УДК 004.056

О. В. Салієва
В. Ю. Лаврик

ВИКОРИСТАННЯ СМАРТ-КОНТРАКТІВ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація

Робота присвячена використанню смарт-контрактів для захисту інформації користувачів у повсякденному житті. Проведено аналіз смарт-контрактів, розглянуто їхні ключові елементи, виділено основні переваги й недоліки їх використання.

Ключові слова: *смарт-контракт, блокчейн, захист даних, Біткоін, Ethereum, Solidity.*

Annotation

The paper is is devoted to the use of smart contracts to protect user information in everyday life. The analysis of smart contracts was carried out, their key elements were considered, the main advantages and disadvantages of their use were highlighted.

Keywords: *smart contract, blockchain, data protection, Bitcoin, Ethereum, Solidity..*

Вступ

У сучасній інформаційній парадигмі смарт-контракти представляють собою програмні коди, що автоматизують та виконують угоди на блокчейн-платформах. Смарт-контракти – це комп'ютерні аналоги звичайних договорів, спеціальні програми (алгоритми), які виконує якісь дії при виконанні сторонами угоди певних умов [1]. Вони базуються на розподіленій технології та використовують код для визначення, виконання та здійснення умов угод. Загальна практика використання смарт-контрактів охоплює сферу фінансів, логістики, медицини та інших секторів, де вони дозволяють автоматизувати та оптимізувати процеси безпосередньо між учасниками системи. Одним з ключових аспектів використання смарт-контрактів є їхній потенціал для захисту даних. Криптографічні методи, вбудовані в смарт-контракти, забезпечують конфіденційність інформації, а також гарантують її цілісність. Такий механізм дозволяє уникнути ризиків порушення безпеки даних, забезпечуючи високий рівень захисту в цифровому середовищі.

Результати дослідження

Смарт-контракти, як концепція, вперше виникли на початку 1990-х років завдяки відомому криптографу Ніку Сабо, який введенням цього терміну намагався охарактеризувати "набір обіцянок, виражених у цифровій формі, включаючи протоколи, в яких сторони дотримуються цих обіцянок" [1]. У 1998 році даний термін був застосований для опису об'єктів на рівні служби управління правами в системі "The Stanford Infobus" [2]. Ця система була частиною Стенфордського проекту цифрової бібліотеки та визначалася високим рівнем цифрової функціональності.

У 2014 році один із засновників платформи Ethereum Віталік Бутерін, висунув власну концепцію для удосконалення мережі Біткоїн. Протягом наступного року вже було виведено на ринок Ethereum-платформу, створену для реалізації тих самих поліпшень, що пропонував Бутерін. Одним із головних інноваційних аспектів Ethereum стало можливе використання автономних смарт-контрактів, які автоматизують виконання угод на базі програмного коду, спрощуючи та ускладнюючи взаємодію учасників в цифровому середовищі.

Існує поширена думка, що технологія смарт-контрактів є винятковою для платформи Ethereum. У реальності, вже з моменту запуску в 2009 році Bitcoin використовує досить розгалужену мову смарт-контрактів під назвою Script [3]. Фактично, концепція смарт-контрактів існувала ще до створення Ethereum. Основна відмінність між мовою контрактів Bitcoin та Ethereum полягає в тому, що Ethereum використовує концепцію повної обчислювальної машини Тьюрінга. У зв'язку з цим, мова розумних контрактів Ethereum, така як Solidity, дозволяє складати більш складні угоди, розширюючи можливості їх аналізу.

Ключовими компонентами смарт-контракту є:

– алгоритм для захисту даних сторін. Учасники угоди, забезпечені алгоритмом захисту, що засвідчує цілісність даних та відповідність вимогам, викладеним раніше, в контексті товару чи послуги;

– предмет договору – товар чи послуги, які потрібно відправити чи надати в обмін за фінансові ресурси. Цей елемент визначає конкретні умови та параметри транзакції;

– умови виконання – конкретні умови, які визначають, коли та як відбудеться автоматичний обмін елементами договору. Наприклад, це може бути відповідність поставленого товару стандартам якості, з якими пов'язана математична специфікація;

– механізм захисту даних – впровадження ефективних криптографічних методів для захисту конфіденційності та цілісності даних, які передаються та обробляються смарт-контрактом. Це може включати в себе використання шифрування та хеш-функцій для забезпечення безпеки інформації в процесі виконання угоди;

– децентралізована платформа – організація, яка дозволяє написання алгоритму (програмного коду) смарт-контракту та забезпечує його функціонування. Ця платформа виступає як основний носій смарт-контрактів та забезпечує їхню автономність та безпеку в екосистемі.

Забезпечення захисту даних через смарт-контракти може бути реалізовано за допомогою різноманітних криптографічних та технічних заходів.

