вирішення проблем безпеки систем підтримки прийняття рішень (СППР) за допомогою використання потенціалу децентралізованих платформ даних, зокрема технології блокчейн. Окрім того, надано комплексний огляд технології блокчейн, її різних типів та алгоритмів консенсусу, які забезпечують її роботу. Зокрема, описано дослідження, як блокчейн може зробити процес введення даних експертами, які взаємодіють з СППР, безпечним і відкритим для аудиту. За допомогою цих інноваційних технологій і методів СППР можуть допомогти організаціям приймати обґрунтовані, безпечні та стійкі до втручання рішення, забезпечуючи цілісність, незмінність і витривалість даних на рівні платформи.

***Ключові слова**: системи підтримки прийняття рішень, незмінність даних, блокчейн, алгоритми консенсусу, масштабованість, безкоштовні транзакції, інформаційна безпека, децентралізовані платформи, розподілені системи.*

1. Проблеми захисту даних у системах підтримки прийняття рішень: сучасний огляд

Системи підтримки прийняття рішень відіграють ключову роль у наданні рекомендацій тим, хто приймає рішення та вирішує задачі за допомогою СППР. Ці рекомендації служать невід'ємним інформаційним доповненням для складних операцій, таких як дослідження поведінки соціальних груп або аналіз складних мереж, де людський розсуд може бути недостатнім [1, 2].

1.1. Проблема довіри в системах підтримки прийняття рішень

Довіра становить основу СППР, де надійність результатів системи має глибокий вплив на процеси прийняття рішень. Проте, ця залежність від довіри створює декілька значних викликів, які можуть перешкоджати загальній ефективності системи, її репутації:

1) по-перше, результати СППР можуть бути складними для інтерпретації, що часто викликає питання та сумніви щодо базових операцій системи. Невизначені результати можуть створювати занепокоєння стосовно точності системи та її придатності для прийняття рішень [3];

2) по-друге, коли СППР перебувають під контролем конкретних сторін, останні мають змогу маніпулювати введенням даних, обробкою та представленням результатів. Ця концентрація повноважень відкриває двері для потенційних упереджень і конфліктів інтересів, що впливає на об'єктивність і справедливість процесу прийняття рішень [1];

3) по-третє, залежність від індивідуальних осіб для керування та підтримки СППР вводить багато точок відмови. Помилки людей, навмисне втручання у вхідні дані або рішення, сприяння особистим інтересам можуть порушити цілісність системи та підірвати довіру до її результатів;

4) нарешті, у випадках, коли рекомендації системи небажані, існує можливість таємного змінювання вхідних даних для задоволення конкретних вимог, що підриває об'єктивність системи [2].

Для вирішення цих викликів і відновлення довіри до систем підтримки прийняття рішень необхідна зміна парадигми у бік більш прозорих і публічно контрольованих рішень. Використання технології блокчейну з його вбудованою незмінністю та децентралізованістю створює перспективний підхід до зміцнення довіри до результатів СППР. Забезпечуючи перевірку експертних вхідних даних і захист від змін, системи, що побудовані на блокчейні, можуть впевнити у довірі до процесу прийняття рішень, одночасно сприяючи прозорості та відповідальності. Використання таких інноваційних методологій приведе до більш стійкого та надійного ландшафту підтримки прийняття рішень, що обслуговує різноманітні галузі з покращеною надійністю і авторитетністю.

1.2. Забезпечення надійності зберігання даних і цілісності знань

У традиційних системах зберігання, таких як СУБД (системи управління базами даних), залежність від централізованої бази даних створює можливість однієї точки відмови, що робить дані вразливими до втрати або пошкодження у випадку надзвичайних ситуацій. Хоча регулярні резервні копії можуть знизити ці ризики, вони часто супроводжуються значними витратами та навантаженням на обслуговування.

З децентралізованими платформами даних (ДПД) ситуація інша: вони пропонують вбудовану перевагу у забезпеченні збереженості даних без уступок у безпеці чи зусиль щодо обслуговування. Розподіляючи дані між мережею вузлів, ці платформи усувають залежність від центральної структури та покращують доступність і стійкість даних. Крім того, децентралізовані системи можуть бути налаштовані для врахування різних потреб у зберіганні, надаючи гнучкий та ефективний підхід [4].

1.3. Зменшення ризиків втручання у дані

Втручання в дані становить значну загрозу надійності та довірливості СППР. Навіть найменші зміни вхідних даних можуть мати великі наслідки для

результатів, які генерує система. Людські помилки, навмисне втручання або двозначність даних можуть підірвати цілісність процесу прийняття рішень [3]. Хоч і можуть бути впроваджені різноманітні заходи для мінімізації помилок вводу, повне усунення ризику залишається складним завданням.

Традиційні моделі безпеки пропонують методи, такі як шифрування, дублювання даних, резервне копіювання та моніторинг для захисту автентичності даних. Незважаючи на ці зусилля, залишається ризик того, що дані можуть бути змінені або пошкоджені без виявлення, особливо після їхнього початкового введення в систему [4]. Для усунення цієї вразливості з'явилися децентралізовані платформи для зберігання даних, такі як блокчейн. Шляхом впровадження незмінного публічного чи дозволеного реєстру, який обслуговується та підтверджується мережею учасників, технологія блокчейн забезпечує затвердження даних після їхнього запису, що унеможливлює їхні зміни [5].

