КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2023.20.619
УДК 004.62

Балацька Валерія Сергіївна
Аспірант кафедри “Захист інформації”
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0000-0002-6262-6792
valeriia.s.balatska@lpnu.ua

Опірський Іван Романович
д.т.н., проф., професор кафедри захисту інформації
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ПЕРСОНАЛЬНИХ ДАНИХ І ПІДТРИМКИ КІБЕРБЕЗПЕКИ ЗА ДОПОМОГОЮ БЛОКЧЕЙНУ

Анотація. Нещодавнє збільшення кількості порушень безпеки та цифрового стеження підкреслює потребу у покращенні конфіденційності та безпеки, особливо персональних даних користувачів. Прогрес у кібербезпеці та нове законодавство обіцяють покращити захист персональних даних. Технології блокчейну та розподіленої книги (DTL) надають нові можливості для захисту даних користувачів за допомогою децентралізованої ідентифікації та інших механізмів конфіденційності. Ці системи можуть надати користувачам більший суверенітет за допомогою інструментів, які дозволяють їм володіти та контролювати власні дані.
Метою статті є дослідження технології блокчейн та механізмів досягнення надійності в блокчейні для захисту та безпеки персональних даних.
Децентралізовані та об’єднані системи ідентифікації надають користувачам контроль над тим, якою, коли та якою кількістю їх персональної інформації можна ділитися та з ким. Ці системи також можуть зменшити загрози кібербезпеці. За допомогою різних алгоритмів консенсусу рішення конфіденційності на основі блокчейну, дозволяють користувачам краще керувати своїми даними та гарантує, що дані та моделі, отримані з них, є більш точними, чесними та надійними.

Ключові слова: блокчейн, алгоритм консенсусу, персональні дані, конфіденційність.

ВСТУП

Обсяг персональних даних, які збираються, на сьогоднішній день досить швидко зростає. Підприємства, організації та державні установи і Уряд використовують ці дані для профілювання людей, а також для прогнозування та контролю їхнього ставлення та поведінки. Це може призвести до персоналізованого досвіду, персоналізованих послуг і більш ефективного використання ресурсів. Це також може призвести до дезінформації та використання суб’єктом, який зібрав дані, або іншими особами, які купують або викрадають їх.

У відповідь на зростання кіберзлочинності та зростаюче занепокоєння користувачів пропонується та впроваджується законодавство щодо захисту персональних даних. Організації, які використовують персональні дані, стикаються зі зростаючими витратами, пов’язаними з керуванням даними та їх захистом. Вони також стикаються зі зростаючими ризиками того, що дані будуть використані або викрадені і що як наслідок потягне за собою правові та фінансові наслідки, а також завдадуть шкоди як своїй репутації, так і відносинам з клієнтами та іншими зацікавленими сторонами.

ISSN 2663 - 4023

Постановка проблеми. Основною проблемою конфіденційності, з якою стикаються розробники та користувачі інформаційних систем, є конфіденційність персональних даних. Особисті дані про клієнтів, співробітників, потенційних клієнтів та інших зацікавлених сторін можуть регулярно збиратися та зберігатися в спільних базах. Сьогодні багато організацій зберігають приватні дані зацікавлених сторін і навіть паролі в незашифрованому вигляді. Навіть якщо дані зашифровані або анонімні, можна ідентифікувати користувачів, якщо в системах керування даними не розроблені добре процеси кібербезпеки. Через часті збої в системі кібербезпеки та посилення регулювання збереження конфіденційності персональної інформації стало проблемою стратегічного занепокоєння для багатьох організацій.

Ідентифікаційна інформація включає будь-які дані, які можна відстежити до конкретної особи, а також окремі елементи, такі як біометричні дані, номери соціального рахунку, номери телефонів або навіть паспортні дані. Ідентифікаційна інформація також може включати комбінації даних, наприклад, поштові індекси, дати народження та стать, або дані про характеристики однієї особи. Організації збирають і зберігають особисті дані про поточних і майбутніх клієнтів і співробітників, а також про інших зацікавлених сторін.

Аналіз останніх досліджень і публікацій. Кібербезпека стає все більш важливою як для державного Уряду, так і для бізнесу. Інформаційна безпека – одна з складових кібербезпеки, зосереджена на захисті цілісності та конфіденційності даних під час їх збирання, зберігання та використання. Люди, процеси та технології, пов’язані з даними, працюють узгоджено для створення та підтримки безпеки.

Незважаючи на прогрес у протоколах безпеки та програмному забезпеченні, порушення конфіденційності зростають. Відповідно до звіту Risk Based Security про порушення даних за 2022 рік, «загальна кількість зламаних записів у 2022 році перевищила 37 мільярдів, що на 141% більше, ніж у 2021 році» [1]. Особисті записи користувачів системи регулярно піддаються злому і мільйони цих записів, включаючи імена, електронні адреси та паролі, стали предметом порушень конфіденційності персональних даних, у багатьох випадках навіть включаючи адреси, дати народження та фінансову інформацію [1].

