doi: https://doi.org/10.15407/visn2024.07.031

КУДІН
Антон Михайлович —
член-кореспондент НАН України, професор кафедри математичних методів захисту інформації Фізико-технічного інституту Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», головний експерт управління безпеки інформації департаменту безпеки Національного банку України

БЛОКЧЕЙН У КІБЕРБЕЗПЕЦІ: ТЕОРІЯ І ПРАКТИЧНЕ ЗАСТОСУВАННЯ

Стенограма доповіді на засіданні Президії НАН України 1 травня 2024 року

У доповіді зазначено, що використання блокчейн-технологій є одним із пріоритетних напрямів досліджень для вирішення завдань забезпечення кібербезпеки та захисту інформації. Найбільш перспективним застосуванням блокчейну для кіберзахисту можна вважати побудову ефективних протоколів узгодження, використання блокчейнів як елементів нових систем виявлення вторгнень та раннього попередження про кіберзагрози, побудову перспективних криптосистем на базі блокчейнів, пошук ефективних практичних рішень на основі блокчейн-технологій для завдань у галузі економіки і юриспруденції.

Шановний Анатолію Глібовичу!
Шановні колеги!
Вашій увазі пропонується доповідь, присвячена використанню блокчейн-технологій у кібербезпеці.

Спочатку доцільно ввести деякі означення для термінів, якими ми оперуватимемо надалі. По-перше, це термін «блокчейн», який найбільш зручно пояснити через його частковий випадок — криптовалюту. Впродовж усієї історії розвитку людської цивілізації гроші, як загальний еквівалент обміну, пройшли певний еволюційний шлях — від предметів натурального обміну до платіжних карток, у яких грошима по суті є цифрові записи на рахунках. Вершиною цієї еволюції на сьогодні є блокчейн.

Криптовалюта являє собою практично ті самі банківські рахунки, але, на відміну від них, при використанні криптовалюти немає єдиного центру емісії грошей. Історично першою криптовалютою був біткоїн, основним складником якого і є технологія блокчейну. Замість грошей у біткоїні використовується реєстр боргових розписок (хто кому і скільки винен грошей), ідентичні копії якого розміщені на кожному вузлі блокчейн-мережі. Зміни до реєстру вносяться виключно за допомогою додавання записів (блоків) за спеціальним протоколом консен-

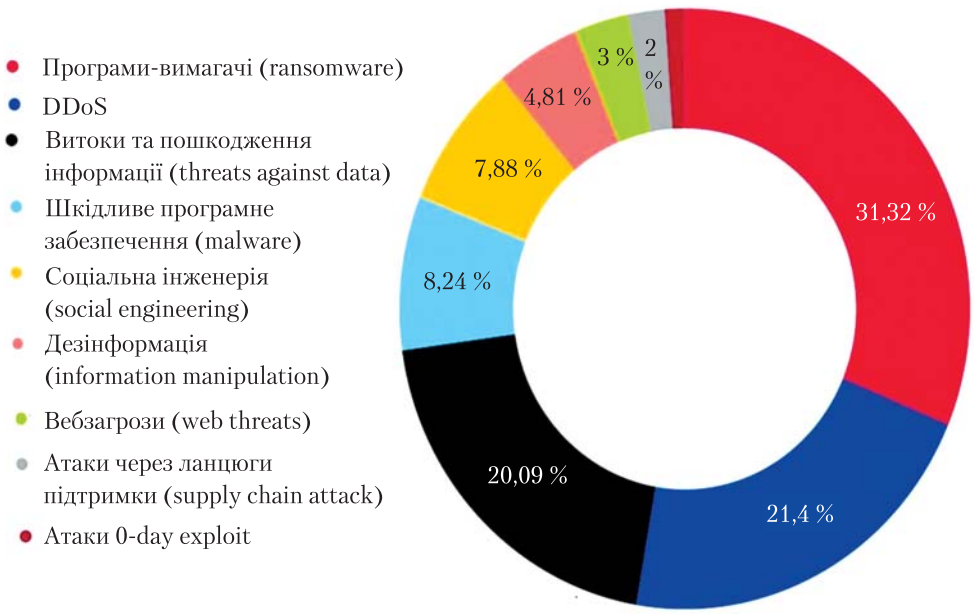

Рис. 1. Розподіл кіберінцидентів за типами загроз (за даними звіту ENISA)

сусу, тобто колегіально. Цілісність інформації і довіра до всіх дій та результатів забезпечується криптографічними механізмами захисту.

