КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№4 (8), 2020
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2020.8.6172
УДК 004.056; 004.4; 004.6

Ткач Юлія Миколаївна
д.п.н., доцент,
завідувач кафедри кібербезпеки та математичного моделювання,
Національний університет «Чернігівська політехніка», Чернігів, Україна
ORCID: 0000-0002-8565-0525
tkach_ym@ukr.net

Бригинець Артур Анатолійович
магістрант кафедри кібербезпеки та математичного моделювання,
Національний університет «Чернігівська політехніка», Чернігів, Україна
ORCID: 0000-0002-0235-545X
is.steel.97@gmail.com

TELEGRAM OPEN NETWORK. КОМПЛЕКСНИЙ АНАЛІЗ ІННОВАЦІЙНОГО ПРОЕКТУ ТА ЙОГО СКЛАДОВИХ

Анотація. Децентралізовані системи займають особливу роль у сучасному житті, а проблеми їх регулювання починають обговорюватися та вирішуватися на державному рівні. Аналіз проекту, який за своїми масштабами та охопленням здатний вплинути на світову економіку та технології в цілому є актуальним та необхідним з точки зору спостереження за технологічними інноваціями. Майбутній повномасштабний запуск комплексної системи з великим потенційним числом користувачів потребує виконання її ретельного дослідження, задля забезпечення усвідомленого використання можливостей системи, а також захисту від потенційних загроз. В статті наведено офіційні матеріали, які проливають світло на внутрішні компоненти, виконуючі роль основних складових системи, а також описано проблеми, які стосуються майбутнього регулювання системи, а також користувацького досвіду, пов'язаного з використанням вбудованих процесів та сервісів, присутніх у системі на етапі запуску. Проведення дослідження та опису основних складових проекту, виявлення їх основних переваг та недоліків, висвітлення основних структурних елементів та понять, реалізованих при розробці складових, можливих нюансів, які матимуть вплив на майбутній досвід користування внутрішніми сервісами проекту. Винесення висновків щодо інноваційності та децентралізованості проекту, його майбутнього потенціалу та впливу на інформаційне середовище в цілому. В статті розглянуто наступні базові компоненти: TON P2P Network, TON DNS, TON Storage, TON Services, TON Payments, TON Blockchain, Gram token, а також складові, використані при їх реалізації. Також описані основні потенційні можливості при майбутньому використанні даних технологій, з'ясовані під час дослідження та аналізу документації складових проекту. Детально описано проблеми технології Blockchain та їх вирішення у реалізованому TON Blockchain. У підсумку приведено висновки щодо проекту в цілому, його складових, можливих проблем у процесі роботи, а також минулі конфузи, що могли підірвати довіру потенційних користувачів. Також наведені висновки щодо можливого майбутнього криптовалюти Gram, її ціни та розповсюдження в мережі, цінності для звичаних користувачів та «валідаторів» мережі.

Ключові слова: TON; Telegram Open Network; блокчейн; сегментування; криптовалюта; децентралізація; смарт-контракт; ICO; токен; хеш.

1. ВСТУП

Актуальність теми дослідження. Розвиток інформаційних технологій впливає на більшість аспектів нашого життя, у сучасному світі ми звикли кожного дня поширювати тисячі цифрових документів різних форматів, це стало звичкою настільки,

ISSN 2663 - 4023

що навіть гроші прийняли цифровий вигляд. Ще у 2017 році Bitcoin та інші криптовалюти стрімко почали брати учать у житті більшої частини населення Землі. Цифрові активи, які до цього були захопленням відносно невеликої групи ентузіастів, перетворилися в чи не головну тему для обговорень по всьому світу, а використання децентралізованих систем стало шляхом забезпечення анонімності та безпеки доступу до інформації в мережі.

Проект Telegram Open Network (TON) привернув до себе величезну увагу, зібравши на стадії ICO кількість заявок на придбання криптовалюти у розмірі 3,8 мільярдів долларів США [1], та оперуючи тим фактом, що після запуску проекту, доступ до відкритої мережі і всіх можливостей відразу отримають сотні мільйонів користувачів месенджеру Telegram. В свою чергу, TON Blockchain, який являє собою основу TON буквально увібрав в себе весь досвід криптоіндустрії, накопичений за останні роки, планує реалізувати велику кількість технологічних процесів, які раніше були тільки на папері.

Постановка проблеми. Оскільки після анонсування системи та її можливостей представники Telegram заявили, що розраховують на конкурування зі світовими лідерами ринку безготівкових операцій – Visa і Mastercard [2], можна зробити висновок про широко масштабне використання вбудованої в мережу криптовалюти, яка представлена токеном Gram. Можна розраховувати, що в результаті буде створена ціла економіка всередині Telegram, про це також йдеться в описі проекту TON.

