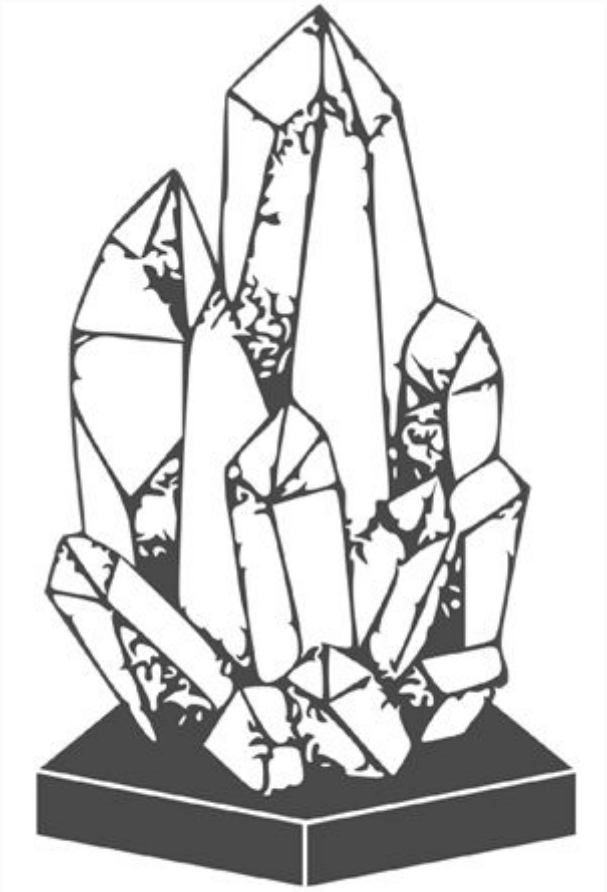


АДАМАНТ

Майбутнє обміну повідомленнями

WHITEPAPER

БІЛА КНИГА

v. 1.1.3 UKR

Резюме **4**

Концепція АДАМАНТу **5**

Захист даних та анонімність 5

Правовий аспект гарантій таємниці листування 7

Зберіегання повідомлень у АДАМАНТі 7

Розрахункова система 8

Дохідність для власників токенів 8

АДАМАНТ Бізнес 8

Огляд альтернативних рішень та їх порівняння **10**

Технічне рішення **11**

Архітектура системи 11

Специфікація токену АДАМАНТ 12

Незалежний блокчейн 13

Транзакції у АДАМАНТі 13

Підтримка інфраструктури і майнінг (форджинг) ADM 14

Надійність та безпека системи 15

Обсяг зберігаємих даних 16

Поточний стан проекту **17**

Месенджер АДАМАНТ 17

Blockchain Explorer 20

Дистрибутив повного вузла 20

Фінансова частина **21**

Обґрунтування цілісності токену 21

Емісія токенів 21

Залучення коштів на розробку і розвиток проекту (кампанії Pre-ICO та ICO) 22

Pre-ICO — залучення коштів інвесторів на найкращих умовах 22

ICO — завершальний етап залучення коштів інвесторів 23

Планування бюджету проекту 24

«АДАМАНТ Зростає» 25

Розміщення токену ADM на криптовалютних біржах 25

Адаптація та просування **26**

Початкові нарахування на гаманці користувачів 26

Кампанія Bounty 27

Дорожна карта проекту (2017-2018) **28**

Колектив АДАМАНТу **29**

Ресурси АДАМАНТу **33**

Резюме

Система передачі повідомлень та даних, заснована на блокчейн-технологіях, у поєднанні з інтегрованою платіжною системою приносить принципові переваги для особистих і бізнес-комунікацій.

АДАМАНТ для приватних осіб — месенджер на блокчейні, доступний з будь-якого пристрою. Неперевершені анонімність та захист даних, зручність у використанні, інтегрована платіжна система.

Месенджер вже доступний для використання: https://msg.adamant.im

АДАМАНТ Бізнес— це корпоративна система передачі повідомлень та документів з можливістю їх цифрового підпису, інтегрована платіжна система, що дозволяє зменшити транзакніонні витрати всередині компанії.

Концепція АДАМАНТу

Захист даних та анонімність

Безпека передачі даних в даний час стає пріорітетом для більшості користувачів електронних пристроїв, як індивідуальних, так і корпаративних. Все більше подій у світі це підтверджують, і великі корпарації, такі як BlackBerry, IBM, Google, Apple, Samsung, Facebook пропонують свої рішення для захисту інформації.

Сучасні засоби шифрування використовують настільки стійкі алгоритми, що на розшифровку наіть невеликої кількості даних буде потрібно 100 років, нехай і застосовуючи суперкомп'ютери . Вони також захищені й від атак типу перехоплення повідомлень завдяки концепнії відкритого й закритого ключа, роблячи захист даних що передаються надійним.

На сьогоднішній день, напевно, не існує месенджера, який не включав би в себе засоби шифрування. Однак не всі користувачі ймуть віри цим месенджерам, і цілком обґрунтовано. Справа не в тому, що вони використовують недостатньо надійне шифрування, а в тім, що їхній програмний код закритий, і ніхто не може бути впевнений в тому, що програми не містять закладок і вони залишають поза передачею вашу інформацію третім особам.

Інша проблема — в отриманні особистих даних користувача. Майже всі месенджери вимагають доступ до адресної книги пристрою, і передають її (разом з іншими особистими даними) на свої сервери. Мотивуючи свою поведінку підвищенням зручності програмного продукту, такий підхід створює загрозу витоку і небажаного використання особистих даних на всіх етапах їх обробки.

Додаючи до цього необхідність попередньої ідентифікації месенджера з використанням номера телефону, електронної пошти, або іншим користувачем інформації, і пов'язуючи акаунт месенджера з акаунтами в соціальних мережах, з активністю в браузерах, корпорації отримують повну інформацію про користувачів, включаючи передані повідомлення і фотографії, місце розташування, контакти з іншими людьми, переваги, і іншу особисту інформацію

Незважаючти на те, що такий збір даних порушує право на недоторканість у особистоиму житті, юридично це приховано за прийняттям угод при встановленні месенджерів (які зазвичай ніхто не читає). Компанії, що збирають дані користувачів, використовують іх на свій розсуд, але особлива небезпека в тому, що є ризик отримання цих данних третіми особами.

Крім усього цього — все це централізовані сервіси обміну повідомленнями, які повністю володіють акаунтами користувачів, що дає їм можливість вносити обмеження в дані акаунти, або зовсім їх закрити. Блокування акаунтів Telegram в зв'язку з так званими “скаргами користувачів” — яскравий приклад даної особливості більшості месенджерів.

Ще однією проблемою існуючих месенджерів є розкриття IP-адреси користувача при встановленні підключення до центрального серверу, або Peer-to-Peer. Це питання вирішується використанням мережі Tor, або таких блокчейн-інфраструктур як АДАМАНТ.

Проект АДАМАНТ призначений вирішити питання надійності захисту передаваних даних, оскільки він базується на концепції захищеного блоку, і його програмний код відкрито. Кожен може провести свій незалежний аудит програмного коду і зібрати з нього повністю працюючу систему самостійно.