1.4. Проблема даних як інтелектуальної власності

Питання власності над інформацією стає все більш критичним при вирішенні завдань традиційних платформ для зберігання даних. У централізованих системах, зазвичай, власність на дані належить одному суб'єкту, що викликає занепокоєння стосовно монополізації даних і можливого зловживання ними.

Навпаки, децентралізовані платформи для зберігання даних надають перевагу розподілу власності на інформацію. Завдяки механізмам, таким як блокчейн, кожен учасник мережі має доступ до копії інформації, що сприяє прозорості та відкритості. Однак, самі дані можуть бути відкритими або зашифрованими залежно від задуманого сценарію використання. Значною перевагою є те, що незмінність даних, яка властива децентралізованим системам, гарантує, що після того, як певний суб'єкт був асоційований як власник даних або змін у даних, ця асоціація зберігається довічно, що зменшує ризик їхніх несанкціонованих змін або передавання [6].

Інтеграція блокчейну та інших децентралізованих платформ для зберігання даних у системі підтримки прийняття рішень дозволяє вирішити ці критичні питання, зміцнюючи довіру, безпеку та цілісність даних. Завдяки використанню цих інноваційних рішень, процеси прийняття рішень можуть отримати переваги більш надійного, прозорого та відповідального застосування, відкриваючи нову еру надійних та ефективних СППР.

2. Децентралізовані платформи даних

Безпека традиційних централізованих комп'ютерних систем, включаючи СППР, є складною задачею без гарантії повного захисту. Незважаючи на значні зусилля, завжди існує практична вразливість, яку можуть використовувати зловмисники.

ДПД, такі як блокчейн, є криптографічно захищеними і пропонують інноваційний підхід до вирішення проблем із безпекою. Вони усувають ризики зміни даних і встановлюють чіткі правила взаємодії і маніпулювання даними. Крім того, ДПД стійкі до відмов, забезпечуючи безперебійну роботу навіть у разі збою певних вузлів децентралізованої мережі [4].

Децентралізовані платформи гарантують постійну та передбачувану роботу, запобігаючи несанкціонованим змінам даних. Це сприяє довірі до системи, запобігаючи неочікуваним результатам і забезпечуючи захист історичних даних [6, 7].

У наступних розділах розглядаються основні аспекти технології блокчейн та алгоритми консенсусу, які забезпечують прозору та безпечну роботу з системами різних типів. Крім того, розглядаються різні типи ДПД, публічні, приватні та консорціум-блокчейни, обговорюючи їхні різноманітні застосування та важливість для СППР та інших критичних галузей.

2.1. Наявні децентралізовані платформи для зберігання даних

Шлях до децентралізованих платформ для зберігання даних почався з появи Bitcoin у 2009 році, запровадженого персонажем з відомим псевдонімом Сатоші Накамото. Bitcoin — це перша криптовалюта яка революціонізувала фінансовий світ і дозволила здійснювати безпечні транзакції без посередників. Далі, у 2015 році було засновано ДПД Ethereum Віталієм Бутеріном, що надав значний стрибок у можливостях децентралізованих систем. На відміну від Bitcoin, Ethereum розширила своє призначення за межі простих переказів монет і представила програмований блокчейн, що дозволяє розробникам розгортати смарт-контракти та децентралізовані додатки (DApps). Цей ключовий крок позначив перехід від простої цифрової валюти до супербезпечної глобальної мережі, що сприяє складним захищеним обчисленням і відкриває нову еру децентралізованого інноваційного розвитку [8, 9].

Існує дві основні технології ДПД, короткий опис яких наводиться нижче.

Блокчейн — це технологія, яка є основою криптовалют, таких як Bitcoin та Ethereum, що базується на ланцюговій структурі даних. У цій структурі блоки інформації зв'язані між собою криптографічно, що додає властивість незмінності даних. Цей дизайн забезпечує те, що зміна будь-яких даних у блоку вимагатиме зміни всіх наступних блоків, що робить це обчислювально неможливим і дуже безпечним.

Блокчейн знаходить різноманітні застосування поза криптовалютами. Наприклад, Ethereum надає розробникам змогу створювати смарт-контракти, які автоматично виконуються, коли виконуються певні умови, що дозволяє створювати децентралізовані додатки для різних галузей. Інші приклади проектів на основі блокчейну включають Polygon (раніше відомий як Matic Network), який поліпшує масштабованість і користувацький досвід Ethereum, а також сам Bitcoin, як перша в світі криптовалюта або «цифрове золото» [10].

Назва «Блокчейн» походить безпосередньо від базового алгоритму, що означає ланцюжок блоків. Транзакції у блокчейні організовані в блоках, і блоки посилаються один на одного. Ця структура з криптографічно захищеними посиланнями між блоками називається блокчейном [10] (рис. 1).

У блокчейні, кожен наступний блок повинен посилатися на свій попередній, щоб уся структура була дійсною. Це посилання фактично — хеш попереднього блоку. Якщо змінюється вміст попереднього блоку, змінюється його хеш, і, отже, посилання на змінений блок стає недійсним. Тому що весь блокчейн перевіряє блоки, кожен недійсний блок просто ігнорується, не залишаючи ніяких шансів комусь змінити дані та залишитися непоміченим.