На даний момент жодна криптовалюта не підходить на роль конкурента Visa і Mastercard, для прикладу можна привести відомий протокол Bitcoin, що зі швидкістю в сім операцій в секунду не може конкурувати з міжнародними платіжними системами, які обробляють в середньому близько двадцяти тисяч операцій в секунду. Швидкість проведення транзакцій в мережі TON заявлена як 10 мільйонів/сек, що досягається використанням смарт-контрактів та технології сегментування (sharding).

Звичайно, такий масштабний проект та обсяги залучених до нього коштів не могли залишитися непоміченими, і у жовтні 2019 року Комісія з цінних паперів і бірж США (SEC) подала позов до суду Манхеттена терміновий позов з метою призупинити незареєстроване первинне розміщення токенів Gram, на підставі того, що токени продавалися незаконно – і домоглася тимчасової судової заборони [3], яка викликала призупинення повномасштабного запуску TON. З даної новини можна зробити висновок, що навіть представники влади не мають повного уявлення про всі можливості та процеси, які стануть доступними при запуску мережі, те ж саме більшою мірою стосується мільйонів майбутніх користувачів мережі.

Основна проблема стосується саме того, що після запуску TON, доступ до мережі отримають мільйони користувачів, які не будуть мати уявлення про внутрішні процеси роботи даної децентралізованої системи, в той час, всі вони зможуть в повній мірі оцінити її переваги і почати використовувати систему за призначенням: розробники – створювати корисні і прибуткові додатки, користувачі - використовувати функціонал корисних додатків, з легкістю оплачуючи його при необхідності. Користування функціоналом без усвідомлення всіх нюансів роботи системи може привести до непередбачених наслідків, саме тому необхідна наявність подібного дослідження та комплексного аналізу складових системи й перспектив її використання, які наведені в даній статті.

Аналіз останніх досліджень і публікацій. Хоча проект TON і перебуває лиш на стадії завершення розробки, своїм масштабом він привертає увагу багатьох спеціалістів, мотивуючи їх на проведення досліджень. Зокрема, в роботах [4], [5]

відзначається, що TON є рушієм прогресу в розробці покращень для технології блокчейн, та являє собою «Найбільший проект» з точки зору блокчейн-платформ та ICO. В свою чергу, розробники проекту надають можливості для досліджень і потенційним користувачам. Так, у травні 2019 року стало можливим використання тестової збірки проекту, а також були представлені технічні описи основних складових TON, посилання на які будуть використовуватися в даній статті, а саме: *TON Whitepaper* – загальний опис TON Network та TON Blockchain [6], *Telegram Open Network Blockchain* – детальний опис блокчейну TON [7], *Telegram Open Network Virtual Machine* – технічний опис TVM (TON Virtual Machine, виртуальної машини TON) [8], *Fift: A Brief Introduction* – опис нової мови програмування Fift, яка передбачена для створення смарт-контрактів у TON [9].

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Виділення недосліджених частин загальної проблеми. Беручи до уваги масштаб проекту, а також відсутність прикладних програмних інтерфейсів, які б надали змогу для тестування мережі у тестовому режимі звичайним користувачам, постають питання, які відносяться до функціонування TON після повномасштабного запуску. А саме, чи дійсно система буде повністю децентралізованою та незалежною від регулювання своїми розробниками; чи стійка економіка системи, основана на токені Gram; чи дійсно архітектура проекту дозволяє здійснювати досить просту інтеграцію з додатками сторонніх виробників, наприклад мессенджерами або соціальними мережами; і головне, як буде формуватися ціна вбудованої криптовалюти, та чи зможуть користувачі понести від роботи з системою реальні збитки, або ж навпаки, накопичити кошти.

Постановка завдання. Враховуючи вплив подібних великомасштабних проектів на світове суспільство та інформаційний простір, а також наведених вище проблем, за мету статті можна виділити комплексний аналіз проекту, який передбачає розгляд історії створення, опис його основних компонентів та використовуваних у них технологічних процесів, а також аналіз відкритих даних щодо властивостей криптовалюти Gram та залучених інвестицій. При розгляді проекту описується багато важливих структур і понять, та що найголовніше – вони становлять не просто декларацію про наміри, адже тестування проекту TON проходить у нинішній час, та вже зараз люди намагаються писати смарт–контракти на конкурс. Отримана в ході дослідження інформація дасть змогу зробити зважені висновки щодо функціонування системи та майбутнього користувацького досвіду.

Опис об’єкту дослідження. Проект Telegram був створений братами Дуровими у 2013 році. Микола Дуров розробив схему шифрування MTProto, яка лягла в основу проекту. Основною концепцією месенджера була анонімність та безпечне спілкування користувачів. Месенджер існував за рахунок особистих фондах Павла Дурова до 2017 року. Проект TON, пов’язаний в основному з роботою месенджера Telegram, в який планується інтегрувати криптовалюту Gram.