Порушення даних відбувається через несанкціонований доступ до бази даних організації, що дозволяє кіберхакерам викрасти конфіденційну особисту інформацію, тобто персональні дані, такі як паролі, номери кредитних карток, номери соціальних рахунків та банківську інформацію [2]. Ці добре задокументовані випадки мали несприятливі наслідки, включаючи шахрайство з кредитними картками та крадіжку персональних даних, що може мати тривалі негативні наслідки для особи та на усунення яких часто потрібні місяці, якщо не роки [2]. Деякі з найбільших останніх кіберзломів включають злом бази даних Yahoo у 2013-2014 р. в результаті кібератаки, було відкрито базу з персональними даними понад 3 мільярдів користувачів. Хакери збирали імена користувачів, адреси електронної пошти, номери телефонів, дати народження, хешовані паролі та незашифровані відповіді на секретні запитання.

У 2017 році агентство кредитної звітності Equifax зазнало кібератаки, у результаті якої постраждали приблизно 143 мільйони користувачів. Системні адміністратори не знали про підозрілу активність протягом двох місяців і не повідомляли про злам цілий місяць після його виявлення. Вважається, що Equifax зламали китайські державні хакери, які займалися шпигунством [3]. Колективний фінансовий вплив на окремих жертв невідомий, а також невідомо, яку небезпеку та стратегічний збиток завдала держава, але

ці випадки підкреслюють потенційний ризик, коли ідентифікаційна інформація зберігається в централізованій базі даних.

Мета статті. Метою статті є дослідження і аналіз зарубіжного досвіду використання власне блокчейн технологій та алгоритмів консенсусу для захисту персональних даних та визначення пріоритетних та перспективних напрямів їх застосування в Україні.

РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ

Порушення кібербезпеки та конфіденційності

Більшість зібраних і збережених даних знаходяться під контролем державних урядів і організацій, які збирають персональні дані, за захист яких вони відповідають. У той же час ці організації можуть монетизувати ці набори даних, використовуючи їх для покращення власних операцій і пропозицій або продаючи їх третім особам. Обсяг даних, що генеруються та збираються, зростає експонентно, розширюючи коло користувачів. Консолідатори даних можуть зв'язувати елементи даних між джерелами даних і об'єднувати дані способами, яких не передбачали ні сторони, які збирали інформацію, ні користувачі, які її надали.

На сьогоднішній день в Україні продовжується війна з країною агресоркою росією. У таблиці 1 та таблиці 2 показано інтенсивність кібератак від початку повномасштабного воєнного вторгнення росії, вони не зменшується, хоча їхня якість – знижується. Найбільше, як і раніше, атакують Уряд і місцеві органи влади, оборонний, фінансовий, енергетичний сектори. Залишаються у полі зору кіберзловмисників також транспортна інфраструктура та телеком-галузь [4].

Таблиця 1

Кібератаки на основні сектори за перші місяці війни

Назва сектору	Кількість здійснених атак
Уряд і місцеві органи влади	179
Сектор безпеки та оборони	104
Фінансовий сектор	55
Комерційні організації	54
Енергетичний сектор	54
Інше	350

Таблиця 2

Найпоширеніші методи кібератак за перші місяці війни

Назва методу кібератаки	Кількість здійснених атак
Збір інформації зловмисником	242
Шкідливий програмний код	192
Втручання	92
Спроби втручання	82
Порушення доступності	56
Інше	132

Правила конфіденційності

Право на приватність вважається основним правом людини в багатьох частинах світу. Ця конфіденційність може поширюватися на право окремих осіб контролювати власні особисті дані. Це право необхідно ретельно захищати, оскільки володіння та управління особистими даними особи може вплинути на стосунки з іншими і навіть на особу власника даних [5].

Положення, що регулюють збір та керування персональними даними, швидко розробляються. Європейський Союз лідирує в законодавстві про конфіденційність через Загальний регламент захисту даних (GDPR), прийнятий у 2016 році. Закон вимагає від організацій, які збирають персональні дані про громадян ЄС для транзакцій із державами-членами ЄС, ретельно захищати ці дані та обов’язково забезпечити їхню конфіденційність.

GDPR визначає нові європейські стандарти у сфері приватності людини. Цей регламент замінив рамкову Директиву про захист персональних даних 95/46/ЄС від 1995 року. Він спрямований на те, щоб у людини було більше законних інструментів контролювати власні дані.

Українські компанії, що працюють на європейський ринок, вже стикаються з вимогами GDPR, оскільки вони обробляють персональні дані резидентів Європейського Союзу. Таким компаніям обов'язково необхідно відповідати усім вимогам GDPR, щоби захистити компанію від штрафних санкцій.

Україна отримала статус кандидата на членство в ЄС, й одним з наступних кроків стане проведення низки реформ — у тому числі тих, що стосуються захисту персональних даних. Українським компаніям варто не гаяти час, й вже задуматися щодо стратегії трансформації, а також використання інструментів та сервісів, які забезпечать виконання усіх вимог GDPR [6].

Відповідно до GDPR організації також повинні мати можливість виконувати свої зобов'язання щодо захисту даних: право [7]:

- знати, які особисті дані збираються;
- знати, чи продається вона чи розкривається та кому;
- відмовитися від продажу своїх персональних даних;
- отримати доступ до своїх персональних даних;
- вимагати від компанії видалення будь-яких персональних даних;
- не піддаватися дискримінації за реалізацію своїх прав на конфіденційність.

Закони про конфіденційність безпосередньо впливають на те, як працюють компанії, і вимагатимуть від компаній, які використовують дані споживачів, впровадження систем і операційних практик, які дозволять їм відповідати цим новим правилам. Технологія блокчейн і розділеної книги (DLT) має унікальне положення, щоб допомогти компаніям дотримуватися існуючих і потенційних майбутніх нормативних актів, які стосуються особистої власності та конфіденційності даних.

