УДК 004.056

АЛГОРИТМ АНАЛІЗУ БЛОКЧЕЙН МЕРЕЖІ ETHEREUM ДЛЯ ВИЯВЛЕННЯ НЕЗАКОННОЇ ДІЯЛЬНОСТІ

Е. В. Абдуллаєва[1,a], Л. Ю. Гальчинський[1]

[1] Навчально-науковий Фізико-технічний інститут

Анотація

Робота присвячена дослідженню блокчейн мережі задля виявлення незаконної діяльності. У цій роботі описано поняття та основні вразливості, що стосуються мережі Ethereum. Під дослідженням розуміється створення алгоритму форензіки протоколу Ethereum для виявлення злочинності в мережі. Результати проведеного дослідження можливо застосуватя для програмної реалізації аналізу та подальшого покращення рівня безпеки блокчейн мережі.

Ключові слова: блокчейн, аналіз мережі, Ethereum, вразливості, форензіка

Вступ

За останні роки спостерігається стрімке зростання та широке впровадження технології блокчейн, зокрема у сфері криптовалюти. Ethereum, будучи однією з провідних платформ у цій сфері, не лише зруйнував традиційні фінанси, але також відкрив нові двері для інновацій та розвитку. Проте, децентралізований та відкритий характер мережі Ethereum також створює значну проблему з точки зору стримування різних форм незаконної діяльності, таких як відмивання грошей, фінансування тероризму та кіберзлочинність. Розуміння та врахування ризиків, пов'язаних зі злочинною діяльністю в мережі Ethereum, дає можливість забезпечити довгострокову стійкість і розвиток цієї технології.

1. Постановка задачі

Мета роботи базується на ознайомлені з основними вразливостями мережі Ethereum, створення алгоритму форензіки цієї мережі, здатного ефективно виявляти незаконну діяльність. Побудова алгоритму розбору різних частин блокчейн мережі базується на різних метриках, які дозволять оцінити стан мережі при дослідженні окремої транзакції або адреси гаманця користувача. До того ж, використання шаблону аналізу дає змогу підвищити рівень безпеки блокчейн протоколу.

2. Вразливості протоколу Ethereum

2.1. Огляд основних понять протоколу Ethereum

Ethereum – це блокчейн-платформа з відкритим кодом, яка дозволяє розробникам створювати та розгортати смарт-контракти та децентралізовані програми (dApps)[1]. Кожен вузол у мережі підтримує копію реєстру, а консенсус досягається через децентралізований механізм, що забезпечує довіру та безпеку. Провівши огляд мережі Ethereum, можна виділити основні концепції протоколу[2, 3]:

- Децентралізовані програми (dApps): це програми, створені на основі блокчейну Ethereum. Вони використовують смарт-контракти, щоб забезпечити децентралізовану безнадійну взаємодію між користувачами, не покладаючись на центральний орган влади.
- Смарт-контракти: це самовиконувані контракти з умовами угоди, записаними безпосередньо в коді. Вони автоматично виконують заздалегідь визначені дії, коли виконуються певні умови, усуваючи потребу в посередниках.
- Віртуальна машина Ethereum (EVM): це децентралізована віртуальна машина, яка виконує смарт-контракти в мережі Ethereum. Він ізолює кожне виконання смарт-контракту в безпечному середовищі ізольованого програмного середовища, забезпечуючи загальну безпеку та стабільність мережі.
- Механізм консенсусу: Ethereum спочатку використовував Proof of Work (PoW) як механізм консенсусу, схожий на біткойн. Однак з тих пір Ethereum перейшов на консенсусний механізм Proof of Stake (PoS), який називається Ethereum 2.0. PoS забезпечує кращу енергоефективність, безпеку та масштабованість порівняно з PoW.

2.2. Основні вразливості протоколу Ethereum

Ethereum, як децентралізована платформа, має власний набір вразливостей і проблем. Деякі з основних вразливостей протоколу Ethereum представлені нижче[2]:

1. Атака 51%. Тип атаки на протокол блокчейну,

[a]esmira.abdullaeva@gmail.com

який відбувається, коли один суб'єкт або група контролює понад 51% обчислювальної потужності мережі. Цей контроль дозволяє зловмиснику маніпулювати блокчейном, скасовуючи транзакції, запобігаючи підтвердженню нових транзакцій або навіть створюючи нові блоки та додаючи їх до блокчейну. Може призвести до руйнування цілої мережі блокчейн, оскільки вона підриває фундаментальну безпеку та довіру до мережі.

