УДК 331.101.38:331.2

Г. І. Тибінка,
к. е. н., доцент кафедри менеджменту,
Львівський національний університет імені Івана Франка
ORCID ID: https://orcid.org/0000-0001-6730-1877
О. Б. Юрченко,
к. е. н., доцент кафедри обліку і аудиту,
Львівський національний університет імені Івана Франка
ORCID ID: https://orcid.org/0000-0002-3941-6340
А. С. Стойко,
аспірант кафедри менеджменту,
Львівський національний університет імені Івана Франка
ORCID ID: https://orcid.org/0009-0009-1142-9690

DOI: 10.32702/2306-6814.2024.1.78

ХАКЕРСЬКІ АТАКИ ЯК ОСНОВНА ЗАГРОЗА ФУНКЦІОНУВАННЯ ОРГАНІЗАЦІЇ ТА МЕТОДИ ЇХ ЗАПОБІГАННЯ

H. Tybinka,
PhD in Economics, Associate Professor of the Department of Management, Ivan Franko National University of Lviv
O. Yurchenko,
PhD in Economics, Associate Professor of the Department of Accounting and Audit, Ivan Franko National University of Lviv
A. Stojko,
Graduate Student of the Department of Management, Ivan Franko National University of Lviv

HACKER ATTACKS AS THE MAIN THREAT TO THE FUNCTIONING OF THE ORGANIZATION AND METHODS OF PREVENTING THEM

В даній статті досліджено теоретичні та практичні основи децентралізованої автономної організації. Актуальність даного дослідження відображається в тому, що власне децентралізована автономна організація сьогодні на практиці не була повністю реалізована, проте, на наше переконання, існують прототипи, які мають гібридну форму ухвалення рішень децентралізовано, які своєю діяльністю сьогодні демонструють вагому ефективність організаційної структури такого типу. Метою нашого дослідження є формування основних теоретичних принципів створення системи управління власне децентралізованої автономної організації, оцінити діяльність компаній, які застосовують систему управління DAO, встановити потенційні можливості та загрози хакерських атак та методи їх запобігання.

Під час написання статті використано надзвичайно велику кількість зарубіжних джерел, в тому числі роботи дослідників, які вивчали проблеми самого формування децентралізованих автономних організацій, дії технології "Блокчейн", "Смарт-контрактів", а також нормативно-правові акти, документи децентралізованих автономних організацій, TheDAO.

This article examines the theoretical and practical foundations of a decentralized autonomous organization. The relevance of this study is reflected in the fact that the actual decentralized autonomous organization has not been fully implemented in practice today, however, we believe that there are prototypes that have a hybrid form of decentralized decision-making, which by their activity today demonstrate the significant effectiveness of this type of organizational structure. The purpose of our research is to form the main theoretical principles of creating a management system of a decentralized autonomous organization, to evaluate the activities of companies that use the DAO management system, to establish potential opportunities and threats of hacker attacks and methods of their prevention.

During the writing of the article, an extremely large number of foreign sources were used, including the work of researchers who studied the problems of the very formation of decentralized autonomous organizations, the actions of "Blockchain" technology, "Smart contracts", as well as regulatory and legal acts, documents of decentralized autonomous organizations, TheDAO.

Today, scientific management is constantly evolving, we believe that the effective management methods of the past are being superseded by new modern methods. In our article, we explore a completely new type of organizational structure, which, we believe, is currently at the initial stage of its own formation — decentralized autonomous organizations.

In our opinion, the problems of systematic research of negative and positive opportunities and threats of management systems of decentralized autonomous organizations are relevant today.

A significant number of practitioners and scientists today study decentralized autonomous organizations, among which we highlight: Benkler Y. [1], Buterin V. [2], as well as Gorton G. B. [3] and others. However, in our opinion, complex processes are taking place in modern conditions today, which require deepening of practical and theoretical knowledge regarding the study of management systems of decentralized autonomous organizations.

Summing up the above, the main purpose of writing the article is to study the level of development of the DAO management system today and identify the main reasons and measures to prevent hacker attacks in order to take them into account when creating effective trends today and development prospects in the future.

Ключові слова: децентралізована автономна організація, система управління DAO, блокчейн, смарт-контракт, хакерська атака.

Key words: decentralized autonomous organization, DAO management system, smart contract, hacker attack.