На початку 2018 року під час закритої ICO Telegram було зібрано 1,7 мільярдів доларів на розробку блокчейн–платформи TON Blockchain. Вся сума була отримана від приватних інвесторів, які придбали токени Gram. Серед інвесторів фігурують досить відомі особистості: Абрамович, Якобашвілі, Солонін [10]. Сама платформа була розгорнута в тестовому режимі восени 2018 року, саме в цей час розробники заявили,

ISSN 2663 - 4023

що мережа готова до використання на 70%, і більшість компонентів вже допрацьовані. Запуск відкритої тестової мережі повинен був відбутися в січні 2019 року, але був перенесений. Закрите тестування криптовалюти Gram, проведене у квітні 2019 року, дало можливість розробникам оцінити правдивість заяв розробників. Тестування проходило шляхом підключення свого вузла до мережі TON. Учасники тестування не поділилися детальною інформацією про свої враження, але вони виділили дійсно високу швидкість проведення транзакцій, що підкреслює реальну роботоспроможність системи та підтвердження заяв розробників.

Офіційний документ проекту (whitepaper) був написаний Миколою Дуровим, де він узагальнив усі позитивні сторони блокчейн–технологій та запропонував інноваційну архітектуру для масштабування та децентралізації. Керівництво Telegram не розголошувало точну дату виходу TON, але раніше малося на увазі, що якщо до 31 жовтня 2019 року не відбудеться запуску проекту, то інвестори матимуть право повернути вкладені кошти. Через позов до суду від Комісії з цінних паперів і бірж США, проект досі на стадії тестування мережі, наразі testnet2, а співзасновник проекту Павло Дуров заявив про готовність повернення 77% коштів інвесторам, але вони згодилися дочекатися старту проекту. Наразі найбільш актуальним джерелом інформації є стаття від розробників проекту за 6 січня 2020 року [11], в якій пролито світло на основні нюанси та запитання щодо проекту. Поява даної публікації може знаменувати запуск TON у найближчий час.

За своєю суттю, Telegram Open Network – це швидкий, безпечний та інноваційний мережевий проект на основі блокчейна, який бере на себе обов'язки реалізації швидкої, практичної та масштабованої мережевої платформи. Реалізований у розподілених по тисячам серверів «суперсервер», на базі якого можуть бути запущені тисячі корисних додатків. Включаючи до вищевказаного власний токен Gram, підтримку мікротранзакцій, та сотні мільйонів існуючих користувачів Telegram, які автоматично отримають доступ до всіх сервісів на платформі TON можна зробити висновок про інноваційність задуму, та беззаперечний вплив на сучасний інформаційний простір та суспільство.

Перше, що потрібно зрозуміти, TON – це не блокчейн. Це розподілена, децентралізована мережа, з блокчейном та мікротранзакціями. У перспективі, користувачі, так само, як вони користуються браузером для доступу до мережі Internet, де є різні сайти і сервіси, точно так будуть використовувати вбудований в TON браузер, для доступу до нової мережі.

TON являє собою сукупність наступних компонентів [6, гл. 1, с. 3–4]: мережа *TON P2P Network* дає можливість доступу до блокчейну та системи зберігання, а також дозволяє спілкуватися між собою сервісам; служба коротких імен *TON DNS*, для використання звичних мережевих адресів, замість громіздких адресів-хешів; розподілена система зберігання *TON Storage*, з доступом P2P за принципом торрентів (файлу будь–якої величини відповідає лише його хеш–сума), для зберігання даних блокчейна, а також будь–яких файлів користувачів; додатки *TON Services*, які виконуватимуть різноманітні задачі та функції, а перебувати і виконуватися ці сервіси можуть як безпосередньо в блокчейні (onchain), так і поза ним (offchain); сервіс для мікроплатежів *TON Payments*, що дозволяє авторам додатків легко та ефективно отримувати оплату з користувачів за послуги, а також здійснювати платежі безпосередньо між користувачами TON без оплати комісій мережі; токен Gram, вбудований токен базової мережі TON, її криптовалюта; багатоцільова блокчейн платформа *TON Blockchain* з необмеженою пропускною спроможністю, смарт-

контрактами, налаштованим сайдчейнами (sidechain) та іншими новітніми технологічними процесам; віртуальна машина *TON Virtual Machine* з підтримкою мови програмування *Fift* для написання смарт–контрактів.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Виклад основного матеріалу. Проведемо дослідження основних компонентів, більш детально зупинившись на TON Blockchain та токені Gram. В першу чергу розглянемо саму мережу TON Network протокол якої вже реалізований. Загалом, на базовому рівні реалізація TON Network включає такі поняття, як абстрактні адреси, сервіси, вузли мережі, протокол *ADNL: Abstract Datagram Network Layer*, TON DHT: розподілену хеш-таблицю, а також підклас перекриваючих (overlay) мереж, для забезпечення зв'язку будь–яким групам користуачів. На зразок вже реалізованого для Telegram протоколу MTProto вона являє собою абстракцію над стандартними протоколами TCP/UDP, та дає кожному вузлу всередині мережі власну адресу і задає стандарти повідомлень між ними [6, гл. 3, с. 81]. Окремо описується додатковий функціонал TON Proxy, що дозволяє здійснювати анонімний доступ до мережі TON [6, гл. 4, с. 103]. Щодо наявності даної технології можна підкреслити увага до деталей в області анонімності ще на стадії whitepaper, це вказує, в якому напрямку розробники планують розвивати проект, в бік співпраці з регуляторами або ж в сторону децентралізації і відмови від відповідальності за все, що відбувається в мережі.