Іншою незаперечною перевагою технології Блокчейн є анонімність. Тобто на відміну від централізованих систем передачі повідомлень, не можна прив'язати переписку до конкретних осіб, завдяки відсутності іденифікаторів (немає номерів телефонів, акаунти електронної пошти або соціальні мережі, платні данні є тільки знеособлений ідентифікатор гаманця).

АДАМАНТ володіє наступними особливостями безпеки і анонімності:

- Повідомлення зберігаються прямо у блокчейні;
- Відсутність доступу до адресної книги користувача
- Немає доступу до місця розташування користувача;
- Особисті дані користувача не передаються;
- Немає ідентифікаторів користувача — повна анонімність;
- Повідомлення шифруються на пристрої відправника, а розшифровуються на пристрої одержувача. Доступу до повідомлень немає ні в кого (включаючи самих розробників) — див. схему передачі повідомлень АДАМАНТ;
- Клієнтський додаток ніколи не передає приватний ключ або мнемонік-фразу по мережі. Вся робота проводиться на пристрої користувача;
- Переписка не зберігається на пристрої взагалі — історія повідомлень довантажується безпосередньо з блокчейну;
- На відміну від P2P-месенджерів, не можна отримати IP-адресу користувача;
- Програмні коди месенджера месенджера і блокчейну відкриті;
- Акаунт АДАМАНТ не може буду обмеженим, заблокованим чи закритим ніким, включаючи розробників.

Правовий аспект гарантії таємниці переписки

Юрисдикція більшості країн світу гарантує недоторканість особистого життя і таємниці собистого життя і таємниці листування на рівні таких базових документів, як конституція.

Наприклад, Конституція РФ, стаття 23

1. *Кожен має право на недоторканність приватного життя, особисту і сімейну таємницю, захист своєї честі і доброго імені.*
2. *Кожен має право на таємницю листування, телефонних переговорів, поштових, телеграфних та інших повідомлень. Обмеження цього права допускається тільки на підставі судового рішення.*

Інший приклад — Конституція Італії, стаття 15:

“Свобода і таємниця листування і всіх інших видів зв'язку непорушні. обмеження їх може мати місце лише в силу мотивованого акту судової влади, з дотриманням гарантій, встановлених законом. "

Однак уряди всіляко намагаються порушити ці принципи, і громадянам доводиться шукати способи, щоб захищати свої права.

АДАМАНТ створений для захисту вашого особистого життя.

Зберігання повідомлень в АДАМАНТі

Всі повідомлення в АДАМАНТі зберігаються децентралізовано у блокчейні.

Це забезпечує:

- Надійне і надмірне зберігання списку повідомлень;
- Неможливість змінити повідомлення "заднім числом";
- засвідчену достовірність джерела і одержувача, захист від атаки MITM (Атака буде виявлена - зміниться ідентифікатор-гаманець відправника);
- Доступ з будь-якого пристрою - як при централізованому зберіганні;
- Надійна і підтверджена блокчейном доставка повідомлень;
- Безпека, забезпечена шифруванням за схемами Ed25519 EdDSA,Curve25519, Salsa20, і Poly1305.

Незважаючи на те, що доступ до всіх зашифрованих повідомлень має будь-який бажаючий, читання (розшифровка) конкретних повідомлень можлива тільки джерелом і одержувачем, що забезпечується сучасними засобами криптографії. Блокчейн, і зокрема, Bitcoin, довели надійність такого підходу - при тому, що баланс

всіх гаманців публічно доступний, ще не було випадків отримання доступу до них шляхом "злому" ключів шифрування..

Розрахункова система

У сучасному світі гостро стоїть питання доступності зручних і надійних платіжних інструментів, особливо на територіях, де застосовуються валюти з великою інфляцією, і де застосування традиційних платіжних систем обмежена в силу різних причин.

Технології Bitcoin і Blockchain вже показали, що здатні вирішити ці проблеми. В даний час існує безліч цифрових валют, зі своїми перевагами і недоліками.

АДАМАНТ включає власну платіжну одиницю - токен ADM, котра:

- Використовується для забезпечення інфраструктури у вигляді комісій за передачу повідомлень, прямі переклади, і додаткові функції системи;
- Має велику швидкість транзакцій (час блоку - 5 сек.);
- Зручна для прямих переказів співрозмовнику прямо в вікні чату;
- Не залежить від сторонніх сервісів і блокчейнів (АДАМАНТ побудований на незалежному блокчейні).

Доходность для владельцев токенов

Всі нерозпродані в рамках ICO-кампанії токени Адамант, будуть поступово і пропорційно розподілені серед всіх поточних власників. Таким чином в Протягом одного-двох років, ми стимулюємо власників до прийняття стратегії накопичення токенів замість звичайного спекулятивного продажу в момент виходу на біржі.

Докладний план цього процесу розподілу нерозпроданих токенов дивіться в фінансової частини цього документа - розділ "АДАМАНТ Зростає".

АДАМАНТ для бізнесу

Крім стандартних для месенджерів функцій передачі повідомлень і файлів, АДАМАНТ включатиме можливість цифрового підпису переданих документів для організації договірних угод.

АДАМАНТ передбачає інтеграцію внутрішньої "платіжної системи", тобто, можливість передачі токенів прямо в рамках чату, крім приєднання документів і файлів. Таким чином, під час діалогу можна зробити яку-небудь угоду, і зробити його оплату. Оскільки дані зберігаються у блокчейні, вони не можуть бути змінені в майбутньому.

У ряді випадків компаніям буде цікаво використовувати не загальний блокчейн ADM, а аналогічний приватний блокчейн, що працює тільки всередині компанії і між її партнерами. Таку можливість надає АДАМАНТ Бізнес

Для територіально-розподілених компаній блокчейн дозволяє значно знизити витрати при внутрішніх взаєморозрахунках: вартість транскордонного перекладу може бути скорочена в тисячі разів. Це особливо актуально, коли одна сума переводиться між обмеженим числом учасників кілька разів на Протягом року, і немає необхідності конвертувати ці кошти в фіатние валюти.

Розрахунки усередині компанії виробляються в токенах, а потім, в певні періоди, компанія конвертує їх в фіат.

Інше можливе застосування блокчейну для організацій — зв'язка токенів з будь-яким ресурсом - таким, як преміальні, трудомісткість, або стаж роботи. Платформа АДАМАНТ стане зручним і ефективним бізнес-інструментом.

Огляд альтерантивних рішень та їх порівняння

Месенджери - найбільш популярний і доступний спосіб комунікацій в сучасному світі. Кількість різних месенджерів обчислюється сотнями, а кількість користувачів в світі, які використовують хоча б один месенджер наближається до 100% від всього числа користувачів смартфонів і ПК. Однак кількість месенджерів, які працюють без централізованого сервера, а також орієнтованих на безпеку і анонімність, значно менше.

Оскільки основними особливостями Адамант є безпека і анонімність, в цьому порівнянні присутні тільки альтернативні рішення (тому з порівняння виключені такі месенджери як Kik Messenger, Skype, Google Hangouts та інші).

Через те, що безпека-анонімність і зручність в ряді випадків стоять по різні боки, в нашому порівнянні як переваги враховується відповідність месенджера саме критеріям безпеки і анонімності. Наприклад, якщо месенджер відображає статус повідомлення як "прочитано" - це збитки анонімності в догоду зручності.