ПОСТАНОВКА ПРОБЛЕМИ

Сьогодні постійно еволюціонує науковий менеджмент, власне ефективні методи управління в минулому, ми вважаємо, витісняють нові сучасні методи. В нашій статті ми досліджуємо цілком новий вид власне організаційної структури, який сьогодні, ми вважаємо, є на початковій стадії власного формування — децентралізовані автономні організації.

На нашу думку, актуальними сьогодні є проблеми системного дослідження негативних та позитивних можливостей та загроз систем управління власне децентралізованих автономних організацій.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Значна кількість практиків та науковців сьогодні досліджують децентралізовані автономні організації, серед яких виділяємо: Benkler Y. [1], Buterin V. [2], а також Gorton G. B. [3] та інші. Проте, на наше переконання, в сучасних умовах сьогодні відбуваються складні процеси, які потребують поглиблення практичних та теоретичних знань відносно вивчення систем управління власне децентралізованих автономних організацій.

ПОСТАНОВКА ЗАВДАННЯ

Підсумовуючи вищесказане, основна мета написання статті — дослідження рівня розвитку системи управління DAO сьогодні та виявлення основних причин та заходів запобігання хакерських атак з метою їх врахування під час створення ефективних тенденцій сьогодні та перспектив розвитку в майбутньому.

МЕТОДИ ДОСЛІДЖЕННЯ

Теоретичну і методичну основу нашого дослідження становлять загальнії та спеціальні методи наукового пізнання, системний і комплексний підходи до вивчен-

ня процесів та явищ в суспільстві. В ході нашого дослідження застосовано загальноекономічні і специфічні методи, серед яких виділяємо: статистичне дослідження, соціологічні методи, , синтез та аналіз, абстрактнологічний та інші методи.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Безпека, на наше переконання, сьогодні надзвичайно важлива у галузі віртуальних активів. Станом на сьогодні в історії MakerDAO не спостерігалися злами програмного коду організації. Оскільки MakerDAO містить сьогодні найбільшу кількість віртуальних активів, про що свідчить рисунок нижче, ми вважаємо, що досить багато було атак на MakerDAO.

Однією із основних проблем децентралізованих фінансів сьогодні, на наше переконання, є хакерські атаки. Чимало нових компаній, які пропонують хороший продукт, мають прораховану бізнес-модель, хорошу підтримку ком'юніті через помилку в програмному коді, що дає можливість зловмисникам вивести практично усі чи навіть усі кошти користувачів продукту зазнають краху. Практично кожна нова компанія у галузі децентралізованих фінансів стає жертвою хакерів, які використовують переваги децентралізації та відкритості, а саме: відкритий програмний код, доступно викладену інформацію як технічно влаштований фінансовий продукт певної компанії, скільки і які саме кошти є на рахунку компанії.

Розглянемо злом децентралізованої автономної організації TheDAO, яка зазнала атаки хакерів, як наслідок, правильні рішення ухвалили надто пізно через децентралізовану природу, що викликало крах організації. Усі учасники The DAO — це власники, які виконували функції менеджерів та були пов'язані спільним контрактом у The DAO, однак, не обов'язково спільними інтереси чи баченнями організації. Механізмом управління довірою став блокчейн, тому учасники довіряли лише системі, що було метою її розробки як власне "ненадійної" системи. Сучасні теорії управління, ми вважаємо, сьогодні не враховують відчуження довіри між сторонами, а також шлюб контролю і власності, за якого існує ряд зацікавлених сторін, які мають конкуруючі інтереси. Теорія агентства, як приклад, уособлює ідеальний випадок, при якому один "підприємець-менеджер" ухвалює оптимальні рішення, після чого реалізовує їх як принципал та агент щодо власних інтересів. Якщо є декілька принципалів та агентів і відсутні будь-які стимули, агенти переслідуватимуть свої власні інтереси сеперативно від інтересів принципалів. DAO створює "наступний найкращий випадок" теорії агентства, за якого є декілька підприємців-менеджерів, які не повинні довіряти один одному, проте, можуть діяти як цілеспрямований єдиний підприємець-менеджер.