Основні варіанти захисту даних в смарт-контрактах включають:

– шифрування даних – застосування алгоритмів шифрування для забезпечення конфіденційності даних, що знаходяться в смарт-контракті. Таким чином, лише уповноважені сторони можуть розшифрувати та отримати доступ до конкретної інформації;

– хешування для цілісності – використання хеш-функцій для створення "відбитка" даних. Цей відбиток служить як унікальний ідентифікатор, і зміна навіть найменших даних призведе до зміни хешу. Такий механізм дозволяє виявляти неправомірні зміни в даних [5];

– мультипідписи – використання технології мультипідписів, де для виконання деякої операції необхідно підпис декількох учасників. Це підвищує рівень безпеки, оскільки для зміни чи доступу до даних потрібні підтвердження від декількох сторін;

– контроль доступу – впровадження механізмів контролю доступу, що обмежують права доступу до певних частин контракту. Такі обмеження можуть бути встановлені на рівні читання, запису чи виконання конкретних функцій;

– анонімізація – використання технік анонімізації для забезпечення конфіденційності особистих даних. Це може включати в себе використання анонімних адрес та транзакцій для приховування особистої інформації;

– концепція «права на забуття» – реалізація механізму видалення чи архівування даних після закінчення строку їхньої актуальності або після виконання певних умов;

– використання ролей для управління доступом – впровадження концепції ролей для управління доступом до різних функцій смарт-контракту. Кожній стороні або учаснику може бути призначена конкретна роль з визначеними правами, обмежуючи їхні можливості та доступ до певних даних.

Застосування різноманітних технік захисту даних в смарт-контрактах, таких як шифрування, хешування, мультипідписи, контроль доступу та використання ролей, є критично важливим для забезпечення безпеки та довіри в цифровому середовищі. Ці техніки працюють у комбінації для створення повноцінного захисту даних, маючи ряд переваг для користувачів та учасників угод.

Як у будь-якої технології, у смарт-контрактів є як переваги, так і недоліки.

Переваги:

– економія часу та ресурсів;

– більш низькі витрати, так як немає потреби в послугах посередників;

– додаткова безпека від використання блокчейна;

– більш швидка перевірка умов виконання контракту.

Недоліки:

– можуть бути помилки та вразливі місця в програмному коді смарт-контракту. Так, внаслідок хакерської атаки на проект «The DAO» в липні 2016 року зловмисникам вдалося вивести з системи 64 млн. доларів [4];

– складність в побудові алгоритму коду, оскільки потрібно передбачити всі можливі варіанти розвитку подій;

– ймовірність втрати ключів доступу або паролів до смарт-контракту сторонами угоди;

– система сприймає умови контракту з точністю, без урахування форс-мажорів;

– немає законодавчої бази використання смарт-контрактів.

Але всі ці недоліки не такі суттєві. Адже ймовірність втрати ключів чи форс-мажорні ситуації є більше людським фактором. І для усунення таких помилок пропонується використовувати більше блокових тестів для контрактів, проведення аудитів або ж перевірки на відкритих веб-ресурсах тестування. Тому, можна впевнено говорити що переваг у захисті даних за допомогою смарт-контрактів більше і їх поширення варто прогнозувати в майбутньому.

Висновки

Із отриманих результатів дослідження, можна зробити висновки, що використання смарт-контрактів є чудовим способом для забезпечення цілісності даних користувачів у цифровому середовищі. Застосування технік криптографії, таких як шифрування та хешування, в поєднанні з механізмами контролю доступу та використання ролей, надає надійний механізм захисту інформації в смарт-контрактах. Смарт-контракти дозволяють автоматизувати та стандартизувати виконання угод, забезпечуючи прозору та ефективну обробку даних. Мультипідписи та розподіл ролей сприяють вдосконаленню системи управління доступом. В свою чергу, анонімізація та шифрування гарантують конфіденційність особистої інформації. Таким чином, використання смарт-контрактів дозволяє користувачам не лише ефективно взаємодіяти в цифровому середовищі, але й має високий потенціал для захисту та збереження цілісності їхніх даних. Це стає ключовим аспектом створення атмосфери довіри в онлайн-середовищі, забезпечуючи користувачам спокій та впевненість у надійності та безпеці їхніх цифрових угод.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Nick Szabo. Smart Contracts. 1994. URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html (accessed 18.11.2023)
2. Martin Röscheisen, Michelle Baldonado, Kevin Chang, Luis Gravano, Steven Ketchpel, Andreas Paepcke The Stanford InfoBus and Its Service Layers. Stanford, August 8, 1997. 28 p. URL: http://ilpubs.stanford.edu:8090/318/1/1998-25.pdf (accessed 18.11.2023)
3. Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2009. 9 p. URL: https://bitcoin.org/bitcoin.pdf (accessed 18.11.2023)
4. Cryptopedia Staff. What Was The DAO? March 16, 2022. URL: https://www.gemini.com/cryptopedia/the-dao-hack-makerdao#section-the-dao-hack-remedy-forks-ethereum (accessed 18.11.2023)
5. Private Smart Contracts Using Homomorphic Encryption, Rand Hindi, May 23, 2023. URL: https://www.zama.ai/post/private-smart-contracts-using-homomorphic-encryption (accessed 18.11.2023)

Салієва Ольга Володимирівна – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: salieva8257@gmail.com

Лаврик Владислав Юрійович – студент групи 2КІТС-22м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: lavrikvlad0107@gmail.com

Saliieva Olha V. *- doctor of philosophy (PhD) in specialty 125 "Cybersecurity", associate professor of the department of management and security of information systems, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@gmail.com.*

Lavryk Vladyslav Y. *- student of group 2KITS-22m, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: lavrikvlad0107@gmail.com*