УДК 004.421

ДОСЛІДЖЕННЯ ОСОБЛИВОСТЕЙ РОБОТИ ПРОТОКОЛУ КРИПТОВАЛЮТИ ETHEREUM

Масальська Олена Олександрівна [1], Мєшков Вадим Ігорович [2]
ДВНЗ «Національний гірничий університет», http://bit.nmu.org.ua/,
E-mail: elmasalskaya@yandex.ua [1], local@i.ua [2]

В роботі розглянуто особливості роботи протоколу криптовалюти Ethereum. Розглянуті вразливості та недоліки роботи алгоритму ДАО (децентралізована автономна організація Ефіріума).

Ключові слова – криптовалюта, Ефіріум, Ethereum, Біткойн, Bitcoin, вразливості криптовалюти, децентралізована автономна організація

ВСТУП

На сьогоднішній день широкого застосування набувають ідеї відходу від традиційних грошей та розвитку грошей електронних. Найвідомішою електронною валютою (або криптовалютою) є Біткойн (Bitcoin). Але через особливості свого алгоритму, Біткойн зараз знаходиться на фінальній стадії генерації монет і із часом поступиться в популярності більш новим криптовалютам, таким як, наприклад, Ефіріум (Ethereum) [1].

Ефіріум позиціонує себе як принципово нова платформа для додатків. Це відразу і платформа, і мова програмування, яка дозволяє розробнику створювати і публікувати розподілені додатки наступного покоління. Ефіріум є різновидом Біткойн, що використовує повну за Тюрінгом мову програмування замість простої мови сценаріїв. Причина цього полягає в тому, що Ефіріум підтримує смарт-контракти. Ефір, внутрішня валюта Ефіріума, діє як «знак обміну» всередині цієї децентралізованої мережі. Мережа може використовуватися для шифрованої і безпечної передачі будь-яких видів інформації: результатів голосування, доменного імені, процесів управління компанією, договорів та угод, а також для спрощення обороту смарт-власності, операцій на фінансових біржах і «краудфандінга» [2].

ОСОБЛИВОСТІ РОБОТИ АЛГОРИТМУ ЕФІРІУМ

Децентралізована Ефіріума концепція запозичена у мережі Біткойн. Однак, протокол Ефіріума є відкритим. Його скриптова мова (на відміну від безальтернативного розрахунку хеш-функції та застосування сценаріїв в Біткойн) може використовуватись для побудови будь-якої програми. При цьому, оригінальну програму можна описати будь-якою мовою програмування з подальшим виконанням в «хмарі». Ефіріум об'єднує переваги технології «блокчейн» і переваги Тюрінг-повних мов програмування.

Окремі облікові одиниці, кожна з яких має назву «1 Ефір» (1 Ethereum – ринкова ціна складає 9,97119548$ – дані на 13 листопада 2016р.), виступають будівельними блоками. Блоки функціонують всередині загальної мережі. Кожен з них являє собою комп'ютерну програму, у якій є свій власний баланс, пам'ять і код. На їх основі будуються додатки з відкритим вихідним кодом.

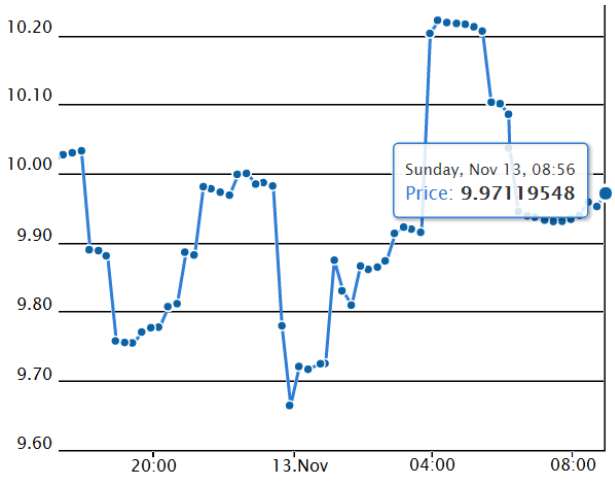

Рисунок 1. Ринкова ціна 1 Ethereum / 1 US Dollar (джерело: https://www.coingecko.com).

На алгоритмі Ефіріума заснований відомий проект «ДАО» (децентралізована автономна організація) - краудфандінговий проект, який позиціонує себе як організація, заснована на хмарному коді, яка не є юридичною особою і керована колективно усіма її інвесторами. Тобто, ДАО закрита і сама керує собою: її програмний код здійснює свою діяльність автономно, а внутрішні правила є невід'ємною і незмінною частиною Ефіріум-блокчейна [3]. ДАО володіє наступними характеристиками:

- по-перше, слід зазначити абсолютну неупередженість у відборі учасників. Використовуючи реалізацію розумних контрактів від Ефіріум, ДАО дозволяє бажаючим з усього світу брати участь в управлінні загальним фондом коштів. Учасники, що підтримали проект, отримують DAO-токени для подальшого їх використання в голосуванні та іншої діяльності компанії.
- по-друге, ДАО – це гнучка структура. Це проявляється в тому, що принцип роботи організації дозволяє підтримувати пропозиції будь-якого характеру, будь то створення корисного для неї продукту, вкладення коштів у венчурні проекти для отримання прибутку або їх спрямування на благодійні потреби (порятунок китів, наприклад). Учасники можуть проголосувати за виділення коштів на

пропозиції інноваційного характеру, за подальшу практичну реалізацію яких візьмуться залучені виконавці.