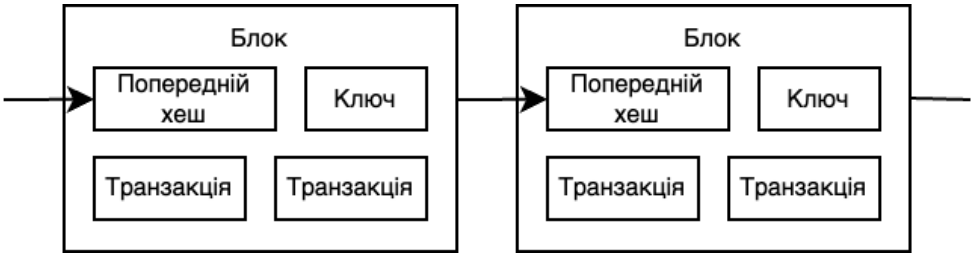

Рис. 1. Структура даних у блокчейні — блоки

Розмір блоків у блокчейні має обмеження, що призводить до проблем масштабованості [11]. Якби розмір блоків не був обмежений, то менше учасників мережі могли би брати участь у формуванні згоди через обмеження обладнання та пропускної здатності мережі, що призводило би до централізації мережі та, відповідно, послабленню її безпеки [12, 13].

Hashgraph — децентралізована платформа для зберігання даних, яка працює на основі структури направленого ациклічного графа (DAG), а не на традиційному блокчейні. Вона використовує алгоритм консенсусу, який базується на комбінації «слухання чуток» (gossip) та «віртуального голосування» (virtual voting) для досягнення згоди. У hashgraph обчислювальні вузли спілкуються асинхронно та обмінюються інформацією про транзакції і події. Цей процес поширення та перевірки інформації призводить до створення високозахищеної і ефективної мережі, яка здатна обробляти тисячі транзакцій за секунду [14]. Приклад структури hashgraph зображено на рис. 2.

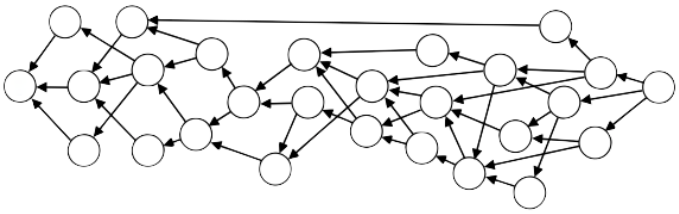

Рис. 2. Структура Hashgraph (спрямований ациклічний граф)

Hedera Hashgraph виділяється серед яскравих прикладів публічної дозволеної платформи hashgraph, яка пропонує високу пропускну здатність і низьку затримку для застосунків корпоративного класу. IOTA — інша платформа, що заснована на hashgraph, спрямована на простір «Інтернету речей» (IoT), забезпечуючи безпечні та безкоштовні транзакції для пристроїв Інтернету речей. Є й інші приклади схожих за структурою до направленого ациклічного графа децентралізованих мереж, наприклад, Tangle [15].

Відмінності Blockchain і Hashgraph. Одна із ключових відмінностей між блокчейном і hashgraph полягає в їхніх алгоритмах консенсусу. Блокчейн використовує детермінований алгоритм консенсусу, де кожен вузол доходить згоди про дійсність транзакцій через процеси, такі як Proof of Work (PoW) або Proof of Stake (PoS). Ці методи забезпечують те, що всі вузли приходять до одного висновку, гарантуючи впевненість у закінченні транзакцій.

З іншого боку, hashgraph використовує ймовірнісний алгоритм консенсусу, поєднуючи «слухання чуток» (gossip) та «віртуальне голосування» (virtual voting) для досягнення згоди щодо транзакцій. Хоча такий підхід пропонує високу пропускну здатність і низьку затримку, він працює на більш імовірнісній основі, що означає, що він може надавати швидку згоду більшість часу, але існує невеликий шанс виникнення роздвоєння або альтернативних точок зору на транзакції, які згодом вирішуються з поширенням більшої кількості інформації через мережу.

Масштабованість може бути вирішена в обох технологіях за допомогою інноваційних рішень, таких як технології другого рівня для блокчейну та вбудованої ефективності DAG для hashgraph. У підсумку, вибір між блокчейном і hashgraph залежить від конкретних вимог і цілей застосунків, і обидві технології продовжують забезпечувати інновації і революціонізувати різні галузі.

2.2. Алгоритми консенсусу блокчейну

Блокчейн, який є однією із ранніх і найбільш поширених децентралізованих платформ обробки даних, продемонстрував значну практичність і застосовність у реальному світі, тому ми більше зосередимося на блокчейні, а не на Hashgraph.

Алгоритм консенсусу в децентралізованій мережі — це процес, за допомогою якого досягається узгодження щодо одного значення даних або стану мережі серед розподілених учасників мережі. У блокчейні алгоритм консенсусу використовується для досягнення згоди щодо найновішого стану реєстру, який підтримується всіма учасниками мережі [14].

Існує багато алгоритмів консенсусу, але лише декілька з них практично довели свою ефективність і широко використовуються: Proof of Work (Підтвердження роботи), Proof of Stake (Підтвердження ставки), Delegated Proof of Stake (Делеговане підтвердження ставки) та інші. Нижче коротко розглядаються основні засади цих алгоритмів і наводиться їхнє порівняння [16, 17].