Блокчейн і конфіденційність

Серед значних переваг блокчейн-рішень є те, що вони дозволяють організаціям обмінюватися даними способами, які раніше були недоступними, відкриваючи можливості для покращеної співпраці, покращення операційної ефективності та збільшення прибутку. Питання про те, як зберегти конфіденційність даних, посилюються в цих середовищах, оскільки дані зберігаються в спільних книгах, які можуть бути доступні кільком учасникам блокчейну.

ConsenSys, компанія, що розробляє технології блокчейну, обговорюючи безпеку загальнодоступних блокчейнів, стверджує, що «насправді конфіденційність не є

властивістю будь-якого блокчейну. Швидше, існують рівні конфіденційності, які можна застосувати до будь-якого блокчейну…» [8]. Розробники повинні ретельно розглянути, яким сторонам дозволено читати та записувати транзакції, а також як трансакції транслюються, перевіряються та зберігаються. Додаткові питання, пов'язані з тим, як дозволи та заходи безпеки оновлюються та застосовуються, також є важливими міркуваннями. Рішення про те, кому належать дані та як дані можуть використовуватися організаціями та комп'ютерними програмами, ще більше ускладнюють обговорення конфіденційності [8].

Децентралізована ідентифікація

Самосуверенна ідентичність, широко поширена точка зору серед прихильників блокчейну, стверджує, що люди повинні контролювати свою власну ідентичність і мати автономію щодо того, як аспекти ідентичності діляться з іншими. Децентралізована ідентифікація (DID) — це втілення самостійної суверенної ідентифікації з підтримкою блокчейну, яка може значно покращити конфіденційність і безпеку персональних даних.

DID стосується індивідуального володіння персональними цифровими даними, що стосуються багатьох елементів ідентифікації. Корпорація Майкрософт, яка бере участь у визначенні стандартів DID, враховує особисту точку зору. «Наразі наша особистість і всі наші цифрові взаємодії належать і контролюються іншими сторонами, про деяких з яких ми навіть не підозрюємо [9]». Повернення права власності на дані особам, до яких ці дані належать, може принести переваги як цим особам, так і організаціям, які в іншому випадку відповідали б за захист даних.

Технологія блокчейн дає змогу DID і надає людям можливість зберігати власні дані поза базами даних сторін, з якими вони здійснюють операції. Дані належать і контролюються цими особами, і вказівники на ці дані або метадані можуть зберігатися в блокчейні та використовуватися для перевірки обґрунтованості претензій користувачів щодо їхніх особистих даних. Наприклад, бюро водійських прав може видати водійське посвідчення користувачу, яке користувач зберігає приватно. Якщо страхова компанія або інша сторона бажає перевірити, чи має користувач ліцензію, користувач може надати ліцензію стороні, наприклад страховій компанії, і сторона може самостійно перевірити емітента та дату закінчення терміну дії.

Будь-хто може створити DID. Коли цей ідентифікатор створюється вперше, до нього не додається жодна інформація. Згодом користувач міг додати водійські права або інші ідентифікаційні дані до цього DID. Процес, який може використовувати третя сторона для перевірки того, що певна особа володіє DID, подібний до процесу підтвердження того, що особа володіє адресою електронної пошти. Наприклад, обліковий запис онлайн-ігор можна приєднати до електронної адреси. Сторона, яка бажає підтвердити, що особа є власником цього облікового запису, може надіслати приватне повідомлення, наприклад код безпеки, на адресу електронної пошти та попросити особу надати цей код, що може бути зроблено лише особою, яка володіє паролем для цієї електронної пошти. адреса може надати.

На відміну від облікового запису електронної пошти, DID належатиме та зберігатиметься людині, а не постачальнику послуг електронної пошти. Пароль або закритий ключ також буде захищений власником. Особиста інформація, пов'язана з ідентичністю, може зберігатися в концентраторі ідентифікації — зашифрованому сховищі особистих даних, яке зберігається поза блокчейном, ймовірно, у поєднанні телефону, комп'ютера та хмарних даних або автономних пристроїв зберігання [9]. Завдяки використанню концентратора ідентифікації особа могла контролювати, якою інформацією ділитися із зовнішньою стороною.

DID зменшують ймовірність небажаної кореляції. Використання загальних ідентифікаторів, таких як адреси електронної пошти на різних веб-сайтах, створює так звану проблему кореляції. Кореляція в цьому контексті означає, що об'єкти можуть без згоди користувача пов'язувати інформацію про одну особу в кількох системах. Адреси електронної пошти використовують дані майже кожного веб-сайту. Коли користувачі надають ту саму адресу електронної пошти на різних сайтах разом із, можливо, додатковою особистою інформацією, як-от номер телефону чи фізичну адресу, вони несвідомо створюють потенціал для кореляції. У цьому випадку суб'єкти можуть співвідносити ці дані між сайтами. Відстеження файлів cookie та веб-клаців дозволяє зв'язувати ідентифікатори між веб-сайтами, що може призвести до того, що сторонні особи отримають повне уявлення про особу користувачів, де вони живуть, їх стать, вік, інтереси та іншу інформацію [9].