З порівняння виключені також месенджери, які в даний час не мають працюючого прототипу: Echo, Status, Crypviser; і месенджери, які працюють тільки на настільних комп'ютерах (і не працюють на смартфонах): RetroShare, Tox, Bitmessage, Ricochet.

	ADAMANT	WhatsApp	Telegram	Facebook Messenger	Connect.im	Signal	Dust	Ring
Open Source Code for server, application and protocol parts	Yes	No	Closed Source Code for server part and Open Source for protocol and client apps	No	Closed Source Code for server part and Open Source for protocol and client apps	Yes	No	Yes
No centralised storage for any part of the User Data	All User Data is stored in the Blockchain (decentralised)	Operator stores Data of all conversations — including images, video and files	Operator stores all Data, except the one from the "Encrypted" chats	Operator stores data of all conversations — including images, video and files	Peer-to-peer, but there are intermediate servers which store undelivered messages	Operator is able to log all Data on servers	All Data is Stored and Viewed by the operator	Peer-to-peer, but there are intermediat servers which store undelivered message
Developers / Provider is NOT able to block user account	Yes	is Able / Blocking	is Able / Blocking	is Able / Blocking	Is Able	Is Able	is Able / Blocking	is Able
o explicit user identification	Yes	Mobile number is used for authorization	Mobile number is used for authorization	Mobile number of Facebook account is used for authorization	Mobile number is used for authorization	Mobile number is used for authorization	Mobile number of Facebook account is used for authorization	User account creatio in the Ring Network
End-to-end encryption (with inability for developers to read user messages)	Yes	There is a potential ability for operator to read all messages	There is a potential ability for operator to read all messages	There is a potential ability for operator to read all messages	Yes	Yes	There is a potential ability for operator to read all messages	Yes
No access to address book	Yes	Asks user for access	Asks user for access	Asks user for access	Asks user for access	Asks user for access	Asks user for access	Asks user for access
No access to user location	Yes	Asks user for access	Asks user for access	Asks user for access	Asks user for access	Yes	Asks user for access	Yes
Does NOT transfer user Private Keys over the network	Yes	Source Code is closed for Review	Source Code is closed for Review	Source Code is closed for Review	Stored encrypted on operator's servers	Yes	Source Code is closed for Review	Yes
Does NOT store message history or any other usage information on the user device	Yes	is Storing	is Storing	is Storing	is Storing	is Storing	Is able to delete messages from both end-users' devices.	is Storing
Does NOT disclosure or expose user IP-address	Yes	Exposed to Operator	Exposed to Operator	Exposed to Operator	Exposed to Operator	Exposed to Operator	Exposed to Operator	Directly interacts wit Ring Network
Not able to get statuses like «Message Read» or «User Online»	Yes	Enabled by default	You can hide only the "Last Seen" Status	You can only switch the "Active" Status	Yes	Asks for user Permission	Forced «Message Read" notifications. No Status for user Availability	Yes

Таблиця порівняння знаходиться за посиланням:
https://adamant.im/docs/ru-adamant-messenger-comparison-table-plain.png

Таким чином, АДАМАНТ покликаний вирішити питання конфіденційності та безпеки.

Технічне рішення

Архітектура системи

АДАМАНТ - децентралізована система на основі алгоритму з делегованим доказом частки (DPoS). Цей вибір заснований на необхідності відповідати певним критеріям:

- DPoS дозволяє надійно підтверджувати угоди за 5 секунд. Це час критично для реалізації швидкої передачі повідомлень;
- DPoS зменшує вартість підтримки системи — для цього не потрібно обчислювальних потужностей і витрати електрики (в порівнянні з PoW);
- Фіксовані комісії за транзакції;
- Гарна масштабованість і надійність.

Система АДАМАНТ складається з двох видів вузлів:

1. Повних нод, які розподілено зберігають і обслуговують всю базу даних блокчейн, а також беруть участь у формуванні нових блоків;
2. Легких клієнтів (лайт-клієнти), які займаються шифруванням даних на своєму боці з подальшою їх передачею в блокчейн.

Однак, всі операції з базою блокчейн виконуються повними нодами, з якими легкі клієнти спілкуються по захищеному протоколу HTTPs (End-to-End шифрування), використовуючи спеціальне API для передачі даних в форматі JSON.

У якості програмної основи повних нод використовується:

- Сервер на ОС Linux (Ubuntu). Можлива установка на інших платформи через додаток Docker;
- Сервер додатків Node.JS;
- PostgreSQL Server for storing the blockchain.

Лайт-клієнти являють собою:

- Прогрессивное Веб-приложение (PWA) — веб-приложение для современных браузеров;
- HTML5, JS, CSS, Vue — программные языки и Веб-технологии;
- Інтерфейс взаємодії з повними нодами за допомогою спеціального API.

Для взаємозв'язку між собою всі вузли використовують P2P-з'єднання поверх протоколу HTTPs.

Специфікація токену АДАМАНТ

- Назва токену: ADAMANT (ADM)
- Технологія DPoS, Delegated Proof of Stake
- Максимальна кількість токенов: 200 млн ADM
- Первісна емісія (Genesis-блок): 98 млн ADM
- Час блоку: 5 секунд (17 280 блоків в день, близько 6 307 200 блоків в рік)
- Розмір блоку: варіативний (без обмежень)
- Винагорода за блок:
    - Перший рік: 1 ADM за блок
    - Наступні роки: винагорода зменшується на 0.05 ADM щороку до досягнення 0.1 ADM
    - Період початку отримання винагород: з блоку номер 1,500,000 (приблизно 3 місяці)
- Винагороди за транзакції (плата за транзакції):
    - Пряма передача токенів: 0.5 ADM
    - Передача повідомлення: 0.005 ADM за кожні 256 символів в UTF-8 (приблизно). Комісія за передачу повідомлення може бути адаптована в подальшому в залежності від ринкової ціни токену
    - Оновлення інформації профілю: 0.05 ADM
    - Завантаження аватара 128x128 пх: 0.1 ADM
    - Передача зображення (без зберігання в блокчейні): 0.05 ADM за кожні 100 КБ
    - Передача документа (з храненням в блокчеїне): 1 ADM за 1 КБ
    - Підпис документа: 10 ADM
    - Реєстрація делегата: 300 ADM
    - Голосування за делегата: 10 ADM
- Первоначальное начисление при створенні кошелька:
    - 0.49 ADM до блоку 6 300 000 (близько року) - 98 безкоштовних повідомлень
    - Далі кожні 125 000 блоків первинне нарахування зменшується на 0.01 ADM до досягнення мінімуму 0.01 ADM (ще близько року);
- Програмний код відкритий (GNU GPLv3)
- Порти за замовчуванням: 36666 для MainNet, 36667 для TestNet

Незалежний блокчейн

Сучасні тенденції використання блокчейну Ethereum в випадку з АДАМАНТ не підходять. Це пояснюється досить високою вартістю "газу" (комісії), який необхідний для проведення кожної транзакції, включаючи всі транзакції з передачі повідомлень. АДАМАНТ же побудований на незалежному блокчейні, тому вартість передачі повідомлень значно нижче і може бути адаптована в залежності від ціни токену в майбутньому.

Крім того, не підходить і технологія Proof of Work, оскільки вартість підтримки такої інфраструктури висока, і зі збільшенням кількості учасників комісія за транзакції також буде рости.