Підтвердження роботи (PoW). Підтвердження роботи є першим алгоритмом консенсусу, запропонованим Сатоші Накамото в 2009 році. У PoW майнери змагаються, щоби вирішити складні математичні головоломки для підтвердження транзакцій і додавання нових блоків до ланцюжка блоків. Перший майнер, який вирішує задачу з «майнінгу», отримує право додати наступний блок і винагороду як стимул у вигляді новоствореної криптовалюти. Цей конкурентний процес забезпечує незмінність ланцюжка блоків, оскільки зміна блоку потребує перероблення всіх наступних блоків, що стає обчислювально неможливим з приростом кількості блоків. PoW славиться своєю безпекою та досі використовується в основних криптовалютах, таких як Bitcoin та Litecoin.

Підтвердження ставки (PoS). PoS є альтернативним алгоритмом консенсусу, розробленим як більш енергоефективний і масштабований варіант PoW. Замість змагання за обчислювальну потужність PoS використовує валідаторів, що обираються для створення нових блоків на основі кількості токенів, які вони «ставлять» або блокують як заставу. Процес вибору часто базується на факторах, таких як вік токенів чи розмір застави. PoS усуває потребу в ресурсоємному майнінгу та знижує негативний вплив на довкілля, зробивши його більш екологічним механізмом консенсусу. Відомі блокчейни, такі як Ethereum, переходять з PoW до PoS за

допомогою оновлення Ethereum 2.0 з метою покращення масштабованості і енергоефективності.

Поза PoW та PoS, було розроблено інші різноманітні алгоритми консенсусу, що враховують конкретні випадки використання та вимоги [17]. Деякі з найвідоміших прикладів такі:

1) **делеговане підтвердження ставки (DPoS)**. DPoS поєднує елементи PoW та PoS, де власники токенів обирають обмежену кількість делегатів для валідації транзакцій і створення блоків від їхнього імені. Цей дизайн підвищує масштабованість і пропускну здатність транзакцій, оскільки кількість продюсерів блоків обмежена. EOS, як приклад іншої децентралізованої платформи даних, використовує DPoS у своєму механізмі консенсусу [18];

2) **чисте підтвердження ставки (PPoS)**. PPoS є варіацією PoS, яка наголошує на справедливості та рівних можливостях для всіх власників токенів участі в підтвердженні блоків. Воно уникає концентрації влади, яка може виникати у системах DPoS, і пропонує більш демократичний підхід. Блокчейн Algorand використовує PPoS для досягнення консенсусу та відомий своїм швидким підтвердженням транзакцій [19].

2.3. Типи доступності децентралізованих платформ даних

Децентралізовані платформи зберігання даних пропонують різноманітні мережеві конфігурації для задоволення різних вимог і сценаріїв використання. Налаштування та доступ до цих платформ можна загалом умовно розділити на публічні, приватні та консорціумні мережі [5]. Публічні мережі передбачають відкриту участь і прозорість, тоді як приватні надають пріоритет конфіденційності й обмеженому доступу. Консорціумні мережі відповідають колективним потребам довірених учасників. Гнучкість і адаптивність цих конфігурацій дозволяють користувачам та організаціям використовувати потенціал блокчейну та інших децентралізованих платформ зберігання даних у різних реальних сценаріях.

Публічні мережі. Публічні мережі є повністю відкритими та вільно доступними, дозволяючи кожному брати участь у платформі без обмежень. Учасники можуть приєднатися до мережі як вузли, майнери або валідатори та сприяти процесу згоди та перевірки транзакцій. Публічні мережі наголошують на децентралізації і прозорості, забезпечуючи глобальну участь і гарантуючи, що жодна окрема сутність не контролює більшість мережі [20].

До прикладів публічних блокчейн-мереж належать Bitcoin, Ethereum та Binance Smart Chain. Ці платформи мають велику кількість децентралізованих додатків, смарт-контрактів і цифрових активів, що робить їх доступними користувачам по всьому світу.

Приватні мережі. Навпаки, приватні мережі є обмеженими та вимагають дозволу на доступ. Зазвичай, їх використовують організації або конкретні групи для внутрішніх цілей, обмежуючи участь затвердженими суб'єктами. Приватні блокчейни часто надають пріоритет конфіденційності, вищому рівню приватності та контролю над операціями мережі [21].

Однією із помітних особливостей приватних блокчейнів є те, що вони можуть періодично «фіксувати» або «закріпляти» свій стан у публічному блокчейні для забезпечення децентралізації і підвищення безпеки. Цей процес передбачає

запис криптографічного хешу стану приватної мережі на публічний блокчейн, створюючи незмінним посилання. Таким чином, приватні мережі можуть користуватися безпекою та прозорістю публічного блокчейну, залишаючи при цьому свою обмежену доступність.

Консорціумні мережі (також відомі як Permissioned DLT). Ці мережі забезпечують баланс між публічними та приватними мережами, працюючи як напівдецентралізована структура. Вони включають групу довірених сутностей, зазвичай, бізнесів або організацій, які спільно управляють мережею. Консорціумні мережі пропонують вищий рівень контролю і ефективності порівняно з повністю публічними мережами, що робить їх привабливими для корпоративних сценаріїв використання [22].

До прикладів консорціумних мереж належать Hyperledger Fabric та R3 Corda. Ці платформи часто використовуються в різних галузях, таких як фінанси, логістичні ланцюги постачання та охорона здоров'я, де консорціум організацій співпрацює на спільній блокчейн-мережі для оптимізації процесів і покращення ефективності [23].