На рисунку 1 показано, як користувач кількох служб і онлайн-сайтів може зберігати дані в центральному місці, контрольованому користувачем, і взаємодіяти окремо з кожним постачальником послуг. Це дозволяє користувачеві контролювати конкретні фрагменти інформації, які може бачити кожен постачальник.

Рис. 1. Децентралізовані ідентифікатори та постачальники послуг

Федеративна ідентифікація з підтримкою блокчейн

DID можуть допомогти користувачам захистити та контролювати власні дані, а також визначити, хто отримає доступ до цих даних. Блокчейни також можуть підвищити безпеку для людей під час взаємодії з декількома інтернет-платформами або службами за допомогою використання децентралізованих федеративних ідентифікацій.

Блокчейни дозволяють об'єктам захищати конфіденційність індивідів — центральну для самосуверенної ідентичності[19.20]. Традиційно користувачі системи або набору систем володіють тим, що називається федеративною ідентифікацією, яку можна описати як єдину ідентифікацію, яка використовується окремими особами для доступу до послуг або інформаційних платформ, наданих декількома сторонами, за допомогою якої вмикається одна ідентифікація та визначається автентифікацією єдиного входу (SSO). Розглянемо мережу охорони здоров'я, яка включає кілька організацій, як-от лікарні, страхові компанії або клініки невідкладної допомоги, де постачальники дозволяють використовувати облікові дані єдиного входу або цифрову федеративну ідентифікацію для доступу до всіх послуг. Цей тип ідентичності, який зазвичай

зберігається та керується в центральному місці постачальником послуг, схильний до вразливості безпеки [10].

Розподілений характер технології блокчейн дає можливість мережам увімкнути єдиний вхід або об'єднані ідентифікатори набагато безпечніше. ElGayyar [11] пропонує структуру федеративної ідентифікації на основі блокчейну (BFID), де мережа самих провайдерів, а не централізована третя сторона, керує системою, ідентифікацією та автентифікацією користувачів. Будь-яка організація в мережі блокчейн може перевіряти облікові дані та видавати ідентифікаційні дані для будь-якого користувача в системі. У BFID усі транзакції записуються та обслуговуються в блокчейні, де система використовує переваги безпечного та незмінного характеру розподіленої книги, тим самим практично усуваючи можливість порушення ідентифікаційної інформації та потенційної крадіжки.

Фреймворки федеративної ідентифікації на основі блокчейну можна налаштувати як на державних, так і на приватних реалізаціях блокчейну та використовувати смарт-контракти, щоб реагувати на потенційні зміни правил, які можуть виникнути під час управління ідентифікацією в системі. Крім того, ці інфраструктури дозволяють користувачам перевіряти та контролювати, як використовуються їхні ідентифікаційні дані, а також надають мережевим бізнес-об'єктам можливість відстежувати, як використовуються їхні послуги, забезпечуючи покращення процесів і кращий загальний досвід користувача.

Докази з нульовим знанням

Підтвердження з нульовим знанням забезпечують легкий доступ до особистих даних та інших важливих даних, зберігаючи при цьому конфіденційність і контроль власності для окремих осіб. Докази з нульовим знанням — це криптографічні методи, за допомогою яких користувач або «доказник» може переконати когось або «верифікатор», що щось про них правдиве, не надаючи, не розкриваючи та не передаючи цю інформацію. Поширеним прикладом є клієнт, який намагається замовити алкогольний напій у бармена, який вимагає знати, що відвідувачу виповнився 21 рік або більше. Надання водійського посвідчення розкриває повну дату народження клієнта, а також зріст, колір очей і домашню адресу — інформацію, якою можна скористатися або вкрасти.

Докази з нульовим знанням використовують криптографічні алгоритми, які дозволяють перевіряючому математично продемонструвати, що твердження правильне, не розкриваючи жодних даних. Існує два типи доказів нульового знання: інтерактивні та неінтерактивні. Найчастіше протоколи з нульовими знаннями є інтерактивними, за допомогою яких перевіряючий (окрема особа або, швидше за все, комп'ютер) і верифікатор беруть участь у послідовному наборі запитань або викликів, які, якщо правильні відповіді задану кількість разів, дозволяють перевіряючому переконати верифікатор, з дуже високою ймовірністю, що заява, яку вони роблять, є істинною.

Приклад інтерактивного доказу нульового знання може включати дві кольорові кулі, ідентичні в усіх відношеннях, які приймають свій колір. Один червоний і один зелений. Припустімо, що верифікатор абсолютно не дальтонік і не може визначити колір будь-якої кульки. Ви хочете довести верифікатору, що кульки справді відрізняються за кольором. Перевіряючий кладе м'ячі за спину і показує один. Прувер вказує колір. Потім перевіряючий робить це ще раз і запитує, чи вони поміняли м'яч. Оскільки ви бачите різні кольори, ви можете з упевненістю сказати, що куля була замінена чи ні. Після кількох раундів цього стає більш статистично правдивим, що насправді є дві різні кулі,

оскільки ймовірність того, що ви зможете правильно вгадати знову і знову, падає майже до нуля [12].