Якщо абстрагуватися від типу даних, які обробляє така мережа, тобто розглядати не лише боргові записи, а й будь-який інший тип даних, наприклад програмний код, ми й приходимо до поняття «блокчейн».

Отже, *блокчейн* (від англ. blockchain — ланцюжок блоків) — це децентралізована інформаційна система, в якій оброблення інформації здійснюється колегіально, під управлінням протоколу консенсусу між елементами системи.

Інший часто вживаний термін *майнінг* (від англ. mining — видобуток корисних копалин) означає діяльність, спрямовану на підтримання блокчейн-мережі та генерацію нових блоків за протоколом консенсусу, і, відповідно, *майнер* — один із типів учасників мережі, які здійснюють таку діяльність. Ця назва історично походить від вузлів блокчейну, які використовують протокол Proof-of-Work і для додавання нового блока мають виконати «складну роботу» з обчислення прообразу геш-функції.

Отже, анатомію блокчейну можна описати як розподілену децентралізовану базу даних, ідентичні копії якої зберігаються у всіх учасників мережі, а протоколи оброблення інформації (модифікації, додавання тощо) засновано на протоколах консенсусу різних типів — Byzantine Fault Tolerance, Proof-of-Work, Proof-of-Stake та ін.

Ще одне поняття, без якого складно обійтися, коли йдеться про блокчейн-технології, — це «кіберпростір». Згідно з українським законодавством, *кіберпростір* — це середовище (віртуальний простір), яке уможливлює здійснення комунікацій та/або реалізацію суспільних відносин і утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Кіберпростір є системою з елементами самоорганізації та децентралізації. Структури даних і процеси, які використовуються в системі, мають бути адекватними принципам функціонування системи, і саме тому в сучасних кіберсистемах застосовують блокчейн-технології та їхні похідні (криптовалюти, смарт-контракти тощо), а також розподілені й хмарні технології.

Крім того, самі кіберзагрози стають все більш децентралізованими. Так, у звіті Агент-

ства ЄС з кібербезпеки* (European Union Agency for Cybersecurity — ENISA) зазначено, що серед головних загроз, які існують на сьогодні в кіберпросторі, перше місце посідають програми-вимагачі, що, як правило, вимагають викуп у вигляді криптовалюти, а друге місце — розподілені атаки на відмови в обслуговуванні (DDoS-атаки), які для керування ними використовують блокчейн-технології (рис. 1).

Особливості моделей загроз у сучасному кіберпросторі ставлять перед безпекою інформації та кібербезпекою такі нові виклики:

1) стрімкий розвиток і доступність інформаційних технологій веде до докорінного змінення кіберпростору, зокрема до розширення можливостей для віддаленої роботи, розвитку Інтернету речей, соціальних мереж, криптовалют та криптобірж, технологій електронних виборів, смарт-контрактів тощо, а отже, кіберпростір стає все більш розподіленим та децентралізованим;

2) відбувається міграція принципів побудови інформаційних систем загального призначення до сфери автоматизованих систем керування критичною інфраструктурою і відповідна міграція загроз з інформаційних систем загального призначення до сфери керування об'єктами критичної інфраструктури;

3) сучасні «інтелектуальні» атаки (APT-атаки) в кіберпросторі можуть здійснюватися впродовж тривалого часу, з латентним періодом, що дуже ускладнює їх виявлення, а підготовка до APT-атаки має не автоматичний, а організаційно-технічний характер. Реалізація APT-атак, як правило, здійснюється організованими угрупованнями кіберзлочинців, і ці атаки стають все більш розподіленими та децентралізованими;

4) у галузі кібербезпеки та безпеки інформації дедалі частіше відбувається міграція від поняття *security* (безпека інформації) до поняття *assurance* (довіра до інформації).