3. Модель безпеки для систем підтримки прийняття рішень

Децентралізовані додатки в ДПД мають потенціал революціонізувати системи з високим ризиком введенням ряду цінних властивостей, таких як:

1) безпека та цілісність даних;
2) забезпечення незмінності даних і прозорої історії змін;
3) надійне та стійке до відмов зберігання даних;
4) надійна та передбачувана обробка даних.

Налаштування приватних або консорціумних типів децентралізованих платформ з даними може бути складним процесом. Це вимагає ретельного планування та реалізації для забезпечення належної функціональності. Тому рекомендується утриматися від такого підходу для окремих осіб та організацій. Замість цього, раціональною буде участь у вже існуючих приватних, консорціумних або публічних децентралізованих платформах з даними, які вже були створені й підтверджені як ефективні у забезпеченні безпеки даних. Таким чином, можна скористатися наявними знаннями та ресурсами, забезпечивши більш гладкий і безпечний досвід управління даними та платити лише незначні кошти за здійснення транзакцій у децентралізованій мережі.

Щодо СППР, то існує кілька можливих підходів до часткової децентралізації та забезпечення їхньої безпеки із використанням технології блокчейн. Автор описує 2 з них, які обидва базуються на децентралізованих платформах з даними, але відрізняються архітектурою і актуальними даними, що зберігаються публічно: повністю публічна модель контролю доступу та напівпублічна модель з дозволами.

3.1. Гібридний підхід для підвищення безпеки СППР з використанням публічних ДПД

Побудова системи повністю на публічній децентралізованій платформі є бажаною через її прозорість і можливість верифікації. Однак, вона супроводжується

практичними викликами, такими як необхідність безпомилкової розробки програмного коду та спеціалізованих методів для його оновлення, щоб уникнути ризиків централізації. Крім того, поточні публічні децентралізовані платформи можуть зіткнутися з обмеженнями щодо масштабованості й ефективності витрат, що призводить до звуження спектра децентралізованих застосунків.

Для вирішення цих викликів пропонується застосовувати гібридний підхід, що поєднує переваги публічних і приватних/консорціумних децентралізованих платформ з даними. У цій гібридній моделі СППР використовують прозорість і незмінність публічних децентралізованих реєстрів, одночасно користуючись конфіденційністю та масштабованістю приватних або консорціумних мереж.

Процес введення та перевірки інформації у цій гібридній моделі можна візуалізувати таким чином (рис. 3):

1) експерт безпосередньо вводить дані до децентралізованого реєстру за допомогою веб-інтерфейсу для зручності. Однак ніхто інший не бере участь у взаємодії між експертом і децентралізованим реєстром;

2) СППР зчитує ці дані з децентралізованого реєстру, отримуючи найбільш актуальну та захищену від підробки інформацію;

3) СППР обробляє вхідні дані та генерує результат, який у подальшому може бути збережений у традиційній базі даних для посилання;

4) результат ретельно перевіряється на відповідність вхідним даним, а публічний запис усіх внесених експертів доступний користувачам для підтвердження його надійності.

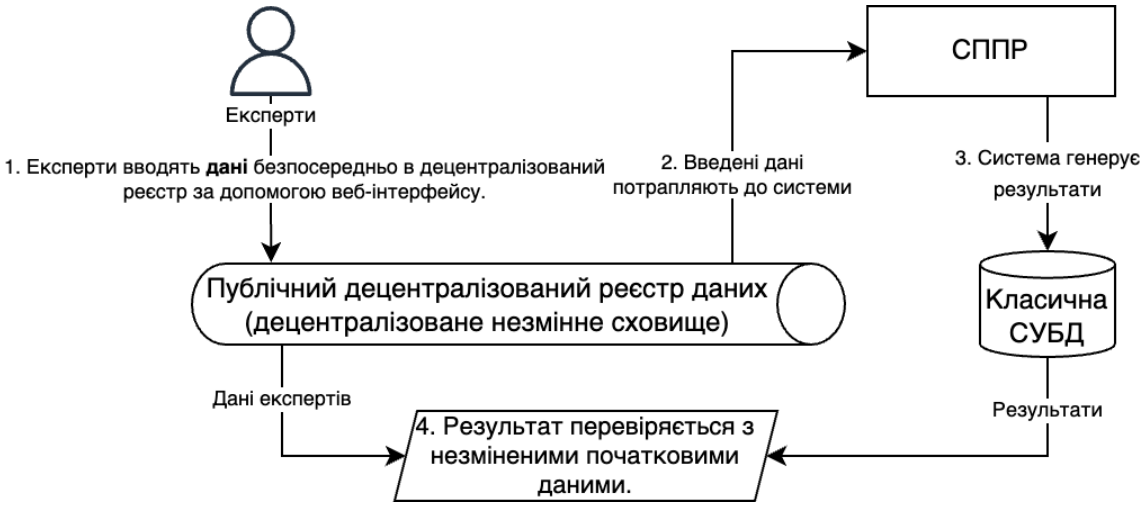

Рис. 3. Модель безпеки системи, де експерти безпосередньо подають інформацію до дозволеної децентралізованої системи

Підсумовуючи, можна сказати, що інтеграція децентралізованої платформи для обробки даних у системі прийняття рішень пропонує новий підхід для підвищення довіри, надійності та цілісності даних. За допомогою гібридної децентралізованої платформи для обробки даних, експерти можуть безпосередньо вводити дані до системи, використовуючи децентралізовані ідентифікатори для перевірки. Це усуває потребу в посередниках і забезпечує незмінність даних.