Неінтерактивне підтвердження більше схоже на наведений вище приклад, коли відвідувач підтверджує свій вік бармену за допомогою підтверджувальної заяви, яка розкриває вік, але не містить додаткової інформації, яка може бути розкрита, якщо перевіряльник покаже своє фото. Доведення того, яке значення має карта в колоді з 52 карт, без ідентифікації її масті, може бути прикладом такого типу доказу. Прувер стверджує, що карта, яку вони тримають, — це король, але не хоче розкривати, якого короля — червового, бубнового, пікового чи трефового. Якщо криптографічний рядок також містить інформацію, яка розкриває інші 48 карт, жодна з яких не є королем, ми можемо знати напевно, що перевіряльник справді має якогось короля.

Підтвердження з нульовим знанням — це потужні інструменти для збереження конфіденційності та контролю власності для осіб, яким може знадобитися надати трохи особистої інформації, але не більше, ніж це абсолютно необхідно.

Як висновок ми можемо побачити, що блокчейн – це розподілена і децентралізована технологія, яка не має центрального органу для перевірки надійності інформації та транзакцій. З цієї причини, починають діяти консенсусні алгоритми. Алгоритми консенсусу вважаються серцевиною технології блокчейн і відіграють важливу роль у забезпеченні дійсності щойно доданого блоку. У наступному розділі обговорюються різні типи механізмів консенсусу.

Механізми досягнення надійності в блокчейні

Дані у блокчейні повинні бути цілісні та добре захищені від зловмисників. Алгоритми консенсусу якраз виконують такі функції, тому вони є чи не найважливішим елементом технології блокчейн. Оскільки дані у блокчейні розподілені і немає якогось одного серверу, розподілені учасники системи повинні якось узгоджувати валідацію транзакцій, що надходять до мережі. Важливо відрізняти алгоритм консенсусу від поняття протоколу [13].

Протокол описує правила, за якими працює система – як повинні взаємодіяти учасники мережі, які дані вони можуть передавати, які вимоги до успішної валідації блоків. У той же час, алгоритм виконує роль механізму, який перевіряє, що правила встановлені протоколом, виконуються – він валідує баланси та підписи, що підтверджують транзакції, а також фактично виконує перевірку блоків.

Консенсус означає, що всі сторони погоджуються щодо конкретного рішення. Що стосується мережі блокчейн, члени мережі досягають консенсусу щодо вмісту блокчейну. Блокчейн – це децентралізована система, що складається з різних суб'єктів, які діють в залежно від власних інтересів та наявної у них інформації. Всякий раз, коли нова транзакція транслюється по мережі, вузли можуть включити цю транзакцію в копію свого реєстру або проігнорувати її. Коли більшість учасників мережі приймають рішення про прийняття певного стану, досягається консенсус. Фундаментальною проблемою в розподілених обчисленнях і багатоагентних системах є досягнення загальної надійності системи при наявності ряду неробочих процесів. Найчастіше для цього потрібно, щоб процеси узгодили між собою деяке значення, яке знадобиться під час обчислення. Ці процеси описуються як консенсус. Щоб консенсусний протокол був безпечним, він повинен бути відмовостійким [14].

Наразі існує безліч алгоритмів консенсусу, що використовуються в різноманітних протоколах блочейнів:

− PoW (Proof-of-Work, доказ працею);

− PoS (Proof-of-Stake, доказ ставкою);

− BFT (Byzantian-Fault-Tolerance);
− Apache Kafka;
− DPoS (Delegated-Proof-of-Stake, делегований доказ ставкою);
− PoC (Proof-of-Capacity, доказ зберіганням даних);
− PoET (Proof-of-Elapsed-Time, доказ очікуванням);
− BFT (Byzantian-Fault-Tolerance).

Proof-of-Work (PoW)

Один з найпопулярніших консенсусів, для того аби отримати доступ до загального ресурсу, користувач повинен обчислити достатньою складну, але обчислювальну задачу, аби запобігти зловживанням ресурсів [15].

Суть концепції така, що усім майнерам дається задача, яку вони повинні порахувати за певний проміжок часу (у мережі Bitcoin цей час становить приблизно 10 хвилин). Задача – «Знайти таке значення x, щоб хеш SHA(x) містив N старших нульових біт».

У мережі Bitcoin час вирішення задачі більш менш сталий, тому що кількість біт, яку треба вирахувати динамічна і залежить від кількості учасників. Функція, що вираховується – SHA-256. Коли один учасник мережі (майнер) знайде 45 правильну відповідь, усі інші звіряються з ним. І коли більшість завалідує знайдення відповіді – консенсус досягнуто, блок записано.

Майнери мають свій інтерес у цьому, адже за кожну записану і підтверджену транзакцію вони отримують плату. І якщо людина хоче щоб її транзакція швидше потрапила до мережі, можна запропонувати майнерам більшу плату – тоді час очікування валідації транзакції зменшиться. Але у такого алгоритму є й мінус – він вимагає багато енерговитрат та потужного апаратного забезпечення.

Proof-of-Stake (PoS)

Другий за популярністю алгоритм консенсусу. У цьому підході майнерам теж доводиться хешувати дані, але тут складність знову ж таки залежить від балансу. У порівнянні з Proof-of-Work, цей алгоритм не потребує великих енерговитрат.

Також до переваг можна віднести те, що задля проведення атаки на таку мережу, зловмиснику необхідно отримати більше токенів і тоді йому стане просто невигідно знецінювати власний токен. Але тут теж є недоліки – може з’явитися група осіб, що спробує тримати токени тільки у своїх руках. У такому разі під сумнів може ставитися сама ідея децентралізації мережі [16].