Отже, блокчейн можна вважати новим етапом у розвитку технологій децентралізованих додатків і технологій забезпечення довіри (*assurance*), які все частіше застосовують у різноманітних задачах кібербезпеки. Основними ознаками децентралізованих додатків (наприклад, краудфандингу, краудсорсингу, краудтестингу, краудвестингу тощо) є відкритий код, внутрішня валюта (токени), децентралізований консенсус, відсутність центральної точки відмови.

Застосування блокчейн-технологій у кібербезпеці можна розглядати у трьох аспектах: *теоретичному*, *системоутворювальному* та *прикладному*. Теоретичне значення блокчейнів для кібербезпеки полягає в тому, що блокчейн-технології є однією з основ створення децентралізованих систем у сучасному, все більш розподіленому та децентралізованому кіберпросторі. Системоутворювальний аспект полягає у формуванні обчислювальних систем на засадах блокчейну, а прикладний — у застосуванні блокчейнів для побудови захищених систем децентралізованих додатків.

В Україні склалися кілька наукових шкіл, які досліджують проблеми, пов'язані зі стійкістю, безпекою та застосуванням блокчейнів. Це, по-перше, школа академіка НАН України Валерія Костянтиновича Задіраки (Інститут кібернетики імені В.М. Глушкова НАН України) з розроблення теорії оцінки рівня інформаційної та кібербезпеки в децентралізованих системах на базі математичних моделей теорії інформації і теорії оптимальних алгоритмів. По-друге, це школа члена-кореспондента НАН України Олексія Миколайовича Новікова (Фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського») з розроблення теоретичних засад та методів використання блокчейн-технологій для вирішення завдань інформаційної та кібербезпеки. По-третє, це наукова школа під керівництвом члена-кореспондента НАН України Володимира Володимировича Мохора (Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України) з практичного застосування блокчейн-технологій у галузі енергетики та юриспруденції.

* https://www.enisa.europa.eu/news/eu-elections-at-risk-with-rise-of-ai-enabled-information-manipulation

Основними проблемами, які досліджують ці наукові школи, є такі:

1) створення нових протоколів консенсусу, ефективних за швидкодією та стійких до атак централізації;

2) розроблення нових криптосистем на основі блокчейнів;

3) оцінка стійкості наявних протоколів консенсусу та криптовалют;

4) створення нових систем захисту інформації та кіберзахисту на основі блокчейнів;

5) розроблення прикладних децентралізованих систем, основаних на блокчейнах, у тому числі систем смарт-контрактів, криптовалют, криптобірж тощо;

6) вирішення економічних завдань, пов'язаних з віртуальними активами, криптовалютами, криптобіржами.

Кожна з цих проблем породжує специфічні завдання, деякі з яких уже вдалося успішно вирішити. Так, що стосується першої проблеми зі **створення нових протоколів консенсусу**, то поточна ситуація характеризувалася обчислювальною неефективністю й низькою швидкодією наявних протоколів консенсусу Proof-of-Work, а також їх нестійкістю до поширених видів атак (DSA та ін.). Запропоноване рішення полягало у зміненні підходу до обчислення функції консенсусу: перехід від обчислень на основі загальної теорії оптимальних алгоритмів до застосування чебишевського радіусу інформації. Це означає, що рейтинг, за яким обирається майнер наступного блока, залежить як від обчислювальних ресурсів майнера, так і від інформації, яка необхідна майнеру для розв'язання задачі з потрібною точністю.

У результаті було розроблено новий протокол консенсусу Proof-of-Accuracy Blockchain Consensus Protocol зі швидкодією, яка в тисячу разів перевищує швидкодію класичного блокчейну біткоїна. При цьому ймовірність здійснення атак на блокчейн є значно нижчою, ніж у разі використання протоколів Proof-of-Work. Створений протокол було успішно реалізовано в системі Advanced Distributed Ledger, розробленій на замовлення компанії Samsung Electronics Ukraine.