З цих причин для реалізації серверної частини (блокчейну) використаний програмний код проекту Lisk, який був розширений для отримання необхідної функціональності.

Архітектура АДАМАНТ досить адаптивна, щоб при необхідності можна було вносити зміни в ціну комісій за транзакції.

Транзакції у АДАМАНТі

Кожен блок включає в себе варіативну кількість транзакцій. Для того, щоб транзакція була підтверджена, необхідно від 6 до 10 підтверджень (це важливо тільки для транзакцій передачі токенов і підписання документів, повідомлення ж приходять після першого підтвердження). Види транзакцій в мережі:

1. Пряма передача токенів
2. Передача повідомлення
3. Оновлення профілю, адресної книги і налаштувань, що зберігаються в блокчейні
4. Завантаження аватар-зображення
5. Створення групового чату
6. Закриття (приховування) чату
7. Передача документа (зберігання у нодах)
8. Підписання документа
9. Реєстрація делегата
10. Голосування за делегата

Транзакції вимагають оплату за їх проведення, вона ділиться між делегатами у вигляді плати за підтримку мережі (див. Специфікацію токенів).

Підтримка інфраструктури та майнінг (форжінг) ADM

Інфраструктура АДАМАНТ підтримується системою розподілених серверів, на яких виконуються повні Ноди (вузли). Витрати на підтримку серверів покриваються токенами ADM ("Майнінг"):

1. Комісії за транзакції
2. Винагорода за створення блоків.

Щоб брати участь в Майнінгу, нода повинна зареєструватися як делегат мережі, і отримати голоси інших користувачів АДАМАНТу. Плата за реєстрацію делегата - 300 ADM. Користувач Адамант, який голосує за делегата, оплачує 10 ADM.

Протокол / алгоритм функціонування схеми DPoS базується на голосуванні, що відбувається в режимі реального часу (на основі рівня репутації учасників мережі), що дозволяє вибрати перелік осіб (делегатів-вузлів), наділених довірою. Ці особи, після обрання, мають право створювати і верифікувати блоки для включення їх в ланцюг блокчейну, а також перешкоджати вторгненню сторонніх в цей процес. Цей перелік довірених осіб створює блоки по черзі, в випадковому порядку, який змінюється кожен раунд.

Делегати виробляють нові токени при створенні блоків.

Кількість вироблених токенів поступово зменшується, на початку існування системи - 1 ADM за 1 блок, але кожні 6 307 200 блоків (приблизно рік) це число буде зменшується на 0.05 ADM, поки не зупиниться на величині 0.1 ADM за 1 блок - близько 19 років.

Виходячи з розрахунків, делегати будуть отримувати винагороди протягом 76 років. Надалі інфраструктура буде підтримуватися тільки завдяки комісіям за транзакції.

Кількість активних делегатів, що беруть участь в процесі створення блоків — 101. У разі, якщо делегатів менше, 101 голос розподіляється серед існуючих вузлів мережі (повних нодів). Мінімальна кількість вузлів — 3.

Система стає більш стабільною і надійною зі збільшенням кількості вузлів.

Для створення кожного нового блоку з використанням DPoS відбувається голосування, в результаті якого вибираються 101 делегат з пулу делегатів для створення наступних 101 блоків.

Голосування проводять вузли автоматично на підставі довіри до делегату, а також часу його знаходження в онлайн. Після того як делегати обрані, їм виділяється порядок формування блоків, і вони починають їх створювати. Створення 101 блоку займає приблизно 8 хвилин.

Виплати за створення блоків починаються з 1,500,000 блоку. Такий захід гарантує, що перші учасники не отримають токени з найменшими зусиллями. А це в свою чергу

забезпечує створення інтересу у нових користувачів і підтримки рівноправності серед всіх користувачів блокчейну.

Інформація про блоки розсилається з інтервалом в 5 секунд, кожен пакет блоків розсилається один раз від вихідного вузла, і по два рази від кожного отримав його вузла для більш швидкого поширення в рамках мережі.

Транзакції, які не розміщені в новому блоці, очікують у черзі транзакцій, чергу може зберігати до 5000 транзакцій, при цьому час життя транзакції 1080 блоків.

Якщо за цей час транзакція не була додана в блок, вона вважається непідтвердженою і не приймається в блокчейн, віддаляючись з пулу очікуючих транзакцій (стан гаманців не змінюється).

Для визначення актуальності блокчейну використовується broadhash — хеш, сформований на основі останніх 5 транзакцій в блокчейні. Він дозволяє швидко упевнитися, що всі ноди мають однакове стан блокчейну.

Плата за транзакції рівномірно ділиться між делегатами, які беруть участь в процесі формування блоку, і проводиться в кінці кожного циклу з 101 блоку.

Надійність так безпека системи

АДАМАНТ є надійною системою, побудованою на блокчейні і здійсненоюї завдяки реалізації концепцій:

- Розподіленість. Блокчейн вдає із себе іммутабельную (незмінну) розподілену базу даних, що дозволяє записувати дані, і не дозволяє вносити в них зміни, за рахунок чого можна використовувати його для безпечного, відкритого, і надійного зберігання інформації;
- Технологія DPoS дозволяє творцям контролювати блокчейн в більшій мірі в порівнянні з PoW. У випадку з PoW можна підключити до мережі комп'ютер значно більшої потужності, отримавши контроль над мережею;
- За рахунок механізму broadhash консенсусу, що вибирає найбільш довгий форк, система забезпечує стійкість перед впливами типу тимчасової десинхронизации частини мережі;
- При створенні гаманця генерується BIP39-мнемокод, на основі якого обчислюється приватний ключ. Даний приватний ключ використовується для генерації публічного ключа, який однозначно визначає адресу гаманця. Після цього користувач може починати користуватися системою. Кількість адрес гаманців прямує до нескінченності.

- Усі транзакції підписані приватним ключем, використовуючи стійкий алгоритм електронного підпису Ed25519 EdDSA;
- Всі повідомлення месенджера шифруються на пристрої-відправника (алгоритми Curve25519, Salsa20, і Poly1305) і розшифровуються на 1 пристрої-одержувачі.
- Клієнтське застосування не передає приватний ключ або мнемонік-фразу по мережі. Вся робота проводиться на пристрої;
- На відміну від P2P-месенджерів, не можна отримати IP-адресу користувача.

Обсяг даних для зберігання

На сьогодні досить важко оцінити обсяги даних, які будуть зберігатися в нодах АДАМАНТ. Але деякі припущення можуть бути зроблені.

Приблизна сума щоденних повідомлень — 10 000 повідомлень кожен день на перший рік з зростанням до 100,000 на наступні декілька років.

Припускаючи, що одне повідомлення містить в середньому 100 символів, обсяг даних, необхідних для безпечного зберігання цього повідомлення в блокчейні, розраховується, як 100 символів * 2 байтів * коефіцієнт збільшення шифрування 1,5 - його загальний розмір приблизно дорівнює 300 байт.

Таким чином, обсяг простору, необхідного для зберігання цих повідомлень протягом першого року, може бути розрахований, як 10 000 повідомлень * 365 днів * 300 = 1 Гб, з можливим збільшенням на 10 Гб на рік. Блокчейн АДАМАНТ має потенціал для збільшення до 50 Гб або більше протягом наступних 10 років.