Але якщо розглянути реалізацію мережі детальніше, можна помітити що TON Proxy відноситься до підкласу туманних сервісів (fog service), які мають на увазі децентралізацію і відкриту участь в них. Тобто TON Proxy – це сервіс, який може підтримувати будь–який учасник, який бажає надати свій вузол в якості посередника, що пересилає пакети між іншими вузлами. При бажанні він може стягувати за це встановлену їм плату - використовуючи систему TON Payments для мікроплатежів (яка, в свою чергу, теж є туманним сервісом). Тобто можна сказати, що децентралізований доступ буде реалізований для кожного сервісу окремо, і сторонній розробник буде сам вирішувати про введення даної технології.

TON DNS в свою чергу э важливим сервісом, який вирішує проблеми зрозумілиих адрес сервісів та контрагентів, наразі проходить конкурс на розробку цього смарт–контракта, але він вже визначений у документації [6, гл. 4, с. 105].

Запланована разподілена система зберігання TON Storage реалізує перевірену часом концепцію протоколу BitTorrent, коли невеликий хеш може відповідати будь–якому великому файлу. Дійсно, існує велика кількі багато даних, що потрібно зберігати розрізнено, торрет є найбільш доцільним варіантом. Протягом останніх років знаходиться багато людей, які готові надавати абсолютно безкоштовно свої дискові та мережеві потужності, щоб користувачі могли завантажити конкретний файл. Також пропонується інтегрувати в дану технологію зручну монетизацію через токени Gram та концепцію «хмарних сервісів» [6, гл. 4, с. 102].

Блокчейн потрібен для того, щоб ним користувалися. Саме тому реалізується технологія TON Services, для того, щоб у великої кількості створених смарт–контрактів і різних пропозицій завжди було взаємодія з клієнтами. Зазвичай розробнику необхідно створити власний веб–сайт, або примусити користувача встановити розширення для браузеру для того, дощ користуватися додатком. Зрозуміло, що такі проекти не здатні на швидке поширення, так як користувачі звикли, що все повинно «просто працювати з

коробки», та ні на що інше не згодні. Тому цілого розділу, що описує створення та взаємодію з додатками вселяє довіру. Виділяється два типи TON Services, по–перше – сервісні послуги, з якими взаємодіють додатки та інші сервіси, та по–друге – власне додатки, якими будуть користуватися звичайні користувачі [6, гл. 4, с. 99–113]. Також вводиться поняття стандартних інтерфейсів в смарт–контракті, для того, щоб з ними можна було взаємодіяти з будь–якого стандартного клієнта. Але залишається відкритим питання, насколько складні інтерфейси можуть бути реалізовані подібним методом.

TON Payments представляє з себе мережу віртуальних банків, де кожен користувач встановлює відносини хоча б з одним контрагентом. Подібні відносини фіксуються смарт–контрактом, який заморожує суми внесків, як гарантію чесності сторін. Після цього можна переводити гроші кому завгодно, важлива лише наявність ланцюгу (chain), що пов'язує двох агентів. Дана процедура необхідна для того, щоб не спамити мережу постійними мікротранзакціями, а записувати в неї тільки оновлені баланси, хто кому скільки винен. Варто зазначити, що платежі за таким принципом будуть практично безкоштовними, при цьому ніхто не заважає безпосередньо переводити токени через блокчейн TON, заплативши відповідну комісію мережі, якщо мається на увазі велика або важлива угода [6, гл. 5, с. 113–123].

Як відомо, основою всього проекту є TON Blockchain. Навіть якби не було всієї перерахованої вище інфраструктури, то все одно він був би вкрай цікавим з технічної точки зору. На даному кроці є сенс ввести основні поняття, які допоможуть краще зрозуміти реалізацію даної інноваційної технології, та окремих частин статті в цілому:

- акаунт (account). Деякий набір даних, ідентифікований 256–бітовим числом *account_id*. У базовому випадку, під цими даними мається на увазі баланс користувача [7, гл. 4, с. 69];
- смарт–контракт (smart–contract). По суті – окремий випадок аккаунта, доповнений власним кодом і сховищем для змінних. Якщо у випадку «гаманця» можна зараховувати і списувати гроші з нього по відносно простих і заздалегідь визначених правил, то у випадку смарт–контракту ці правила записані в вигляді його коду (мається на увазі мова Fift);
- стан блокчейна (state of blockchain). Сукупність станів всіх акаунтів або смарт–контрактів (в абстрактному сенсі – хеш–таблиця, де ключами є ідентифікатори акаунтів, а значеннями – збережені в акаунтах дані) [7, гл. 1, с. 23];
- транзакція (transaction). Факт доставки повідомлення. Транзакції змінюють стан блокчейна. Саме з транзакцій (записів про доставку повідомлень) складаються блоки в блокчейні [7, гл. 4, с. 75].