Ідея для вирішення проблеми зі **створення нових криптосистем** полягала у використанні для побудови таких систем замість неінтерактивних протоколів доказів із нульовими знаннями нових криптографічних конструкцій на основі блокчейну. Було виконано кілька науково-дослідних робіт, за результатами яких розроблено нові криптографічні протоколи з блокчейн-ядром на основі протоколу консенсусу типу Proof-of-Accuracy. На відміну від відомих протоколів на основі NZnP, до протоколів Proof-of-Accuracy неможливо застосовувати атаку типу brute-force. Побудовано нову аксіоматику криптосистем на основі інформаційно-обчислювального підходу. При цьому як загальний вимір стійкості криптосистем також обрано чебишевський радіус інформації.

Проблемою **оцінки стійкості наявних протоколів консенсусу та криптовалют** займається переважно наукова група під керівництвом Людмили Василівни Ковальчук з Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. Дослідники довели, що в разі застосування відомих протоколів, зокрема протоколу Proof-of-Work, потрібно враховувати синхронізацію в мережі. Так, у класичному випадку зловмиснику для здійснення атаки необхідно контролювати більш як 50 % обчислювальних ресурсів мережі, але якщо зловмисник синхронізований набагато краще, ніж чесні майнери (наприклад, існує один локальний майнінговий пул), то йому, щоб керувати блокчейном, вистачить і 45 % чи навіть 30 % контролю над мережею.

Проведено практичні розрахунки необхідного для повного контролю над блокчейном відсотку контролю обчислювальної потужності мережі залежно від часу затримки поширення інформації в мережі.

Створення нових систем захисту інформації та кіберзахисту на основі блокчейнів ґрунтується на розумінні того, що децентралізовані додатки на основі блокчейнів змінюють кіберпростір та генерують нові кіберзагрози, а відповідно, мають змінюватися і засоби кіберзахисту. При розробленні нових систем раннього безшаблонного виявлення вторгнень