- по-третє, ДАО може отримувати прибуток з розроблюваних в рамках проекту продуктів або послуг. З клієнтів стягується плата, а потенційний прибуток може бути спрямований на подальше зростання організації або просто конвертований в ДАО-токени і розподілений серед учасників проекту.

ВРАЗЛИВОСТІ ТА НЕДОЛІКИ АЛГОРИТМУ

При всій своїй зовнішній привабливості Ефіріум не позбавлений деяких недоліків. Наприклад, є одна частина системи, яка не захищена криптографічно. Припустимо, за товар відправлено 100 монет, і нехай це цифровий товар з миттєвою доставкою. Далі зловмисник переводить ті ж монети собі, і намагається переконати мережу, що друга угода повинна знаходиться на першому місці, і саме вона є справжньою. Для цього йому буде потрібно роздвоїти ланцюжок блоків. А, так як найдовший ланцюжок за замовчуванням є правдою, зусилля зловмисника в кінцевому рахунку приречені на невдачу. Але це звичайно, до тих пір, поки він не зосередить 51% потужності мережі в одних руках [4].

Також у червні 2016 року, в коді ДАО (платформи для автономного управління інвестиційним капіталом), був виявлений несподіваний «баг», який дозволив хакеру витонченими методами вивести деяку кількість коштів. Ця вразливість була експлуатована невідомою стороною, якій вдалося перемістити близько однієї третини валюти Ефіріум, наявної в ДАО (на той час на суму близько 50 мільйонів доларів США), в одну з дочірніх ДАО, контроль над якою був тільки в атакуючої сторони. Однак, завдяки особливості реалізації ДАО всі ці кошти були недоступні для виведення протягом місяця. Розглянемо більш докладно принцип атаки [3].

Припустимо учасник ДАО хочу вийти з інвестиційної схеми та вивести свої кошти з проекту. Для цього йому необхідно надати ДАО частину свого власного коду з транзакцією для передачі йому Ефіріум-монет. Код Ефіріум є рекурсивним, що означає, що функція, що реалізує Ефіріум, може визивати сама себе.

На цьому етапі може виникнути помилка, що полягає в тому, що, коли викликається функція Ефіріума, вона буде викликати код одержувачів для передачі Ефіріум-монет, після чого код одержувачів буде викликаний ще раз, перш ніж закінчити процес. Це змушує процес повторюватися, передаючи більше Ефіріум-монет, ніж потрібно насправді (рисунок 2).

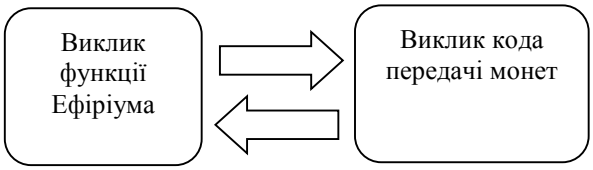

Рисунок 2. Рекурсивний виклик функції Ефіріума

Цей процес може тривати нескінченно, поки не дістане всі монети ДАО, що зможуть бути використані зловмисником за місяць.

Тобто, Ефіріум має вразливості, що закладені самим математичним алгоритмом (навіть, не його програмною реалізацією), усунути які на сьогоднішній день не представляється можливим. Але великим полем для діяльності є часовий проміжок в місяць, в який зловмисник ніяк не зможе використати монети, отримані в процесі атаки. Тобто, актуальним напрямком наукових досліджень є пошук методів «відкату» операцій зловмисника з метою повернення нелегально здобутих коштів законному власникові. Але не треба забувати й про правовий аспект питання: всі дії з повернення коштів повинні проводитися тільки після однозначної ідентифікації факту порушення, що само собою являю нетривіальний процес.

ВИСНОВКИ

Протокол Ефіріума був задуманий як модернізована версія криптовалюти, що забезпечує розширені функції за допомогою вельми узагальненої мови програмування. Він дозволяє підтримувати довільні контракти, що теоретично можуть бути створені для будь-якого типу транзакцій або додатків. Протокол Ефіріума сьогодні вийшов далеко за межі тільки валюти. Поняття довільної функції стану переходу, що реалізована протоколом Ефіріума, забезпечує платформу з унікальним потенціалом, що це дуже добре підходить в якості основного шару для дуже великого числа фінансових і нефінансових протоколів в наступні роки за умови знаходження ефективного алгоритму нейтралізації розглянутих вразливостей.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ethereum. Вікіпедія [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Ethereum

2. Ethereum. Блог [Електронний ресурс]. – Режим доступу: https://blog.ethereum.org/

3. Bitcoin конференція [Електронний ресурс]. – Режим доступу: https://bitcoinconf.com.ua/ru/news/4-samie-prodavaemie-knigi-o-bitcoin-obzor/

4. О Биткоине и блокчейне. Форум [Електронний ресурс]. – Режим доступу: https://forum.bits.media/index.php?/topic/21907-piat-neobkhodimykh-knig-o-bitkoine-i-blokcheine/