Загальна сума комісій, отриманих майнерами за таку кількість відправлених повідомлень, починається з 10 000 * 365 * 0,005 ADM = 18 250 ADM на перший рік, повільно зростаючи до 182 500 ADM протягом наступних років.

Враховуючи ті факти, що майнери також отримають свої нагороди за обрахунок блоків, збільшення ринкової ціни токену ADM і досить дешеві витрати на зберігання даних, інфраструктура АДАМАНТ буде ефективно підтримуватися, а майнери постійно отримуватимуть прибуток.

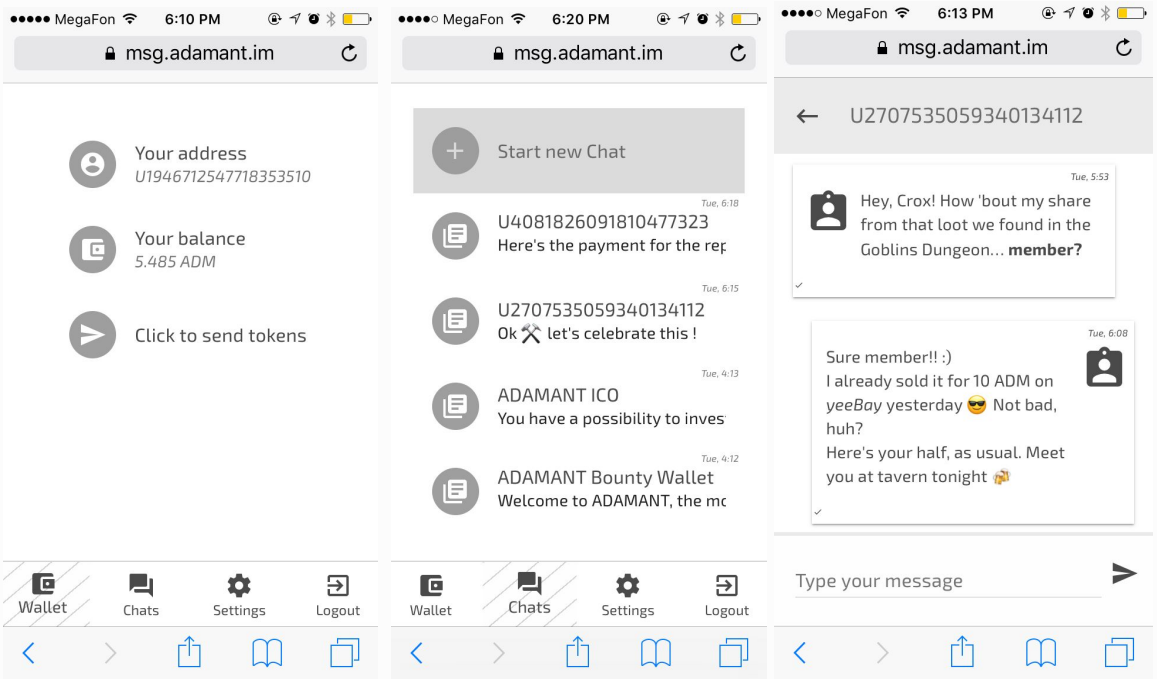
Поточний стан проекту

До моменту запуску Pre-ICO (14.12.2017) система АДАМАНТ являє собою повністю функціональний продукт, що має такі особливості:

- Передача повідомлень (Месенджер АДАМАНТ);
- Зберігання та передача токенів;
- Дослідження інформації про стан блокчейну ADM;
- Повністю готова інфраструктура нод мережі Blockchain.

Месенджер АДАМАНТ

АДАМАНТ месенджер є доступним по наступному посиланню https://msg.adamant.im



На даний момент месенджер АДАМАНТ реалізується як прогресивний веб-додаток (PWA), який працює в основних сучасних браузерах мобільних і настільних платформ. Також планується розробка власних додатків для платформ Android і iOS.

Системні потреби месенджеру АДАМАНТ:

- Для смартфонів:
  - Apple iOS 9 та вище
  - Google Android 5.0 та вище / браузер Google Chrome (версія 62+)
- Для настільних комп'ютерів:
  - Будь-який сучасний браузер.

Месенджер АДАМАНТ має можливість зберігати та надсилати токени ADM (гаманець).

Функції месенджеру АДАМАНТ:

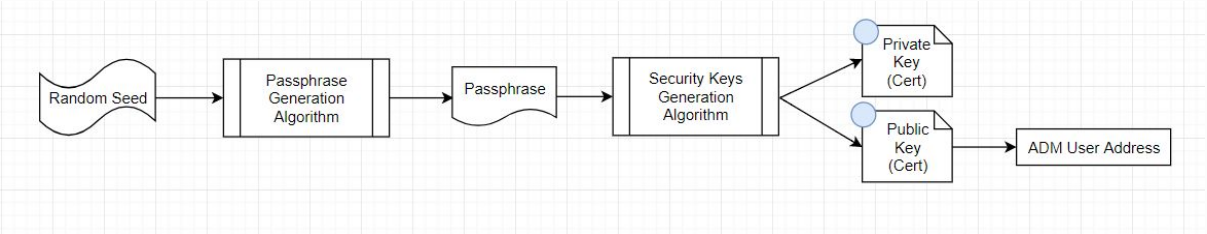
- Шифрування передачі повідомлень;
- Список діалогів та історія переписок;
- Список транзакцій;
- Сповіщення про повідомлення;
- Деталізованна інформація про кожну транзакцію;
- Встановлення імені (або псевдоніму) для адреси співрозмовника;
- Підтримка смайлів;
- Підтримка розмітки Markdown.

Заплановані функції месенджеру АДАМАНТ:
(будь ласка, перегляньте “Дорожню карту” нашого проекту)

- Внутрішня адресна книга;
- Зберігання профілів на базі блокчейну;
- Передача токенів через вікно чату;
- Передача токенів через сповіщення в вікні чату;
- Передача фотографій;
- Зберігання документів на базі блокчейну;
- Цифровий підпис (підтвердження) документу;
- Улюблені чати та повідомлення (закладки);
- Пошук по контактам та повідомленням;
- Полегшений вхід за допомого. пін-коду;
- Проховані чати;
- Групові чати.

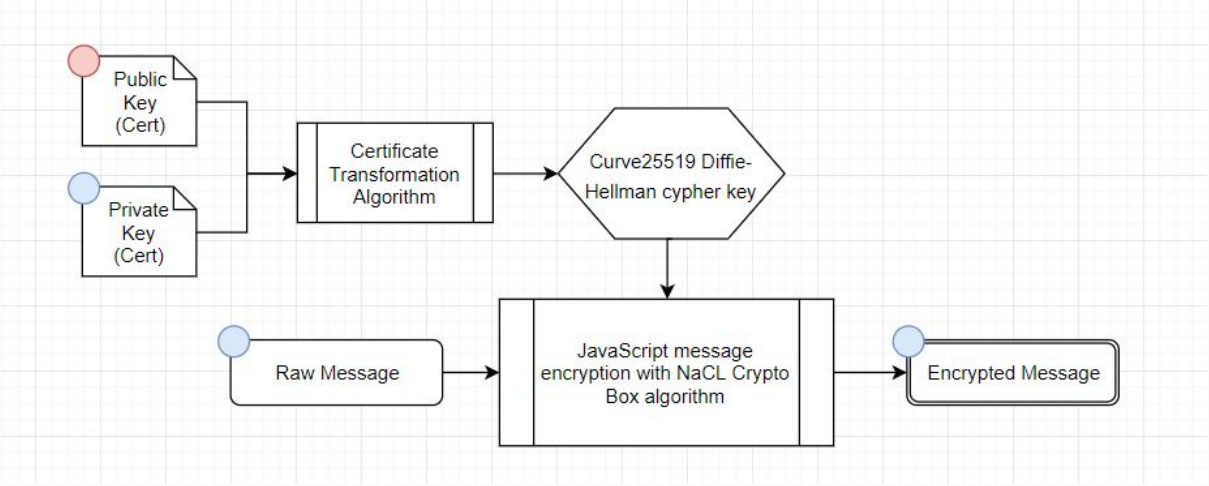
Ви можете взнати про всі переваги АДАМАНТу детальніше, в вкладці “Концепція АДАМАНТу” цього документу.