Коли СППР обробляє вхідні дані та генерує рекомендації, кожен результат ретельно порівнюється та перевіряється із вхідними даними, що підсилює прозорість і знімає відповідальність системи над вхідними даними. Використання децентралізованої платформи для обробки даних дозволяє створити надійний і стійкий до втручань реєстр, гарантуючи незмінність записаних даних.

Крім того, масштабованість та обчислювальні можливості обраної децентралізованої платформи для обробки даних визначають, в якому ступені всю СППР можна побудувати на її основі. Якщо платформа може ефективно справлятися з навантаженням та обчислювальними ресурсами, необхідними для роботи, то всю СППР можна інтегрувати в ДПД, надаючи повністю децентралізований і безпечний інтерфейс прийняття рішень.

Таким чином, використання гібридної децентралізованої платформи для обробки даних не тільки зменшує ризики підробки даних і несанкціонованих змін, але й закладає основу для інноваційної і надійної СППР. Шляхом використання переваг децентралізованої технології, організації та установи можуть надати експертам більше можливостей, покращити прозорість і створити стійкі СППР для широкого спектра реальних задач.

3.2. Гібридний підхід: практична реалізація з використанням публічних децентралізованих платформ для обробки даних

Оскільки публічні децентралізовані платформи для обробки даних можуть вимагати великих витрат на зберігання даних безпосередньо на блокчейні, пропонується до використання альтернативний підхід, який оптимізує витрати, забезпечуючи надійну та безпечну систему без довіреного посередника для процесів прийняття високоризикових рішень.

Для досягнення ефективності з точки зору витрат, запропонована модель безпеки мінімізує обсяг даних, які зберігаються в децентралізованій платформі, що значно зменшує оперативні витрати. За допомогою такого підходу, вартість на один повний процес прийняття рішення може бути зменшена до частини від попередньої вартості. Наприклад, використовуючи децентралізовану платформу Ethereum (враховуючи середню вартість транзакції на 5 квітня 2023 року), вартість може бути знижена до $0,01 за один запис експерта або за весь процес, якщо хеш криптографічного стану вхідних даних подається лише один раз для всіх експертів.

У цій моделі процес вводу даних починається зі збору вхідних даних у звичайній централізованій базі даних. Після того, як всі експерти надають свої вхідні дані (експертні оцінки), вони піддаються криптографічному хешуванню, створюючи унікальний хеш, що представляє стан даних. Цей криптографічний хеш потім публікується в публічній децентралізованій платформі для доказу оригінальності вхідних даних.

Пізніше, в ході процесу прийняття рішень, фактична вхідна інформація розкривається, і експерти незалежно перевіряють, що результатний хеш відповідає початковим вхідним даним. Цей процес перевірки діє як цифровий підпис, забезпечуючи гарантії, що вхідні дані є автентичними та незмінними.

Рис. 4 ілюструє цей підхід, де лише захешована інформація зберігається в децентралізованому безпечному реєстрі. Цей хешований блок служить доказом

законних вхідних даних, які перевіряються з оригінальним вводом після завершення процесу прийняття рішень.

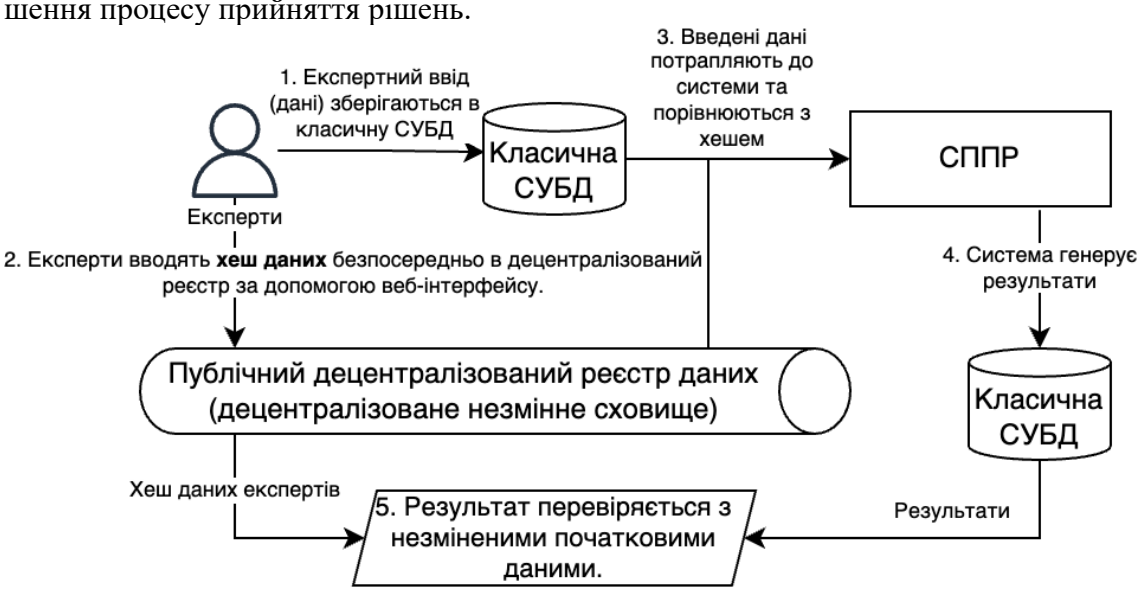

Рис. 4. Ілюстративний приклад моделі безпеки системи, що демонструє, як в децентралізованій платформі даних зберігається лише хешована інформація, що дає змогу виконувати ефективні за вартістю операції

Важливо визнати, що в цьому сценарії існує можливість втрати оригінальних даних, що призведе до необхідності існування хешу, який уже не відповідає жодним конкретним даним. Для кінцевих користувачів це означатиме, що процес прийняття рішень не був належним чином організований, і що має місце можливість підробки або недостовірність прийнятого рішення.