2. Вразливості смарт-контрактів. Гарантування виконання угоди буде відповідати логіці, прописаній в смарт-контраті та після виконання попередньо визначеної логіки кінцевий стан мережі залишиться незмінним. Проте, правильне виконання коду смарт-контракту не може гарантувати його повну безпеку. Ключовими вразливостям можна вважати[4]:
   - Помилки кодування: смарт-контракти написані на різних мовах програмування, а це в свою чергу вимагає від розробників обережності. Будь-які помилки коду можуть призвести до небажаних наслідків, зокрема до втрати коштів або несанкціонованого доступу.
   - Атаки повторного входу: атака, яка відбувається при вдалій спробі зловмисника неодноразово викликати функцію в смарт-контракті до завершення її початкового виконання.
   - Маніпуляції з часовими мітками: контроль часових позначок майнерами, може призвести до потенційних маніпуляцій, які впливатимуть на результат виконання смарт-контракту.
   - Відсутність конфіденційності: інформація у блокчейні загальнодоступна, отже доступ до коду смарт-контракту може спричинити проблеми з конфіденційністю.
   - Ризики централізації: при децентралізації самого блокчейну, смарт-контракти можуть покладатися на централізовані служби або компоненти, які можуть створювати єдині точки відмови або довіри.
3. Вразливості алгоритму консенсусу. Зловмисник, який отримує старі закриті ключі, потенційно може створити альтернативний ланцюжок, починаючи зі старого блоку, що призведе до реорганізації ланцюжка та атак подвійного витрачання[2].
4. Фрагментація мережі. Тимчасовий або постійний поділ мережі блокчейну на окремі підмережі, які не з'єднані між собою, призводить до фрагментація мережі. Це може статися через різні причини, включаючи помилки програмного забезпечення, затримку мережі, DDoS-атаки або навіть навмисні спроби порушити роботу мережі.

3. Алгоритм форензіки мережі Ethereum

В основу алгоритму дослідження було покладено етапи блокчейн форензіки, до яких входить[5, 6]:

- збір даних;
- аналіз даних;
- візуалізація результатів;
- представлення доказів;
- закриття розслідування.

І у ході дослідження було розроблено алгоритм проведення аналізу блокчейн мережі на основі протоколу Ethereum, який буде використано для написання програмної реалізації на мові програмування Python. Даний алгоритм наведено на рис. 1. Було розроблено 4 основних етапи аналізу мережі. Варто розібрати кожен з них більш детально:

1. Першим етапом аналізу варто виокремити збір даних. Використання бібліотеки `web3.py` дозволяє зібрати точні дані про транзакцій для певного діапазону блоків або періоду часу. Для зручної реалізації варто використати сервіс infura.io, який пропонує легкий доступ до Ethereum через кінцеві точки API без необхідності налаштовувати та підтримувати власні повні вузли. Метод, який буде використовуватись для збору інформації – `get_transaction()`: метод, що проходить по блоку транзакцій, розділяє їх та виокремлює основні дані кожної з них, такі як:
   - `"hash"` – геш транзакції;
   - `"from"` – відправник;
   - `"to"` – отримувач;
   - `"value"` – сума проведеної транзакції;
   - `"gasPrice"` – комісія за виконання транзакції.
2. Другий етап, основний, сам процес аналізу отриманих даних. Нижче наведені методи, які будуть використані для аналізу:
   - `count_transactions_in_block()` – метод, який підраховує кількість отриманих транзакцій з блоку.
   - `address_balance()` – метод, який надає дані про баланс адреси.
   - `suspicious_transactions()` – метод, який виявляє транзакції, які пов'язані з адресами гаманців з чорного списку.
   - `find_bots()` – метод, що знаходить можливу активність боту.
   - `monitor_large_transactions()` – метод, який виявляє транзакції, що були проведені на великі суми.
   - `high_frequency()` – метод, який виявляє транзакції, які проводяться з великою частотою.
3. Візуалізація графа транзакцій – є одним з ключових етапів, виявлення порушень в мережі й буде виокремлено в окремий етап – третій. Розпізнавання щільно пов'язаних між собою адрес, тобто мережевої кластеризації, допоможе виявити закономірності та структури в мережі,