Схема створення акаунту в месенджері АДАМАНТ— на пристрої користувача:



1. Генерація випадкового значення
2. На основі Seed генерується пароль (мнемонічна пасфраза)
3. На основі пассфрази генерується публічний і приватний ключі
4. На основі публічного ключа генерується ADM-ідентифікатор (адреса гаманця користувача)

Робоча схема месенджеру АДАМАННТ — на пристрої користувача:



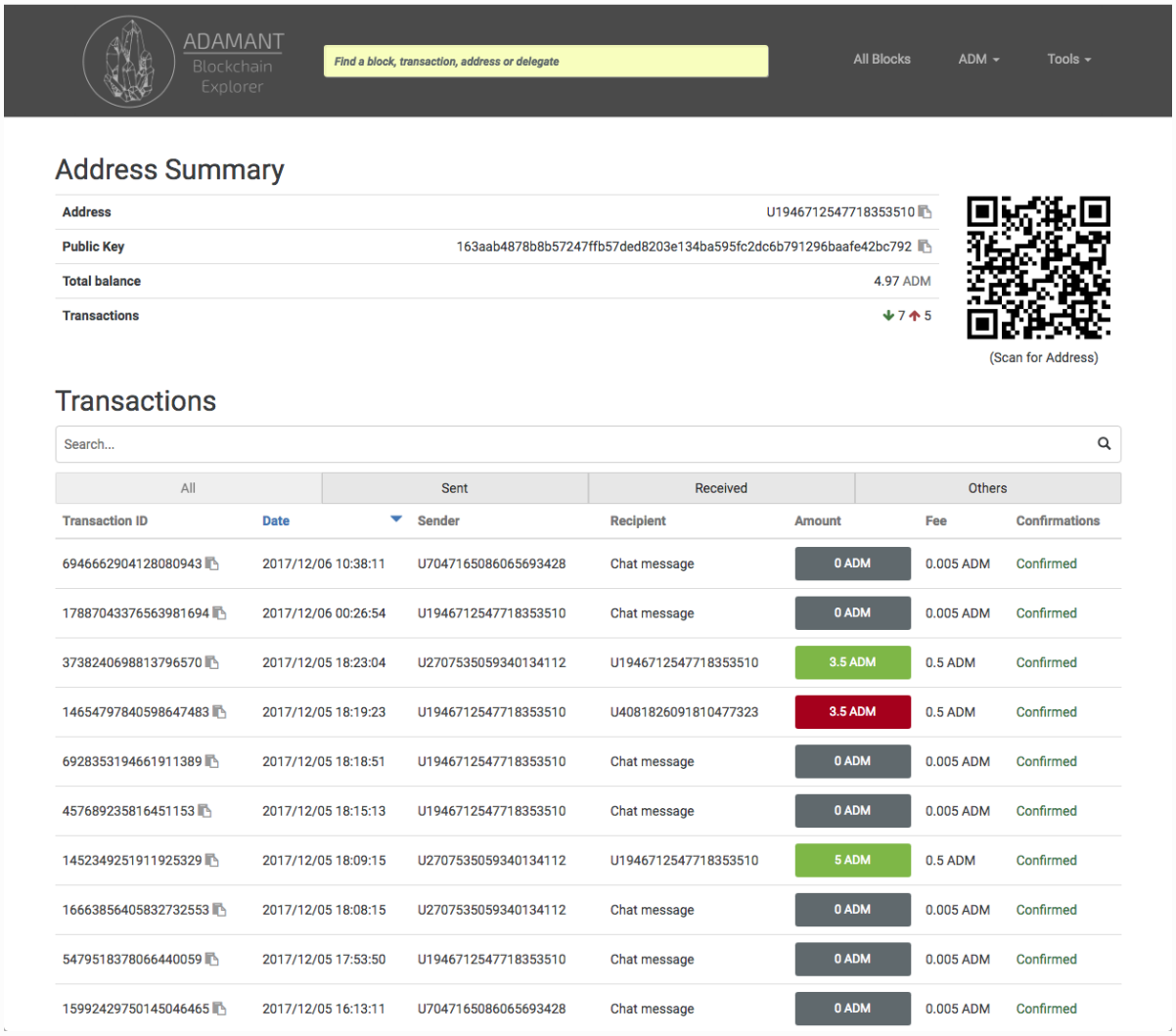
1. Повідомлення локально шифрується на пристрої користувача (використовуючи Curve25519, Salsa20, and Poly1305 алгоритми)
2. Зашифроване повідомлення передається за допомогою випадкового виділеної ноди до блокчейну.

Оскільки всі повідомлення повністю зашифровані на пристрої користувача перед відправкою до блокчейну, немає точного способу визначити точний розмір повідомлення (загальна кількість символів всередині нього). Тому плата за переказ розраховується приблизно - 0,005 ADM для кожного отриманого 255 символьного UTF-8 повідомлення. Плата за передачу повідомлень буде додатково скорегована відповідно до ринкової ціни токенів ADM.

Месенджер АДАМАНТ доступний для використання кожному. Впродовж двох років після випуску першого релізу, всі нові облікові записи отримають невелику кількість токенів ADM, для ознайомлення з месенджером.

Blockchain Explorer

Blockchain Explorer відображає інформацію про стан блокчейну АДАМАНТ, показує список блоків, список транзакцій і інформацію по ним, включає графік активності, інформацію про делегатів і мережі.



Blockchain Explorer доступний за посиланням https://explorer.adamant.im

Дистрибутив повного вузла

Кожен, хто хоче підтримати інфраструктуру АДАМАНТ, може розгорнути повний вузол, зареєструватися як делегат і отримувати винагороду за блоки та комісії за транзакції (для реєстрації в якості делегата передбачена плата 300 ADM, а так само потрібно отримати голоси користувачів).

Інструкції по встановленню на сайті: https://adamant.im/devs/

Фінансова частина

Обґрунтування цінності токену

ADM - токен з цінністю, забезпеченою платою за передачу повідомлень і даних. Це плата за гарантовану анонімність та захищеність даних. АДАМАНТ Бізнес також включає функції підпису документів.

Додаткова цінність токену ADM забезпечується розподілом нерозпроданих на ICO токенов. Користувачі, які зберігають на своїх гаманцях токени ADM, щомісяця отримують винагороди пропорційні своїм активам.