За допомогою цієї ефективної, з точки зору витрат моделі безпеки, організації та інституції можуть використовувати публічні децентралізовані платформи для обробки даних для забезпечення цілісності даних і створення надійних СППР, не зазнаючи значних витрат. Цей підхід забезпечує баланс між безпекою та ефективністю витрат, роблячи його придатним рішенням для систем високого ризику, які вимагають прозорості та довіри до своєї роботи.

3.3. Приклади застосування ДПД за межами СППР

Децентралізовані платформи зберігання даних, зокрема, блокчейн, можуть вирішити багато раніше нерозв'язних або компромісних проблем [24]. Нижче наведено кілька реальних прикладів, що використовують дещо схожі методи застосування ДПД для СППР.

1. **Охорона здоров'я** — електронні медичні записи Естонії. Система охорони здоров'я Естонії впровадила гібридну децентралізовану платформу для управління електронними медичними записами (EHR). Уряд Естонії розробив X-Road — національний рівень обміну даними, який діє як гібридна платформа. X-Road дозволяє різним медичним постачальникам і установам отримувати доступ до медичних записів пацієнтів й оновлювати їх у безпечний і взаємовигідний спосіб. Дані зберігаються на приватних і безпечних серверах, які утримуються медични-

ми постачальниками, але важливі медичні записи знаходяться на публічному блокчейні. Це забезпечує цілісність і прозорість EHR, дозволяючи пацієнтам та уповноваженим медичним фахівцям перевіряти точність і повноту медичної інформації.

2. **Управління ланцюжками постачання** — Walmart та IBM. Walmart спільно з IBM впровадили гібридну децентралізовану платформу для покращення управління ланцюжками постачання. Завдяки використанню технології блокчейн як публічного децентралізованого реєстру, Walmart та його постачальники можуть реєструвати весь шлях продукції від виробника до поличок магазину. Кожен запис, такий як джерело сировини, деталі виробництва, транспортування та зберігання, безпосередньо реєструється на блокчейні. Це забезпечує необоротний і прозорий запис, запобігаючи змінам даних або підробці на будь-якому етапі ланцюжка постачання. Крім того, з метою забезпечення конфіденційності та безпеки деяка чутлива інформація може бути збережена в приватній мережі консорціуму, а дані про кінцевий продукт публічно закріплені на блокчейні.

3. **Права на інтелектуальну власність** — WIPO та IBM. Всесвітня організація інтелектуальної власності (WIPO) співпрацює з IBM для створення блокчейн-базового рішення для захисту прав інтелектуальної власності. Система WIPO дозволяє творцям і інноваторам встановлювати часові відбитки своїх творчих робіт, винаходів або інновацій безпосередньо на публічному блокчейн-реєстрі. Це створює незворотній запис дати створення та права власності, запобігаючи суперечкам і несанкціонованим претензіям. При цьому, детальна інформація про права на інтелектуальну власність може зберігатись у конфіденційній приватній мережі, але часовий відбиток і доказ створення фіксуються на публічному блокчейні.

4. **Реєстрація прав власності на землю** — Lantmäteriet Швеції. Це орган реєстрації землі, експериментує з гібридною децентралізованою платформою для реєстрації прав власності на землю. Транзакції з продажу землі реєструються на приватному блокчейні консорціуму, який управляється та підтримується урядом і надійними установами. Однак, остаточні записи про право власності на землю періодично закріплюються на публічному блокчейні, забезпечуючи те, що найновіші та точні правовласницькі титули можуть бути публічно перевірені та не можуть бути змінені без виявлення. Це підвищує безпеку та надійність реєстрації прав власності на землю, зменшуючи ризик шахрайства та суперечок.

Ці приклади демонструють, як компанії та установи уряду скористалися децентралізованими платформами збереження даних, поєднуючи переваги як публічних, так і приватних або консорціумних блокчейнів. За допомогою збереження важливих даних на публічному блокчейні та збереження конфіденційної інформації у приватних мережах, ці організації досягають підвищеної прозорості, безпеки та надійності в своїх критичних операціях.

Висновок

Системи з високим ризиком, такі як СППР, повинні бути надзвичайно безпечними та надійними. Децентралізовані платформи даних, як нова технологія, надають рішення для зменшення ризиків втручання та підвищення безпеки і довіри до систем, що їх використовують. Шляхом прийняття запропонованої у цій

статті децентралізованої моделі безпеки, системи з високим ризиком, такі як СППР, можуть стати більш захищеними, а їхні результати — такими, що можна верифікувати, незалежно від їхньої внутрішньої будови.

Децентралізовані платформи збереження даних пропонують революційний підхід до побудови довірених і безпечних систем. Ці платформи дозволяють зберігати дані таким чином, щоб їх не можна було легко змінити або підробити, забезпечуючи цілісність інформації, яка використовується у процесах прийняття рішень. З покращеним рівнем безпеки за допомогою ДПД організації можуть працювати з більшою прозорістю та захистом, що робить їхні критичні процеси захищеними від несанкціонованого доступу чи змін.