Delegated-Proof-of-Stake (DPoS)

Delegated-Proof-of-Stake – ще одна альтернатива Proof-of-Work та разом з тим вдосконалення Proof-of-Stake. Суть алгоритму полягає у тому, що учасник може передати свою «роботу» іншим.

Можна делегувати свій голос іншому учаснику мережі, і той буде підтримувати роботу мережі від імені іншого. Оскільки це удосконалий PoS, то 46 чим більше баланс токенів, тим більшу вагу має голос учасника. У такій системі, як правило, винагорода за записаний блок ділиться між учасниками, що проголосували за того, хто власне записав блок.

Перевага у порівнянні з класичним Proof-of-Stake – учасники мотивовані працювати чесно, адже у будь-який момент за вас можуть перестати голосувати. До того ж, він працює швидше, ніж класичний варіант.

Proof-of-Authority (PoA)

Блоки записують перевірені валідатори, що завчасно обираються та по факту є модераторами системи [17]. Тут мають цінність не кількість токенів, а репутація.

Таким чином блокчейн за певним алгоритмом обирає валідатора, який запише наступний блок.

Важливо зазначити, що просто так стати валідатором важко, адже треба вкласти певну кількість грошей, а також заробити довіру інших учасників мережі, аби ті голосували за нього. Але такий процес гарантує, що валідатором стане не пересічна людина.

Proof-of-Importance (PoI)

Цей алгоритм надає перевагу користувачам, які отримали хорошу репутацію у мережі – «спочатку ви працюєте на репутацію, потім вона на вас». Репутація зростає з активним життям у екосистемі блокчейну та взаємодії з іншими учасниками. Чим краща репутація – тим більший шанс на створення наступного блоку [18].

Proof-of-Importance вирішує проблему Proof-of-Stake коли один учасник або група людей мали можливість контролювати мережу, отримавши більше токенів. Тут же кількість токенів на балансі не збільшують шанси на створення блоку. До 47 того ж, коштами треба активно користуватися, адже торгувати ними вигідніше, аніж просто тримати на балансі.

Таблиця 3

Порівняльний аналіз різних алгоритмів знаходження консенсусу

Алгоритм	Ціль	Переваги	Недоліки
Proof of Work, PoW	Забезпечення складності у формі обчислювального завдання, щоб надати можливість обміну даними між ненадійними учасниками.	Важко досягти відмови в обслуговування (атакаDDoS неефективна)Відкритий для всіх, у кого є обладнання, щоб вирішити обчислювальне завдання.	Високе обчислювальне навантаження, високе енергоспоживання Потенціал для 51% атаки, отримавши достатню обчислювальну потужність.
Proof of Stake, PoS	Забезпечення менш складної у обчислювальному плані перешкоди для додавання нових блоків, ніж у PoW, щоб надати можливість обміну даними між ненадійними учасниками.	Менш вимогливий у обчисленнях, ніж PoW. Відкритий для всіх.	Зацікавлені сторони контролюють систему. Існує можливість формуванню пулу зацікавлених сторін для створення централізованої влади. Потенціал для 51% атаки.
Delegated PoS	Створення механізму консенсусу через «демократію», де учасники голосують (використовуючи криптографічно підписані повідомлення), щоб вибрати та відкликат права делегатів	Вибрані делегати економічно мотивовані залишатися чесними. Менш вимогливий у обчисленнях, ніж PoW	Найменша різноманітність вузлів, ніж у PoW або в чистих реалізаціях PoS Оскільки всі делегати «відомі», у виробників блоків може бути стимул змовлятися, ставлячи під загрозу безпеку
Proof of Authority/ Identity, PoA, PoI	Створити централізований процес погодження, щоб мінімізувати час створення блоків та швидкість підтвердження	Швидкий час підтвердження. Дозволяє збільшити темпи виробництва блоків. Може використовуватися в sidechain, які використовують іншу модель консенсусу	Вважається, що валідуючий вузол не був скомпрометований. Існує центральна точка відмови
Round- robin	Забезпечити систему для додавання блоків серед довірених вузлів	Низька обчислювальна потужність. Ідея проста в розумінні.	Вимагає великої довіри серед вузлів.

Будучи децентралізованою та розподіленою системою, блокчейн потребує певного механізму перевірки блоків, які мають бути доданим до існуючого блокчейну. Механізми досягнення консенсусу життєво важливі для функціонування розподілених систем. На сьогоднішній день найбільшим вдалим введення було використання Proof of Work, що дозволяє користувачам погоджуватися із загальним набором фактів.

Алгоритми консенсусу сьогодні лежать в основі не лише систем цифрових грошей, а й блокчейнів, що дозволяють розробникам запускати код у розподіленій мережі, що у свою чергу дає можливість якісніше та надійніше захищати персональні дані користувачів. В даний час алгоритми є наріжним каменем блокчейн-технології та мають вирішальне значення для довгострокової життєздатності різних існуючих мереж.

Персональні дані і взагалі конфіденційні дані не повинні бути довірені стороннім особам, де вони будуть вразливі до атак і неправильного використання. Натомість користувачі повинні володіти і контролювати свої дані без шкоди для їх безпеки. Алгоритм консенсусу у свою чергу від користувачів не вимагає довіряти будь-яким третім сторонам та завжди користувачі можуть бути у курсі про дані, які збираються про них і як вони використовуються.