Емісія токенів

З моменту запуску блокчейну був створений генезис-блок - гаманець первісної емісії в розмірі 98 млн ADM.

Розподілення початкової емісії

- 75% (73,500,000 ADM) - гаманець для проведення ICO;
- 4% (3,920,000 ADM) - резерв на розробку і підтримку інфраструктури;
- 4% (3,920,000 ADM) - резерв на маркетингові кампанії АДАМАНТ Бізнес;
- 9% (8,820,000 ADM) — initial Investors' rewards;
- 8% (7,840,000 ADM) - гаманець Adoption на забезпечення кампанії Bounty і первинних нарахувань користувачам.

Максимальна (кінцеве) кількість токенов - 200 млн одиниць.

Таким чином, 102 млн ADM (а також комісії за транзакції) будуть використані в якості плати майнерам за підтримку мережі.

Винагорода за блок - 1 ADM в перший рік, зменшується на 0.05 ADM кожен наступний рік до досягнення 0.1 ADM. З огляду на, що кількість створюваних блоків в рік близько 6,307,200, делегати будуть отримувати винагороди за блоки протягом 76 років, в подальшому інфраструктура буде підтримуватися тільки завдяки комісіям за транзакції.

Період початку отримання винагород: з блоку номер 1,500,000 (приблизно 3 місяці).

Залучення коштів на розробку і розвиток проекту (кампанії Pre-ICO і ICO)

Для завершення розробки Адамант, його підтримки і розвитку, планується залучити кошти інвесторів на Pre-ICO і ICO, завдяки продажу токенов ADM з генезис-блоку (обсяг гаманця для проведення ICO - 73,500,000 ADM).

Всі нерозпродані токени гаманця ICO будуть розподілені між користувачами гаманців АДАМАНТу згідно з планом, представленому в розділі "АДАМАНТ Росте"

Pre-ICO - залучення коштів інвесторів на найкращих умовах

Терміни проведення: 14.12.2017-25.01.2018.

- Спосіб проведення: прямий переклад на гаманці розробників. Запити приймаються на англійській і російській мовах через месенджер АДАМАНТ гаманця ICO (U7047165086065693428).
- Отримання токенів ADM: прямий переклад на гаманець інвестора
- Криптовалюта, що приймається: ETH, BTC, BCH, DASH, DOGE, LTC, XMR, NEM, ETC, ZEC, WAVES, LSK, REP, GNO, ICN, MCO, ANT, CVC, EOS, DNT, OMG, DCR
- Ціна токену: 1 000 ADM = 1 ETH (1 ADM = 0.001 ETH). Ціна токену в інших криптовалютах перераховується по відношенню до ETH.
- Мінімальна інвестиція: 2 ETH (або еквівалент)
- Бонуси інвестування:
    - від 20 до 30 ETH: + 20% ADM
    - від 30 до 50 ETH: + 30% ADM
    - від 50 до 90 ETH: + 40% ADM
    - від 90 і більше ETH: + 50% ADM

Фінальна стадія ICO

Графік: 30.01.2018—30.03.2018

- Як інвестувати в ICO: через систему обміну на веб-сторінці https://adamant.im/ico/
- Як отримати токени ADM: через автоматичну передачу токенів інвесторам відразу після того, як платіж було отримано та підтверджено мережею
- Приймаються криптовалюти: ETH, BTC, BCH, DASH, DOGE, LTC, XMR, ETC, ZEC, LSK
- Ціна токену: від 0.002 ETH до 0.005 ETH за 1 ADM токен.
  Точна ціна токену ADM для інших криптовалют динамічно розраховується на основі фактичної ціни ETH на дату вашої покупки.
- Мінімальна сума інвестування: відсутня
- Фази ICO:
  - Перша:
    - 30.01.2018—14.02.2018
    - Ціна токену: 1 ADM = 0.002 ETH
  - Друга:
    - 15.02.2018—28.02.2018
    - Ціна токену: 1 ADM = 0.003 ETH
  - Третя:
    - 01.03.2018—14.03.2018
    - Ціна токену: 1 ADM = 0.004 ETH
  - Четверта:
    - 15.03.2018—30.03.2018
    - Ціна токену: 1 ADM = 0.005 ETH
- Інвестиційні бонуси (однакові для всіх фаз):
  - від 20 до 30 ETH: + 20% до загального обсягу отриманих ADM
  - від 30 до 50 ETH: + 30% до загального обсягу отриманих ADM
  - від 50 до 90 ETH: + 40% до загального обсягу отриманих ADM
  - більше, ніж 90 ETH: + 50% до загального обсягу отриманих ADM

УВАГА: Для участі в будь-який ICO-кампанії ви повинні строго керуватися правовим законодавством своєї країни свого перебування (наприклад - формально резидентам США і Китаю брати участь в ICO-кампаніях заборонено).

План бюджету проекту

Усі кошти, отримані в рамках ICO, будуть використовуватися для розробки, підтримки та розвитку АДАМАНТу.

Soft cap — $500,000. Hard cap — $30,000,000.

Soft cap забезпечить необхідну кількість ресурсів, потрібну для розробки основних функцій месенджера та всієї його інфраструктури, а кошти, що перевищують його дозволяють пришвидшити розробку та залучити максимальну кількість користувачів.

Дворічний план розподілу залучених коштів:

- Підтримка інфраструктури — 10%
    - Сервери
    - Зарплата персоналу
- Розробка — 30%
    - Зарплата персоналу
    - Оренда та обслуговування офісних приміщень
    - Технічне оснащення
    - Вихід на криптовалютні біржі
    - Зовнішні консультанти
- Зовнішній аудит кода і безпеки — 10%
- Залучення користувачів — 50%
    - Оффлайн-кампанії та участь в конференціях
    - Зарплата співробітникам
    - Контекстна реклама
    - Реклама на тематичних ресурсах
    - Написання та публікація тематичних статей

«АДАМАНТ Росте»

З метою підвищення цінності ADM-токенів, всі непродані на ICO токени ADM гаманця ICO буде розподілятися між поточними власниками - щомісяця кожен гаманець буде рости на 5%.

Термін нарахувань - до вичерпання гаманця ICO.

Таким чином, чим раніше інвестувати в АДАМАНТ, і чим довше зберігати токени, тим більше прибутковість.

- Старт розподілу: 11.04.2018
- Періодичність розподілу: щомісяця
- Відсоток нарахувань
- Закінчення розподілу: до вичерпання гаманця ICO

Не беруть участь в розподілі токенов:

1. Системні гаманці (ICO, винагороду засновників, Adoption, гаманці резерву);
2. Гаманці, баланс яких менше 10 ADM;

Інформація про кожен раунд розподілу відкрита, доступна в експлорері, і буде публікуватися на сайті Проекту.

Розміщення токену ADM на кріптовалютних біржах

Після завершення кампанії ICO планується розміщення токенів ADAMANT (ADM) для вільної торгівлі на кріптовалютних біржах: Livecoin, Yobit, Liqui, Bittrex..

Адаптація і просування

Месенджери є зручним засобом комунікацій. Користувачів месенджерів стає все більше, поступово наближаючись до позначки в 100% населення.

АДАМАНТ знайде свою категорію користувачів, яким важлива безпека переданих повідомлень в сукупності зі зручністю передачі токенов.