Відомо, що блокчейн – це структура даних, елементи (блоки) якої упорядковані в «ланцюг», і кожен наступний блок ланцюга містить в собі хеш попереднього. Власне, вся складність структури блокчейна реалізована заради запобігання втручань в збережені в ньому дані. Однак блокчейн в TON виглядає ще складніше, ніж в більшості інших розподілених систем – і на те є дві причини. Перша – прагнення мінімізувати потребу в форках (fork – відділена копія). У традиційних криптовалютах всі параметри задані на початковому етапі і будь-яка спроба їх змінити призводить фактично до появи «альтернативної криптовалюти». Друга причина – підтримка сегментування (sharding, шардингу) блокчейну. Блокчейн – структура, яка не здатна стати менше з плином часу, і зазвичай кожен вузол, який відповідає за працездатність мережі, змушений зберігати її повністю. У централізованих системах для вирішення подібних проблем застосовується

ISSN 2663 - 4023

сегментування: частина записів в базу даних знаходиться на одному сервері, інша частина – на іншому, і так далі. У випадку з криптовалютою така функціональність поки що досить рідкісна – зокрема, через те, що складно додати сегментування в систему, де воно не було заплановано спочатку.

TON Blockchain планує вирішити обидві вищеописаних проблеми. В першу чергу, необхідно вирішити, що ж планується зберігати в блокчейні, а саме стан акаунтів і смарт–контрактів. По суті, це буде звичайна хеш–таблиця – ключами в ній будуть ідентифікатори *account_id*, а значеннями – структури даних, що містять в собі такі речі, як:

- баланс;
- код смарт–контракту (тільки для смарт–контрактів);
- сховище даних смарт–контракту (тільки для смарт–контрактів);
- статистика;
- публічний ключ для перекладів з аккаунта, за замовчуванням account_id;
- чергу вихідних повідомлень (сюди вони заносяться для пересилки одержувачу);
- список останніх доставлених акаунту повідомлень.

Як було сказано вище, безпосередньо блоки складаються з транзакцій – повідомлень, доставлених різним акаунтам з полем account_id. Однак крім account_id повідомлення містять також 32–бітове поле *workchain_id* – ідентифікатор так званого воркчейну (workchain, working blockchain). Це дозволяє мати кілька незалежних один від одного блокчейнів з різними конфігураціями. При цьому workchain_id = 0 вважається особливим випадком, нульовим воркчейном – саме в ньому знаходяться баланси, які будуть відповідати криптовалюті Gram. Можна передбачити, що в перший час після запуску проекту воркчейнів не буде існувати зовсім.

Щодо сегментування, уявімо, що кожному аккаунту (account_id) виділено свій власний блокчейн – в ньому знаходяться всі повідомлення, а стани всіх таких блокчейнів зберігаються на окремих вузлах. Можна зробити висновок, що це досить марнотратно: швидше за все, в кожен з цих шардчейнов (shardchain, shard blockchain) [7, гл. 5, с. 96-100] транзакції будуть надходити дуже рідко, а потужних вузлів знадобиться багато. Тому шардчейни об'єднують в собі аккаунти по двійковим префіксам їх ідентифікаторів: якщо шардчейн має префікс 0720, то в нього потраплять транзакції всіх account_id, які починаються з цих цифр. Цей *shard_prefix* може мати довжину від 0 до 60 біт – та головне, що він може змінюватися динамічно. Як тільки в один з шардчейнів починає надходити надмірна кількість транзакцій, працюючі над ним вузли по заздалегідь визначеним правилам розподіляють його на два дочірніх – їх префікси будуть на один біт довше. Наприклад, shard_prefix = 0720t розщепиться на 07200t і 07201t. У свою чергу, якщо два «сусідніх» шардчейна будуть обробляти надто малу кулькість транзакцій, вони знову зіллються воєдино під окремий префікс, дана технологія має назву *Infinite Sharding Paradigm* (парадигма нескінченного сегментування).

Вище перераховано багато видів інформації про різні види блокчейнів, яку саму по собі теж слід десь зберігати. Зокрема, мова йде про наступні дані: кількість та конфігурація воркчейнів; кількість шардчейнів та їх префіксів; які вузли в даний момент відповідальні за які шардчейни; хеші останніх доданих блоків в усі шардчейни. Звичайно, можна винести логічний здогад, що всі перелічені дані записуються в ще одне сховище–блокчейн – мастерчейн (masterchain, master blockchain) [7, гл. 5, с. 101-103]. Завдяки наявності в його блоках хешу від блоків всіх шардчейнів, він робить

ISSN 2663 - 4023

систему зв'язаною. У тому числі це означає, що генерація нового блоку в мастерчейні відбуватиметься безпосередньо після генерації блоків в шардчейнах – очікується, що блоки в шардчейнах будуть з'являтися майже одночасно приблизно кожні 5 секунд, а черговий блок в мастерчейні – через секунду після цього.