Попри прозорість блокчейну, існувала численна кількість інформаційних асиметрій між учасниками The DAO. Учасники не були знайомі, не знали мотиви або амбіції один одних інвестувати в The DAO, цінності та пріоритети. Зрозуміло, що певні учасники могли не довіряти запропонованим рішенням певної проблеми настільки, щоб вони могли голосувати за або проти. Цінності і пріоритети не збігалися, не виникало непередбачених обставин для визначення того, контролювати чи управляти конфліктами. В результаті виник хаос під час кризи і, як наслідок, розкол організації. Ми вважаємо, необхідні зусилля для повного розуміння цього нового явища, окреслити наслідки останнього для корпоративного управління, дослідити, як організації ці нові виклики долатимуть в майбутньому.

Сьогодні існує декілька видів управління, спрямованих на створення теоретичного ідеалу, який базується на розподілі прав ухвалення рішень, залишкових претензій, ризиків, додаткових організаційних структур. Проте, сучасні види корпоративного управління відображають певну форму поділу контролю і власності, яка спричинена розподілом прав власності і залишкових вимог. Такий поділ потрібний у випадку, якщо певним учасникам організації довіряють діяти від імені усіх власників, так як, особам, які ухвалюють рішення, як правило, довіряють тільки у випадку наявності певного відомого стимулу діяти на користь організації та в інтересах власників. Різні форми управління існують для керівництва у випадку відсутності довіри між учасниками, які відповідають за ухвалення рішень та моніторинг, через формування механізмів довіри, як приклад, технологічних рішень, що полегшують співпрацю. Саме тому, ми вважаємо, значна кількість літературних джерел сьогодні акцентує увагу на необхідності власне довіри між керівництвом фірми і власниками.

Стимули, розподіл прав на ухвалення рішень та ризиків, розподіл залишкових претензій керуються оперативно, на наше переконання, за допомогою застосування явних та неявних контрактів, які, на прикладі DAO контракти, виступають розумними "ненадійними" контрактами. Сьогодні недослідженими залишаються питання чим розумні контракти відмінні від аналогів, які написані природною мовою. Розумні контракти, ми вважаємо, втілені і здійснюються у комп'ютерному коді, не потребують "довіри", водночас, контракти на природній мові, які, на наше переконання, сьогодні становлять основу сучасних корпорацій, потребують "довірених" сторін для їхнього трактування, реалізації та моніторингу через властивий суб'єктивний характер природної мови, що застосовується при їх написанні. Отже, робимо висновок, що в ідеалі смарт-контракти не потребують тлумачення, примусової реалізації та моніторингу, і, як наслідок, не виникає потреби вирішення конфліктів, оскільки всі вони — важливі елементи поточних теорій корпоративного управління. Це робить складнішим управління непередбаченими подіями чи вирішення суперечок, які пов'язаними із смарт-контрактами, тому що не існує правової бази або центрального управління. Як свідчить DAO, це може спровокувати вагому загрозу здатності організації вчасно реагувати та виживати під час кризових ситуацій, за яких час — дорогоцінний ресурс.

Варто зазначити, на наше переконання, що більшість учасників The DAO не мали потрібного досвіду для розуміння вихідного коду, що становить основу смарт-контракту. Альтернативою є вже те, що учасники справді мають експертні знання, однак, не прочитали

попередньо до погодження договір, що мало імовірно, враховуючи власне суму грошей, що може викликати правові наслідки. DAO повинен був працювати як інвестиційний центр, у якому розумні контракти ділили права голосу між інвесторами або власниками відносно їх акцій у The DAO. Інвестори мали можливість проголосувати за пропозиції, які були подані "підрядниками", затверджені "кураторами", також перевіряли достовірність та законність пропозицій, проте, не мали повноважень ухвалювати рішення. Теоретично, на наше переконання, безпосередньо передавши керівництво власникам, DAO забрало можливість у менеджерів неправильно витрачати або спрямовувати кошти інвесторів. Як наслідок, вони позбулися механізмів довіри для контролю та мотивації ухвалення рішень. Власникам не потрібно довіряти учасникам, які ухвалюють рішення, тому що вони самі почали ухвалювати рішення, довіряти необхідно було тільки розумному контракту, який становив основу The DAO.

Складність коду смарт-контракту у випадку DAO відображала, що функції підтримки децентралізованої системи ухвалення рішень, були, ми вважаємо, його ахіллесовою п'ятою. Швидке розгортання складного коду відображало непередбачувану і епізодичну поведінку. Спричинені ризики посилювалися його децентралізованою моделлю ухвалення рішень, яка була громіздкою і повільною на реалізовані згодом загрози.