У додаток, блокчейн розпізнає користувачів як власників своїх персональних даних. З усіх алгоритмів консенсусу, Proof of Work залишається домінуючим. Більш надійної та безпечної альтернативи поки що не запропоновано. Тим не менш, існує величезна кількість досліджень і розробок в області заміни PoW у майбутньому.

ВИСНОВКИ

Технологія блокчейну вдосконалюються швидкими темпами та створює можливості для обміну та об’єднання даних у спосіб, який раніше не передбачався. Водночас прогрес у цій технології відкриває нові можливості для етичного використання даних. Передача персональних даних створює головоломку для компаній і окремих осіб, що може принести цінні переваги, але також може створити великі ризики та витрати як для особи, так і для організацій, з якими надаються особисті дані.

Блокчейн надає нові механізми, такі як децентралізовані ідентифікаційні дані та підтвердження з нульовим знанням, які дозволяють обмінюватися даними таким чином, щоб зберегти конфіденційність особи та дозволити користувачам зберігати контроль над своїми власними даними. Ці досягнення можуть забезпечити як підвищену кібербезпеку, так і більш етичне використання персональних даних. Учасники блокчейну можуть досягти цих результатів шляхом ретельної розробки структур і механізмів управління.

Також ході роботи були проаналізовані п’ять алгоритмів консенсусу: PoW, PoS, DPoS, PoA, PoI. На сьогодні це базові та найпопулярніші алгоритми консенсусу, втім серед нерозглянутих у статті алгоритмів теоретично можуть бути більш підходящі алгоритми консенсусу, ніж навіть PBFT. Для оцінки та порівняння алгоритмів консенсусу, а також обґрунтованого вибору алгоритму консенсусу для оптимізації роботи блокчейн запропоновано використовувати такі ключові характеристики ціль, переваги та недоліки. Розглянуті показники були сформовані, базуючись на огляді літературних джерел та технічної документації щодо конкретних алгоритмів консенсусу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 RiskBased Security. 2022 Year End Report: Data Breach Quickview. https://flashpoint.io/resources/report/state-of-data-breach-intelligence-2022-midyear/

2 Kellerman, R. Five of the Biggest Data Breaches of the 21st Century. STAGE2DATA. https://www.stage2data.com/five-of-the-biggest-data-breaches-of-the-21st-century/
3 Fruhlinger, J. Equifax Data Breach FAQ: What Happened, Who was Affected, What was the Impact? https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
4 Держспецзв'язку: Статистика кібератак за чотири місяці війни. https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni
5 Heister, S., Yuthas, K. (2020). The blockchain and how it can influence conceptions of the self. *Technology in Society*, *60*, 101218. https://doi.org/10.1016/j.techsoc.2019.101218
6 GDPR. https://www.konicaminolta.ua/uk-ua/rethink-work/security/1000-days-of-gdpr-what-have-businesses-learned
7 Що таке ідентифікаційна інформація для GDPR? https://www.groundlabs.com/blog/what-is-pii-for-gdpr/
8 Consensys. Busting the Myth of Private Blockchains. https://consensys.net/enterprise-ethereum/best-blockchain-for-business/busting-the-myth-of-private-blockchains/
9 Microsoft. Decentralized Identity. https://www.microsoft.com/en-us/security/business/identity/own-your-identity
10 Mir, S., Capretz, M. A. M., Grolinger, K., ElYamany, H. F., ElGayyar, M. M. (2020). Blockchain-based federated identity and auditing. *International Journal of Blockchains and Cryptocurrencies*, *1*(2), 179. https://doi.org/10.1504/ijbc.2020.10031109
11 Lesavre, L, Varin, P, Mell, P, Davidson, M, Shook, J. A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. https://csrc.nist.gov/publications/detail/white-paper/2019/07/09/a-taxonomic-approach-to-understanding-emerging-blockchain-idms/draft
12 Доведення з нульовим розголошенням. https://uk.wikipedia.org/wiki/%D0%94%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%BD%D1%8F_%D0%B7_%D0%BD%D1%83%D0%BB%D1%8C%D0%BE%D0%B2%D0%B8%D0%BC_%D1%80%D0%BE%D0%B7%D0%B3%D0%BE%D0%BB%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D1%8F%D0%BC
13 Camenisch, J., Dubovitskaya, M., Enderlein, R. R., Lehmann, A., Neven, G., Paquin, C., Preiss, F.-S. (2020). *IFIP Working Conference on Policies and Research in Identity Management*, *19*, 25 - 44.
14 Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
15 Camenisch, J., Kiayias, A., Yung, M. (2019). On the Portability of Generalized Schnorr Proofs. *EUROCRYPT 2019 (LNCS)*, *5479*, 425 – 442.
16 Coinmarketcap. https://coinmarketcap.com/
17 Creating a Trusted Experience with Blockchain. Sony Global Education. https://blockchain.sonyged.com/
18 Ekblaw, A., Azaria, A., Halamka, J. (2021). Case Study for Blockchain in Healthcare: «MedRec» prototype for electronic health records and medical research data. *MIT Media Lab, Beth Israel Deaconess Medical Center*, *13*, 1–13.
19 Василишин, С., Опірський, І. (2022). Перспективи військового застосування технології блокчейну. *НАУ: «Безпека інформації», 28*(2), 57-66.
20 Василишин, С., Опірський, І. (2022).Розробка безпеки систем електронного урядування на основі блокчейну». *НАУ: «Захист інформації», 24*(2), 58-70.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (20), 2023
ISSN 2663 - 4023