Постає питання, які вузли будуть відповідальні за реалізацію всієї роботи – за пересилку повідомлень, виконання смарт–контрактів, формування блоків в шардчейнах та мастерчейні, а також перевірку блоків на помилки? Невже все це будуть в прихованому режимі робити телефони мільйонів користувачів з встановленим на них клієнтом Telegram? Документація надає відповідь, згадуючи про так зване коло «валідоторів» – потужних вузлів, коло яких буде змінюватись час від часу [7], звісно можна зробити висновок, що валідатори мережі повинні отримувати винагороду за свою роботу, що очевидно підкреслено використанням консенсусу *Proof-of-Stack* у криптовалюті Gram.

Останнє, але не менш важливе – токен Gram, основна криптовалюта для всього TON Blockchain, початкове її призначення – оплата послуг мережі (utility token). Для того, щоб взаємодіяти з блокчейном, відправити транзакцію, завантажити смарт–контракт або запустити його, потрібно заплатити невелику комісію, так званий gas, яка оплачується Gram'ами. Для того, щоб стати валідатором і мати можливість впливати на рішення, що приймаються в мережі – потрібно внести в заставу дуже велику суму, знову ж Gram'ами. На цьому корисність utility токена, насправді закінчується, більше він ні для чого не потрібен. По факту це просто цифрові значення, існуючі на кожному акаунті, спочатку вони з'являються у власників мережі, а потім вже пересилаються всім, хто в них зацікавлений. Однак іноді у токенов з'являється особливість. Люди починають ними розплачуватися між собою, припускаючи, що ці прості цифри на акаунтах несуть якусь цінність. Причому цінність ця практично не залежить від об'єктивних чинників. Майже десять років тому за простий товар могли заплатити 10 тисяч біткоїнів, а зараз за таку кількість зацікавлені особи готові віддати мільйон доларів. Такий випадок має назву commodity token, віртуальний токен, як вираз цінності. Різниця між utility і commodity сутностями токена може здаватися неістотною, але вона дуже важлива для регуляторів, особливо в США. Одна справа – поширювати utility token, зовсім інше – commodity token. Угода з початковими інвесторами і фактичні дії з розповсюдження токенов спрямовані на те, щоб Gram вважався (і був) саме utility токеном.

Спочатку було створено п'ять мільярдів Gram'ів. Це загальна кількість монет в мережі. Кожен Gram може бути поділений на мільярд частин, з чого можна зробити висновок, що проблем з мікрокоміссіями і платежами не буде. Потім дана сума була спрямована на спеціальний аккаунт TON Reserve, спеціально створеної організації, яка займається розповсюдженням криптовалюти серед великих інвесторів. Формула розповсюдження створена таким чином, що ціна монет, проданих через TON Reserve може тільки рости, кожна наступна коштує дорожче за попередню.

Приблизно 2,9 з п'яти мільярдів токенів було продано на розпродажах приватним інвесторам. Ще 200 мільйонів було зазначено для оплати витрат на розробку, а 500 мільйонів – на операційні витрати. Можна порахувати, що при проданих 3,6 мільярдах монет стартова ціна продажу при запуску проекту з TON Reserve складе 3,65$. Це «опорна» ринкова ціна, від якої всі будуть відштовхуватися. 2 жовтня 2019 року інвестори отримали листа з важливою інформацією. У ньому зазначено, що до 16 жовтня необхідно було згенерувати приватні ключі для своїх акаунтів в мережі TON і повідомити їх адреси. Крім того, їм пропонувалося стати валідаторами, так як і

Telegram і TON Foundation добровільно відмовилися від контролю над мережею навіть на самому початку її роботи, що підкреслює ідею децентралізації.

Після запуску проекту доля криптовалюти Gram буде залежати вже від широкого числа користувачів. Якщо хоча б частина користувачів Telegram придбає токенів хоча б на 5–10$, заради простої спроби використання ресурсів мережі – це вже будуть багатомільйонні інвестиції в вартість токена, які не тільки підтримають курс, а й дадуть позитивний новинний фон, сигнал для інвесторів не поспішати фіксувати прибуток, а для розробників, починати створювати додатки для мережі, лише в такому випадку проект запрацює на 100%. Якщо цього не станеться, є надія на викуп токенів мережею, та що інвестори будуть грамотно маніпулювати ринком і його очікуваннями, аби не допустити різкого зниження ціни.