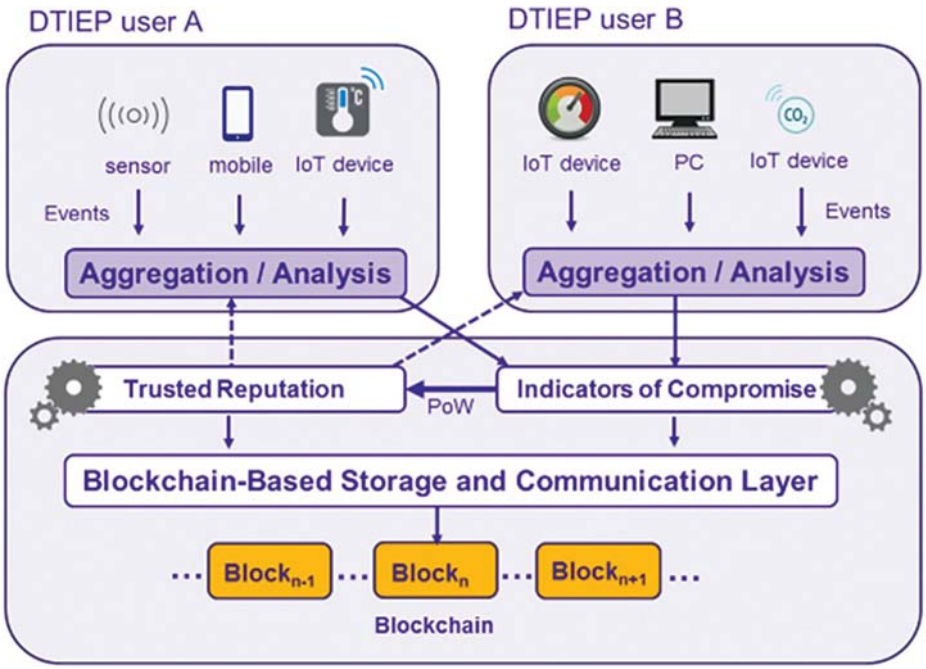

Рис. 2. Схема використання блокчейну для аналізу кіберінцидентів

на базі блокчейну виникають труднощі як теоретичного характеру (складність створення адекватних метрик стану безпеки інформації та атак у сучасних системах; неузгодженість даних спостережень від сенсорів із різними метриками; довіра до таких сенсорів), так і практичного (відсутність впровадження сучасних моделей у комерційні системи; використання для виявлення/блокування атак переважно «сигнатурних» систем; проблеми з впровадженням систем, заснованих на виявленні аномалій).

Таку розподілену децентралізовану систему раннього виявлення вторгнень зі збереженням репутації джерел було створено в рамках виконання проєкту CRDF Global Project A Distributed System for Early Intrusion Detection and Assessment of Cybersecurity G-202102-67499. У цій системі рівень false/positive є в рази меншим, ніж у наявних системах (рис. 2).

З використанням блокчейну можна підвищити ефективність систем захисту інформації (систем виявлення та протидії вторгненням (IDS/IPS), фільтрації контенту, безпечних поштових шлюзів (SMG)) завдяки побудові на основі блокчейн-технологій репутаційних списків IP-адрес, інформаційних ресурсів, поштових адрес тощо. Крім того, із застосуванням блокчейну можна створювати нові методи організації систем моніторингу та аналізу інцидентів (SIEM-системи), а також нові методи побудови анонімних систем поширення інформації про кіберінциденти.

Отже, підсумовуючи проведені нами дослідження, можна виокремити такі найважливіші результати:

• розроблено ефективні за швидкодією та стійкі в теоретико-інформаційному сенсі нові протоколи консенсусу;

• створено нові криптографічні протоколи з блокчейн-ядром, що вирізняються підвищеною швидкодією та стійкістю до криптоаналізу;

• розроблено децентралізовану систему раннього виявлення вторгнень на основі безшаблонного виявлення аномалій та збереження репутації в блокчейні;

• отримано нові оцінки стійкості класичних протоколів криптовалют.

Основною перевагою використання блокчейн-технологій у криптографії та кіберзахисті є їхня децентралізованість та здатність до самоуправління, що підвищує живучість і

швидкість адаптації до змінення систем, створених на їх основі.

Найбільш перспективними напрямами застосувань блокчейну в кібербезпеці можна вважати такі:

• створення нових криптосистем та систем кіберзахисту з децентралізованими системами довіри;

• використання блокчейн-технологій як елементів нових систем виявлення вторгнень та раннього попередження про кіберзагрози, систем моніторингу кіберінцидентів;

• розроблення систем обчислень на блокчейнах;

• створення прикладних децентралізованих систем, зокрема систем смарт-контрактів, наприклад для p2p-продажу «зеленої» електроенергії, криптовалют, криптобірж тощо;

• аналіз стійкості блокчейнів з різними протоколами до основних відомих атак (розгалуження, подвійної витрати, цензурування, атак на смарт-контракти тощо) та розроблення методів захисту від таких атак.

Дякую за увагу!

Anton M. Kudin

National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
National Bank of Ukraine, Kyiv, Ukraine

ORCID: https://orcid.org/0000-0002-3966-6489

BLOCKCHAIN IN CYBERSECURITY: THEORY AND PRACTICAL APPLICATION

Transcript of scientific report at the meeting of the Presidium of the NAS of Ukraine, May 1, 2024

The report states that the use of blockchain technologies is one of the priority fields of research for cyber- and information security. The most promising applications of blockchain for cybersecurity include building effective consensus protocols, new early intrusion detection systems for cyber threats using blockchains as elements, creating advanced blockchain-based cryptosystems, and finding effective solutions for tasks in the field of economics and law based on blockchain technologies.

Cite this article: Kudin A.M. Blockchain in cybersecurity: theory and practical application. *Visn. Nac. Akad. Nauk Ukr.* 2024. (7): 31—36. https://doi.org/10.15407/visn2024.07.031