Valeriia S. Balatska
Cybersecurity department postgraduate
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-6262-6792
valeriia.s.balatska@lpnu.ua

Ivan R. Opirskyy
Dc.S., Professor, Professor of Information Security Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8461-8996
ivan.r.opirskyi@lpnu.ua

ENSURING THE CONFIDENTIALITY OF PERSONAL DATA AND SUPPORTING CYBER SECURITY WITH THE HELP OF BLOCKCHAIN

Abstract. The recent increase in security breaches and digital surveillance highlights the need to improve privacy and security, especially of users' personal data. Advances in cybersecurity and new legislation promise to improve the protection of personal data. Blockchain and distributed ledger (DTL) technologies provide new opportunities to protect user data through decentralized identification and other privacy mechanisms. These systems can give users greater sovereignty through tools that allow them to own and control their own data.
The purpose of the article is to research blockchain technology and mechanisms for achieving reliability in blockchain for the protection and security of personal data.
Decentralized and federated identity systems give users control over what, when and how much of their personal information can be shared and with whom. These systems can also reduce cybersecurity threats. Through various consensus algorithms, blockchain-based privacy solutions allow users to better manage their data and ensure that the data and models derived from it are more accurate, honest and reliable.

Keywords: blockchain, consensus algorithm, personal data, privacy.

REFERENCES

1 RiskBased Security. 2022 Year End Report: Data Breach Quickview. https://flashpoint.io/resources/report/state-of-data-breach-intelligence-2022-midyear/
2 Kellerman, R. Five of the Biggest Data Breaches of the 21st Century. STAGE2DATA. https://www.stage2data.com/five-of-the-biggest-data-breaches-of-the-21st-century/
3 Fruhlinger, J. Equifax Data Breach FAQ: What Happened, Who was Affected, What was the Impact? https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
4 Derzhspetszviazku: Statystyka kiberatak za chotyry misiatsi viiny. https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni
5 Heister, S., Yuthas, K. (2020). The blockchain and how it can influence conceptions of the self. *Technology in Society*, *60*, 101218. https://doi.org/10.1016/j.techsoc.2019.101218
6 GDPR. https://www.konicaminolta.ua/uk-ua/rethink-work/security/1000-days-of-gdpr-what-have-businesses-learned
7 Shcho take identyfikatsiina informatsiia dlia GDPR? https://www.groundlabs.com/blog/what-is-pii-for-gdpr/
8 Consensys. Busting the Myth of Private Blockchains. https://consensys.net/enterprise-ethereum/best-blockchain-for-business/busting-the-myth-of-private-blockchains/
9 Microsoft. Decentralized Identity. https://www.microsoft.com/en-us/security/business/identity/own-your-identity
10 Mir, S., Capretz, M. A. M., Grolinger, K., ElYamany, H. F., ElGayyar, M. M. (2020). Blockchain-based federated identity and auditing. *International Journal of Blockchains and Cryptocurrencies*, *1*(2), 179. https://doi.org/10.1504/ijbc.2020.10031109

11 Lesavre, L, Varin, P, Mell, P, Davidson, M, Shook, J. A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. https://csrc.nist.gov/publications/detail/white-paper/2019/07/09/a-taxonomic-approach-to-understanding-emerging-blockchain-idms/draft
12 Dovedennia z nulovym rozgholoshenniam. https://uk.wikipedia.org/wiki/%D0%94%D0%BE%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%BD%D1%8F_%D0%B7_%D0%BD%D1%83%D0%BB%D1%8C%D0%BE%D0%B2%D0%B8%D0%BC_%D1%80%D0%BE%D0%B7%D0%B3%D0%BE%D0%BB%D0%BE%D1%88%D0%B5%D0%BD%D0%BD%D1%8F%D0%BC
13 Camenisch, J., Dubovitskaya, M., Enderlein, R. R., Lehmann, A., Neven, G., Paquin, C., Preiss, F.-S. (2020). *IFIP Working Conference on Policies and Research in Identity Management*, *19*, 25 - 44.
14 Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
15 Camenisch, J., Kiayias, A., Yung, M. (2019). On the Portability of Generalized Schnorr Proofs. *EUROCRYPT 2019 (LNCS)*, *5479*, 425 – 442.
16 Coinmarketcap. https://coinmarketcap.com/
17 Creating a Trusted Experience with Blockchain. Sony Global Education. https://blockchain.sonyged.com/
18 Ekblaw, A., Azaria, A., Halamka, J. (2021). Case Study for Blockchain in Healthcare: «MedRec» prototype for electronic health records and medical research data. *MIT Media Lab, Beth Israel Deaconess Medical Center*, *13*, 1–13.
19 Vasylyshyn, S., Opirskyi, I. (2022). Perspektyvy viiskovoho zastosuvannia tekhnolohii blokcheinu. NAU: *«Bezpeka informatsii»*, *28*(2), 57-66.
20 Vasylyshyn, S., Opirskyi, I. (2022).Rozrobka bezpeky system elektronnoho uriaduvannia na osnovi blokcheinu». *NAU: «Zakhyst informatsii»*, *24*(2), 58-70.