Особливістю релізу нового месенджера є його нерівномірна швидкість приросту кількості користувачів. Спочатку кількість нових користувачів росте повільно, в подальшому, в міру того, як нові користувачі запрошують своїх друзів і знайомих, починається експоненціальне зростання кількості активних користувачів.

Проект АДАМАНТ передбачає наступні кампаній для збільшення кількості активних користувачів:

- Проведення ICO, залучення користувачів крипто-спільноти;
- Бонусна кампанія;
- еклама у соц. мережах;
- Маркетингові кампанії (онлайн та офлайн);
- Організація конференцій;
- Початкові нарахування на гаманці користувачів
- АДАМАНТ для бізнесу.

Початкові нарахування на гаманці користувачів

Всі транзакції в блокчейні вимагають мінімальної комісії. Це необхідно для підтримки інфраструктури мережі.

Для того, щоб користувачі могли ознайомитися з перевагами АДАМАНТ безкоштовно, передбачені початкові нарахування при створенні нового гаманця:

- 0.49 ADM до блоку 6 300 000 (близько року) - 98 безкоштовних повідомлень
- Далі кожні 125 000 блоків первинне нарахування зменшується на 0.01 ADM до досягнення мінімуму 0.01 ADM (ще близько одного року)

Оскільки комісія за прямий переклад становить 0.5 ADM, первинного нарахування недостатньо для зловживання і накопичення отриманих токенів в одному гаманці. Початкові нарахування проводяться в перші хвилини створення акаунта з гаманця Adoption (7,840,000 ADM). Таким чином, орієнтовна кількість користувачів, які зможуть протестувати роботу системи безкоштовно - від 7 до 14 мільйонів.

Кампанія Bounty

Бонусні кампанії проводиться для того, щоб дозволити користувачам зробити свій внесок у розвиток АДАМАНТ та отримувати свої винагороди за допомогою токенів ADM.

Кампанія відбудеться між 14.12.2017 та 20.03.2018 та включає в себе:

- Нагороди за підписи та аватари Bitcointalk.org;
- Активність в соціальних мережах;
- Переклад і підтримка основної гілки на Bitcointalk і гілки Bounty на Bitcointalk.org;
- Переклад сайту, додатку-мессенджера, Whitepaper;
- Статті в блогах і на сайтах;
- Розміщення банерів на веб-сайтах.

Додаткова інформація про бонусні кампанії розташована на https://adamant.im/bounty/

Дорожня карта проекту (2017-2018)

✓ 2-й квартал 2017

✓ Розробка концепції АДАМАНТ
✓ Консультація з експертами цієї гілки
✓ Розгортання тестової мережі "АДАМАНТ"

✓ 3-й квартал 2017

✓ Розробка веб-додатку (гаманець та месенджер)
✓ Створення Whitepaper

4-й квартал 2017

✓ Розробка веб-сайту
✓ Запуск робочої мережі АДАМАНТ
✓ Ствоврення пакету дистрибутиву вузла мережі (full node)
✓ Створення ADAMANT Blockchain Explore
✓ Налаштування інформаційних ресурсів (соціальні мережі, форуми і блоги)
✓ Запуск Bounty-кампаній (заохочення активних учасників)
✓ Внутрішній аудит безпеки
✓ Початок Pre-ICO (14.12.2017)

1-й квартал 2018

✓ Закриття Pre-ICO (25.01.2018)
✓ Початок CO (01/30/2018)

- Адаптація мессенджера АДАМАНТ і просування (маркетинг)
- Переклад інформаційних ресурсів на популярні мови
- Расширение функционала мессенджера АДАМАНТ (профили пользователей, упрощённый логин, передача файлов и токенов прямо из чата)
- Завершення ICO (03/30/2018)

2-й квартал 2018

- Публікація месенджера АДАМАНТ для мобільної ОС iOS
- Розміщення токену ADM на кріптовалютних біржах
- Масштабування усієї робочої інфраструктури
- Розширення функціональності месенджера АДАМАНТ (адресна книга, групові чати, пошук за списком повідомлень, приховування чату)

3-й квартал 2018

- Запуск Бізнес-версії системи АДАМАНТ (з функціями підпису документів і їх зберігання в базі блокчейн)
- Публікація месенджера АДАМАНТ для мобільної ОС Android
- Маркетингові кампанії

4-й квартал 2018

- незалежний аудит безпеки
- Установка АДАМАНТ Бізнес компаніям-партнерам
- Маркетингові кампанії

Колектив АДАМАНТу

В нашій команді більше 20-ти учасників.
(головні з них є нижче)

Керівник проекта — Євгенов Павло Сергійович

Менеджер і інноватор, під керівництвом якого завершено безліч проектів в IT і фінансах. Ступінь MBA.Закінчив IMEI за фахом Державне і муніципальне управління. Секретар Молодіжної Громадської Палати м Москви

http://vk.com/p.evgenov

Ведучий розробник — Лебедев Олексій Юрійович

Блокчейн-ентузіаст. Сертифікований фахівець: IBM Certified Solution Designer — IBM Rational Unified Process. Досвід роботи в IT-проектах 15 років. Керівник компаній ІнфоРешенія і irSoftware.

lebedevau@gmail.com

Ведучий розробник— Солодухин Дмитро Андрійович

Магістр кафедри Інформаційних Систем ВлГУ. Розробник і системний архітектор інформаційних систем різного призначення, включаючи блокчейн. Спеціаліст IT широкого профілю. Інтереси: Lego, фото.

https://www.linkedin.com/in/dmitriy-soloduhin

Головний дизайнер — Пихтовніков Максим Костянтинович

Випускник факультету Мікроприладів і технічної кібернетики (MIET). Дизайнер і маркетолог з досвідом роботи у великих міжнародних компаніях. З 1999 року захоплюється питаннями мережевої безпеки і захисту інформації.IT-консультант і керівник, коуч.

https://www.linkedin.com/in/pikhtovnikov/

Радник — Анісімов Леонід Андрійович

Випускник МНТУ ім. Н. Е. Бауманта факультету енергомашинобудування. Фрилансер та інвестор. Полюбляє подорожі та екстримальний спорт.

https://www.facebook.com/leonid.anisimov.16

Радник — Соколов Денис Євгенович

Московський Державний Університет ім. Н. Е. Баумана. державний Університет Управління (MBA). Інвестор IT-компанії HHI. Захоплення: подорожі, спорт.

https://www.facebook.com/denis.sokolov.9/

Радник — Медведєв Андрій Юрійович

Закінчив ліцей із золотою медаллю. МГУЕСІ з червоним дипломом. захоплюється східними єдиноборствами. Венчурний інвестор. Заступник з фінансів в колегії адвокатів «магнетари».

https://www.facebook.com/andrey.zebir

Ресурси АДАМАНТу:

- Веб-сайт: https://adamant.im
- Месенджер: https://msg.adamant.im
- Оглядач блоків (Block Explorer): https://explorer.adamant.im
- Вихідний код на Github: https://github.com/Adamant-im
- Twitter: https://twitter.com/adamant_im
- Facebook: https://www.facebook.com/adamant.im
- ВКонтакте: https://vk.com/adamant_im
- Slack: https://adamant-im.slack.com
- Telegram: https://t.me/adamant_im
- Форум Bitcointalk: https://bitcointalk.org/index.php?topic=2626754