Ризики, які пов'язані із складним кодом та децентралізованою системою ухвалення рішень для DAO проявилися в червні 2016 року при анонімному зломі і викраденні 60 мільйонів доларів США. Злом застосовував спосіб кодування смарт-контрактів DAO власне на блокчейні. Проте, питання чи було це "зломом" сьогодні залишається спірним. У технічному аспекті код містився у блокчейні, тому погоджувався, керувався і зберігався у безпеці всіма учасниками The DAO. Технічно DAO зламати практично неможливо, тому що необхідно проникнути на більшість мережевих комп'ютерів DAO одночасно для того, щоб внести та підтвердити зміни в односторонньому порядку в коді.

The DAO "Хакери" застосували "функцію рекурсивного поділу" для перенаправлення цифрової валюти собі.

Були спроби зупинити захоплення криптовалюти, проте, ми вважаємо, не вдалося отримати від колективу потрібного консенсусу голосів за такий короткий час. За ефективної системи управління, план реакції на інциденти дав би можливість керівникам виправити код і швидко заморозити кошти. На жаль, такого плану не було, не було менеджерів, які зуміли б вжити заходів у DAO. Будь-які коригувальні заходи у DAO, повинні бути невід'ємним елементом коду смарт-контракту за згодою його членів.

В результаті, більшість інвесторів The DAO погодилися сформувати "хардфорк" для повернення коштів, у якому багато користувачів змінили свою копію блокчейну на нову версію, у якій "злам" не відбувався ніколи. Це сформувало паралельний блокчейн, у якому не було вкрадено кошти, отже, помилку виправлено.

DAO являють собою нову форму явного робочого контракту із використанням смарт-контрактів та підтримкою блокчейну, є втіленням явного екстремального розумного робочого контракту. Угоди закодовані на блокчейні як власне смарт-контракт і є абсолютно прозорими та загальнодоступними. DAO реалізує строго контрольований набір логічних правил управління ухвалення рішень і реалізації організаційних дій, який сформовано з метою усунення ризику, що сторона певного контракту відхилиться від початкових намірів або буде діяти небажаним чи непередбачуваним чином. В цілому, DAO досягла цілі прозорості, хоча є питання відносно незмінності через потребу створювати блокчейн для виправлення логіки смарт-контракту.

ВИСНОВКИ

Отже, підсумовуючи проведені вище дослідження, можемо зробити висновок, що DAO був сформований так, щоб не довіряти і успішно функціонував без потреби в довірі протягом короткого періоду, що спровокувало питання відносно адекватності існуючих теорій управління. Невдача DAO, на наше переконання, не робить неіснуючими організації подібного типу, а визначає проблеми, які потрібно вирішити для досягнення успіху останніми, а також необхідність переглянути і вдосконалити існуючі теорії управління, врахувавши роль довіри.

DAO створює можливість відносно широкого спектру та різноманітності власне організаційних структур, дизайну роботи в власне автономних організаціях, які частково або повністю управляються розумними контрактами, які реалізованими на блокчейні. Ми прогнозуємо коло організацій, які засновані на технології блокчейн, смарт-контрактах, із новими типами "ненадійних" організацій, що цілком відчужують довіру через застосування явних робочих контрактів, а також більш традиційними організаціями, без відчуження довіри через застосування комбінації явних та неявних трудових контрактів у власній структурі керівництва.

Література:

1. Benkler, Y. The Wealth of Networks : How social production transforms markets and freedom. Yale University Press, 2006.

2. Buterin, V. DAOs, DACs, DAs and More : An Incomplete Terminology Guide. 2014.

3. Gorton, G. B. The Orkney Slew and Central Bank Digital Currencies. 2021.

References:

1. Benkler, Y. (2006), The Wealth of Networks : How social production transforms markets and freedom, Yale University Press, New Haven, USA.

2. Buterin, V. (2014), "DAOs, DACs, DAs and More : An Incomplete Terminology Guide", available at: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide (Accessed 10 Feb 2023).

3. Gorton, G. B. (2021), "The Orkney Slew and Central Bank Digital Currencies", available at: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=3737&context=articles (Accessed 10 Feb 2023).

Стаття надійшла до редакції 23.12.2023 р.