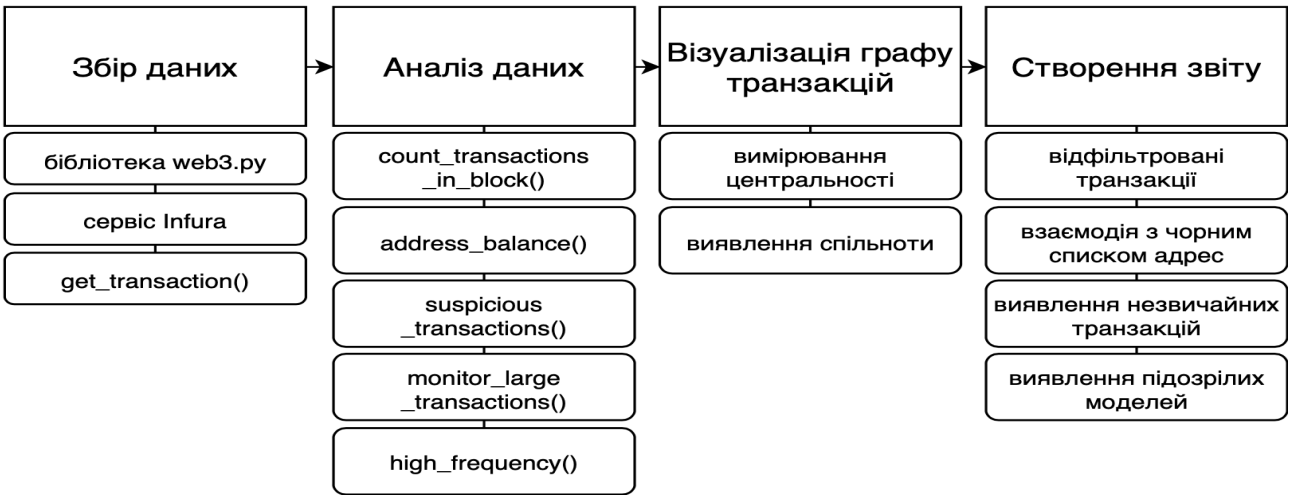

Рис. 1. Алгоритм форензіки мережі Ethereum

які інакше було б важко розпізнати. Виявлення цих кластерів може допомогти розпізнати скоординовану діяльність, потенційні злочинні мережі чи інші цікаві моделі. Основний метод:

- аналізу візуалізації, щоб ідентифікувати потенційно підозрілі шаблони або кластери адрес.

4. Останній, четвертий етап - це створення звітності по проведеному аналізу. Цей етап включає в себе наступне:
   - створення звіту, який буде містити відфільтровані транзакціями та список адрес, які взаємодіють із адресами з чорного списку;
   - виділення будь-яких помітних моделі або незвичайних транзакції для подальшого дослідження.

3.1. Метрики ідентифікації незаконної діяльності

Блокчейн форензіка передбачає використання аналітичних методів та інструментів для дослідження та відстеження транзакцій у мережі блокчейнів. Щоб розпочати аналіз, важливо визначити основні криміналістичні показники блокчейна. Ці показники будуть використані для відстежування потіку коштів і оцінювання безпеки мережі та надання доказів правоохоронним органам. Детальну таблицю сформовану в ході дослідження, можна знайти за посиланням "Метрики". До основних метрик відносяться:

- обсяг транзакції;
- вартість транзакції;
- баланс адреси;
- коефіцієнт кластеризації;
- комісія за транзакцію.

4. Висновки

У даному дослідженні розглядались принцип роботи, основні вразливості блокчейн мережі на основі протоколу Ethereum, було створено алгоритм аналізу мережі для виявлення незаконної діяльності. На початку було проведено огляд основних понять протоколу Ethereum та вразливостей, які найчастіше зустрічаються в ньому. Хоч це і децентралізована платформа, вона не ідеальна та має власний набір вразливостей і проблем. Проаналізувавши вразливості, було запропоновано алгоритм аналізу та дослідження блокчейн мережі на предмет незаконної діяльності. Метою створення цього алгоритму є спроба допомогти незаконну діяльність, таку як відмивання грошей, шахрайство та інші незаконні операції. Використання отриманої інформації можливе для створення справ проти окремих осіб або організацій, які займаються незаконною діяльністю. Загалом, аналіз мережі Ethereum є важливим інструментом для підтримки безпеки та цілісності блокчейну, а також для забезпечення його використання в законних цілях.

Перелік використаних джерел

1. What is blockchain technology? — URL: https://www.ibm.com/topics/blockchain.
2. *Топчій М.*, *Гальчинський Л.* Підвищення рівня безпеки смарт-контрактів у мережі Ethereum від шахрайства за рахунок використання ревесивних токенів. — 2022-11-11. — С. 14—21.
3. *Goyal H.*, *B. S.* Blockchain Forensics in Policing and It's Global Scenario // Lupine Publishers. — 2022-05-25.
4. Blockchain: A new perspective in cyber technology / T. Venkat Narayana Rao, P. P. Likhar, M. Kurni, S. K. — 2022. — P. 33–66.
5. *Salisu S.*, *Filipov V.*, *Penne B.* Blockchain Forensics: A Modern Approach to Investigating CyberCrime in the Age of Decentralisation. — 2022-06-30.
6. *T. K.* Digital forensics of cryptocurrency wallet. — 2022-05-20. — P. 14–21.