Застосування децентралізованих платформ даних дозволяє системам з високим ризиком створювати більш стійке та безпечне середовище. Ця передова парадигма надає СППР та іншим критичним застосункам довіру користувачів, знаючи, що їхні дані та операції захищені від можливих загроз. З децентралізованою технологією в основі, критичні системи стають більш безпечними та надійними, надаючи основу для майбутньої цифрової ери.

1. Saaty T.L. Principia Mathematica Decernendi — Mathematical principles of decision making — Generalization of the Analytic Network Process to neural firing and synthesis. Pittsburg: RWS Publications, 2010.

2. Tsyganok V., Kadenko S., Andriychuk O., Roik P. Usage of multicriteria decision-making support arsenal for strategic planning in environmental protection sphere. *Journal of Multi-Criteria Decision Analysi*s. 2017. **24**. P. 227–238. https://doi.org/10.1002/mcda.1616.

3. Driscoll J.W. Trust and participation in organizational decision making as predictors of satisfaction. *Academy of management journal.* 1978. **21**(1). P. 44–56. https://doi.org/10.5465/255661.

4. Benisi N.Z., Aminian M., and Javadi B. Blockchain-based decentralized storage networks: A survey. *Journal of Network and Computer Applications*. 2020. **162**. P. 102656. https://doi.org/10.1016/j.jnca.2020.102656.

5. Tsyganok V.V., Kadenko S.V. & Andriichuk O.V. Using different pair-wise comparison scales for developing industrial strategies. *International Journal of Management and Decision Making*. 2015. Vol. 14, Issue 3. P. 224–250. https://doi.org/10.1504/IJMDM.2015.070760.

6. Rahardja U., Hidayanto A.N., Lutfiani N., Febiani D.A., and Aini Q. Immutability of Distributed Hash Model on Blockchain Node Storage. *Sci. J. Informatics*. 2021. **8**(1). P.137-143. https://doi.org/10.15294/sji.v8i1.29444

7. Dhillon G., and Torkzadeh G. Value focused assessment of information system security in organizations. *Information Systems Journal*. 2006. **16**(3). P .293–314. https://doi.org/10.1111/j.1365-2575.2006.00219.x

8. Puthal D., Malik N., Mohanty S.P., Kougianos E., and Yang C. The blockchain as a decentralized security framework. IEEE Consum. Electron. Mag., 2018. **7**(2). P. 18–21. https://doi.org/10.1109/MCE.2017.2776459

9. Seebacher S., and Schüritz R. Blockchain technology as an enabler of service systems: A structured literature review. In International Conference on Exploring Services Science Springer, Cham. 2017, May. P. 12–23.

10. Pilkington M. Blockchain technology: principles and applications. *Research handbook on digital transformations*. 2016. **11**. P. 225.

11. Swan M. Blockchain: Blueprint for a new economy. O'Reilly Media, Inc., 2015.

12. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. URL: https://bitcoin.org/bitcoin.pdf

13. Wood G. Ethereum: A secure decentralized generalized transaction ledger. *Ethereum project yellow paper*. 2014. **151**. P. 1–32.

14. Hoxha L. Hashgraph the Future of Decentralized Technology and the End of Blockchain. *European Journal of Formal Sciences and Engineering*. 2018. **1**(2). P. 29–32. https://doi.org/10.26417/ejef.v2i2.p86-89

15. Popov S. The tangle version 1.4. 3. 2018. URL: https://iota.org/IOTA_Whitepaper.pdf

16. Croman K., Decker C., Eyal I., Gencer A.E., Juels A., Kosba A., Miller A., Saxena P., Shi E., Sirer E.G., and Song D. On scaling decentralized blockchains. In International Conference on Financial Cryptography and Data Security Springer. Berlin, Heidelberg. 2016, February. P. 106–125. https://doi.org/10.1007/978-3-662-53357-4_8

17. Zheng Z., Xie S., Dai H., Chen X., and Wang H. An overview of blockchain technology: Architecture, consensus, and future trends. In Big Data (BigData Congress). 2017 IEEE International Congress on IEEE. 2017, June. P. 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

18. Larimer D. Delegated Proof of Stake. Bitshares.org., 2014. From Bitshares.org (Last accessed 2016/11/21).

19. Lepore, C., Ceria, M., Visconti, A., Rao, U.P., Shah, K.A. and Zanolini, L. A sur-vey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS. *Mathematics*. 2020. **8**(10). P. 1782. https://doi.org/10.3390/math8101782

20. O'Dwyer K.J., and Malone D., Bitcoin mining and its energy footprint. ISSC 2014 / CIICT 2014, Limerick. P. 26–27. https://doi.org/10.1049/ cp.2014.0699

21. Bentov I., Gabizon A., and Mizrahi A. Cryptocurrencies without proof of work. In International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg. 2016, February. P. 142–157. https://doi.org/10.1007/978-3-662-53357-4_10

22. Cachin C. Architecture of the hyperledger blockchain fabric. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers. 2016, July. Vol. 310.

23. Vukolić M., The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In International Workshop on Open Problems in Network Security. Springer, Cham., 2015, October. P. 112–125. https://doi.org/10.1007/978-3-319-39028-4_9

24. Zheng Z., Xie S., Dai H.N., and Wang H. Blockchain challenges and opportunities: A survey. Work Pap., 2016.

Надійшла до редакції 25.05.2023