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Провівши аналіз проекту та його складових, історії, а також визначних подій, можна зробити висновки щодо інноваційності проекту, його технологічної реалізації, використання можливостей та потенційних загроз в процесі користування. По–перше, можна не сумніватися в децентралізованості мережі проекту, з обмовкою на те, що деякі сервіси все ж не будуть «туманними», в будь–якому випадку, дане питання буде вирішувати розробник сервісу (додатку). Децентралізацію можна вважати великим плюсом, з точки забезпечення анонімності та відмови від будь–якої цензури, головне щоб цим плюсом не змогли користуватися зловмисники та розповсюджувачі незаконних товарів, як це буває у інших анонімних мережах. Цю проблему візьме на себе криптовалюта Gram, яка не повинна стати аналогом реальних грошей, та діяти лише з точки зору «цифрових» мотивів, використовуючись для оплати послуг додатків проекту.

Беручи до уваги масштаби проекту та рівень реалізації складових можна зазначити про її швидкість, ефективність та безпеку. Теж буде стосуватися щоденних комерційних операцій у всьому світі.

Важливо не забувати, що токени Gram є utility токенами, і вони не роблять нікого співвласниками проекту TON. Вони просто дають право на його використання і на участь в валідації. Щоб почати «майнінг» потрібно мати певну кількість токенів, доки невідому, але судячи з усього це будуть сотні тисяч доларів, потім ці токени потрібно буде заморозити на спеціальному смарт–контракті, придбати швидкий сервер для обробки транзакцій і почати підтримувати роботу мережі. За це буде нараховуватися винагорода. Тобто токени «Gram не допоможуть вам розбагатіти» [11], що в свою чергу підкреслює взаємовигідне та основане на послугах використання проекту, а не ставлення цілей у власному збагаченні. Окремо можна виділити мову написання смарт–контрактів Fift, яка є досить низькорівневою, досить мала кількість спеціалістів зможе судити про безпеку написаних на ній сервісів, тому даній технології необхідна високоривнева абстракція, задля забезпечення відкритості коду.

Однак ще на стадії продажу токенів, величезна кількість шахраїв, беручи до уваги популярність криптовалют та розповсюдженості даної новини, намагалися «перепродавати» Gram’и, розповсюджуючи підробні дані про наявність токенів [12]. Описане шахрайство було досить глобальним у колах користувачів, які цікавилися криптовалютами, і на той час нажаль стало досить успішним. Нещодавно команда розробників TON також нагадала, що «Ніхто ще не може купити або продати Gram’и»

[11], але деяка кількість можливих майбутніх користувачів зазнала збитків ще до запуску проекту TON. Тобто врешті решт, використання інновацій та найактуальніших послуг в сучасному інформаційному просторі не робить нікого захищеним від власних помилок.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Telegram during preliminary ICO collected applications for $ 3.8bn. News of Telegram. [online]. Доступно: https://t.me/tlgblg/16. Дата звернення: 11 Січень 2020.
[2] TON GRAM - будущий конкурент мировым платежным системам. Tgram. [online]. Доступно: https://t.me/Tgram/143. Дата звернення: 11 Січень 2020.
[3] Суд в США приостановил ICO Telegram Павла Дурова. BBC. [online]. Доступно: https://www.bbc.com/russian/news-50023412. Дата звернення: 11 Січень 2020.
[4] Федорова Т. А. ICO и проблемы экономической безопасности / Татьяна Аркадьевна Федорова. // Технико-технологические проблемы сервиса. – 2018. – №1. – С. 105–111.
[5] Куприяновский В. П. и др. Умный контейнер, умный порт, BIM, Интернет Вещей и блокчейн в цифровой системе мировой торговли // International Journal of Open Information Technologies ISSN: 2307-8162 vol. 6, no.3, 2018.
[6] Durov, N., 2019. Telegram Open Network. [online]. (Останнє оновлення 2 Березень 2019) Доступно: https://test.ton.org/ton.pdf. Дата звернення: 11 Січень 2020.
[7] Durov, N., 2019. Telegram Open Network Blockchain. [online]. (Останнє оновлення 3 Жовтень 2019) Доступно: https://test.ton.org/tblkch.pdf. Дата звернення: 11 Січень 2020.
[8] Durov, N., 2019. Telegram Open Network Virtual Machine. [online]. (Останнє оновлення 12 Грудень 2019) Доступно: https://test.ton.org/tvm.pdf. Дата звернення: 11 Січень 2020.
[9] Durov, N., 2019. Fift: A Brief Introduction. [online]. (Останнє оновлення 5 Жовтень 2019) Доступно: https://test.ton.org/fiftbase.pdf. Дата звернення: 11 Січень 2020.
[10] Понзель М. Г., 2018. Роман Абрамович вложился в Telegram. [online]. Доступно: https://protocol.ua/ua/roman_abramovich_vlogilsya_v_telegram/. Дата звернення: 11 Січень 2020.
[11] A Public Notice About the TON Blockchain and Grams. The Telegram Team. [online]. (Останнє оновлення 6 Січень 2020) Доступно: https://telegram.org/blog/ton-gram-notice. Дата звернення: 11 Січень 2020.
[12] Some websites offer Grams to the public and pretend to be affiliated with Telegram. *Telegram News*. [online]. Доступно: https://t.me/telegram/118. Дата звернення: 11 Січень 2020.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (8), 2020
ISSN 2663 - 4023

Yulia M. Tkach
Doctor of Pedagogical Sciences, Associate Professor, Head of the Department of Cybersecurity and Mathematical Modeling,
National Univercity «Chernihiv Polytechnic», Chernihiv, Ukraine
ORCID: 0000-0002-8565-0525
tkach_ym@ukr.net

Arthur A. Bryhynets
Master of the Department of Cybersecurity and Mathematical Modeling,
National Univercity «Chernihiv Polytechnic», Chernihiv, Ukraine
ORCID: 0000-0002-0235-545X
is.steel.97@gmail.com

TELEGRAM OPEN NETWORK. COMPLEX ANALYSIS OF THE INNOVATIVE PROJECT AND ITS COMPONENTS

Abstract. Decentralized systems play a special role in modern life, and the problems of regulating them are beginning to be discussed and resolved at the governmental level. The analysis of a project that, by its scale and scope, is capable of influencing the global economy and technology as a whole is relevant and necessary in terms of observing technological innovation. Future full-scale launch of the integrated system with a large number of potential users of its execution requires careful research to ensure informed use of the system and protect against potential threats.In this frticle have shown the official materials that shed light on the internal components that serve as the main parts of the system and described issues related to future system regulation as well as user experience related to the use of embedded processes and services present on the system at startup. Conducting research and description of the main components of the project, identifying their main advantages and disadvantages, highlighting the basic structural elements and concepts realized in the development of components, possible nuances that will affect the future experience of using the internal services of the project. Drawing conclusions on the innovation and decentralization of the project, its future potential and impact on the information environment as a whole. Consider the following basic components: TON P2P Network, TON DNS, TON Storage, TON Services, TON Payments, TON Blockchain, Gram token, and components used in their implementation. It also outlines the main potentials for future use of these technologies, which were clarified during the study and analysis of the documentation of the project components. Blockchain technology problems and their solutions in TON Blockchain implemented are described in detail. As a result, conclusions about the project as a whole, its components, possible problems in the process of work, as well as past confusion that could undermine the trust of potential users. It also draws conclusions about the possible future of Gram cryptocurrency, its pricing and distribution, values for common users and «validators» of the network.

Keywords: TON; Telegram Open Network; blockchain; sharding; cryptocurrency; decentralisation; smart-contract; ICO; token; hash.

REFERENCES

[1] Telegram during preliminary ICO collected applications for $ 3.8bn, News of Telegram. [online]. Available: https://t.me/tlgblg/16. Accessed on: 11 January 2020.
[2] TON GRAM - budushchii konkurent mirovym platezhnym sistemam. Tgram. [online in Russian]. Available: https://t.me/Tgram/143. Accessed on: 11 January 2020.
[3] Sud v SShA priostanovil ICO Telegram Pavla Durova. BBC. [online in Russian]. Available: https://www.bbc.com/russian/news-50023412. Accessed on: 11 January 2020.
[4] Fedorova T. A. ICO i problemyi ekonomicheskoy bezopasnosti / Tatyana Arkadevna Fedorova. // Tehniko-tehnologicheskie problemyi servisa: no.1, 2018.

[5] Kupriyanovsky V. et al. Smart container, smart port, BIM, Internet Things and blockchain in the digital system of world trade // International Journal of Open Information Technologies ISSN: 2307-8162 vol. 6, no.3, 2018
[6] Durov, N., 2019. Telegram Open Network. [online]. (Updated 2 March 2019) Available: https://test.ton.org/ton.pdf. Accessed on: 11 January 2020.
[7] Durov, N., 2019. Telegram Open Network Blockchain. [online]. (Updated 3 October 2019) Available: https://test.ton.org/tblkch.pdf. Accessed on: 11 January 2020.
[8] Durov, N., 2019. Telegram Open Network Virtual Machine. [online]. (Updated 12 December 2019) Available: https://test.ton.org/tvm.pdf. Accessed on: 11 January 2020.
[9] Durov, N., 2019. Fift: A Brief Introduction. [online]. (Updated 5 October 2019) Available: https://test.ton.org/fiftbase.pdf. Accessed on: 11 January 2020.
[10] Ponzel M. G., 2018. Roman Abramovich vlozhilsia v Telegram. [online in Russian]. Available: https://protocol.ua/ua/roman_abramovich_vlogilsya_v_telegram/. Accessed on: 11 January 2020.
[11] A Public Notice About the TON Blockchain and Grams. The Telegram Team. [online]. (Updated 6 January 2020) Available: https://telegram.org/blog/ton-gram-notice. Accessed on: 11 January 2020.
[12] Some websites offer Grams to the public and pretend to be affiliated with Telegram. Telegram *News*. [online]. Available: https://t.me/telegram/118. Accessed on: 11 January 2020.