ADAMANT

БУДУЩЕЕ ОБМЕНА СООБЩЕНИЯМИ

WHITEPAPER

БЕЛАЯ КНИГА

v. 1.5.2 RUS

Резюме

Система передачи сообщений и данных, основанная на блокчейн-технологиях, в сочетании с интегрированной платежной системой вносит принципиальные преимущества для личных и бизнес-коммуникаций.

АДАМАНТ для частных лиц — мессенджер на блокчейне, доступный с любого устройства. Непревзойденные анонимность и защита данных, удобство использования, интегрированная платежная система.

Для поддержки инфраструктуры АДАМАНТа используется Utility-токен ADM, работающий как внутренняя обменная единица.

Мессенджер доступен для использования: https://msg.adamant.im

АДАМАНТ Бизнес — корпоративная система передачи сообщений и документов, с возможностью их цифровой подписи, интегрированная платежная система, позволяющая снизить транзакционные издержки внутри компании. АДАМАНТ Бизнес позволяет каждой компании развернуть собственную сеть для обмена зашифрованными сообщениями.

Концепция АДАМАНТа

Защита данных и анонимность

Безопасность передачи данных в настоящее время становится приоритетом для большинства пользователей электронных устройств, как индивидуальных, так и корпоративных. Все больше событий в мире это подтверждают, и крупные корпорации, такие как BlackBerry, IBM, Google, Apple, Samsung, Facebook предлагают свои решения для защиты информации.

Современные средства шифрования используют настолько стойкие алгоритмы, что на расшифровку даже небольшого количества данных потребуется сотни лет даже с использованием суперкомпьютеров. Они также защищены и от атак типа перехвата сообщений благодаря концепции открытого и закрытого ключа, делая защиту передаваемых данных надежной.

На сегодняшний день, наверное, нет мессенджера, который бы не включал средства шифрования. Однако не все пользователи доверяют этим мессенджерам, и вполне обоснованно. Дело не в том, что они используют недостаточно надежное шифрование, а в том, что их программный код закрыт, и никто не может быть уверен в том, что программы не содержат “закладок” и они не передают вашу информацию третьим лицам.

Другая проблема — в получении личных данных пользователя. Почти все мессенджеры требуют доступ к адресной книге устройства, и передают её (вместе с другими личными данными) на свои серверы. Мотивируя такое поведение повышением удобства программного продукта, такой подход создает угрозу утечки и нежелательного использования личных данных на всех этапах их обработки.

Добавляя к этому необходимость предварительной идентификации мессенджера с использованием номера телефона, электронной почты, или другой учетной информации, и связывая аккаунт мессенджера с аккаунтами в социальных сетях, с активностью в браузерах, корпорации получают полную информацию о пользователях, включая передаваемые сообщения и фотографии, местоположение, контакты с другими людьми, предпочтения, и другую личную информацию.

Несмотря на то, что такой сбор данных нарушает право на неприкосновенность личной жизни, юридически это скрыто за принятием соглашений при установке мессенджеров (которые, как правило, никто не читает). Компании, собирающие данные пользователей, *используют их по своему усмотрению*, но особая опасность в том, что есть риск получения этих данных третьими лицами.

Помимо всего этого — все централизованные сервисы обмена сообщениями полностью владеют аккаунтами пользователей, что дает им возможность вносить ограничения в данные аккаунты, или совсем их закрыть. Блокировка аккаунтов

Telegram в связи с так называемыми “жалобами пользователей” является ярким примером данной особенности большинства мессенджеров.

Еще одной проблемой существующих мессенджеров является раскрытие IP-адреса пользователя при установлении подключения к центральному серверу, или Peer-to-Peer. Этот вопрос решается использованием сети Tor или таких Blockchain-инфраструктур как АДАМАНТ.

Проект АДАМАНТ призван решить вопрос доверия к защите передаваемых данных, поскольку он основан на концепции защищенного блокчейна, и его программный код открыт. Каждый может провести свой независимый аудит программного кода и собрать из него полностью рабочую систему самостоятельно.

Другим неоспоримым преимуществом технологии Blockchain является анонимность. То есть, в отличии от централизованных систем передачи сообщений, нельзя привязать переписку к конкретным лицам — благодаря отсутствию идентификаторов (нет номера телефона, аккаунтов email или соц-сетей, платежных данных, есть только обезличенный идентификатор кошелька).

АДАМАНТ обладает следующими отличительными особенностями безопасности и анонимности:

- Сообщения хранятся прямо в блокчейне;
- Нет доступа к адресной книге пользователя;
- Отсутствие доступа к местоположению пользователя;
- Личные данные пользователя не передаются;
- Нет идентификаторов пользователя — полная анонимность;
- Сообщения шифруются на устройстве отправителя, а расшифровываются на устройстве получателя. Доступа к сообщениям нет ни у кого (включая самих разработчиков) — см. схему передачи сообщений АДАМАНТ;
- Клиентское приложение никогда не передает приватный ключ или мнемоник-фразу по сети. Все работа производится на устройстве пользователя;
- Переписка не хранится на устройстве вообще — история сообщений подгружается напрямую из блокчейна;
- В отличие от P2P-мессенджеров, нельзя получить IP-адрес пользователя;
- Программные коды мессенджера и блокчейна открыты;
- Аккаунт АДАМАНТа не может быть закрыт, заблокирован или ограничен никем, включая разработчиков.

Правовой аспект гарантий тайны переписки

Юрисдикция большинства стран мира гарантирует неприкосновенность личной жизни и тайны переписки на уровне таких базовых документов, как конституция.

Например, Конституция РФ, статья 23:

1. *Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.*
2. *Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения.*

Другой пример — Конституция Италии, статья 15:

“Свобода и тайна переписки и всех других видов связи ненарушимы. Ограничение их может иметь место лишь в силу мотивированного акта судебной власти, с соблюдением гарантий, установленных законом.”

Однако правительства всячески пытаются нарушить эти принципы, и гражданам приходится искать способы, чтобы защищать свои права.

АДАМАНТ создан для защиты вашей личной жизни.

Хранение сообщений в АДАМАНТе

Все сообщения в АДАМАНТе хранятся децентрализовано в блокчейне.

Это обеспечивает:

- Надежное и избыточное хранение списка сообщений;
- Невозможность изменить сообщения “задним числом”;
- Заверенную достоверность источника и получателя, защита от атаки MITM (атака будет обнаружена — изменится идентификатор-кошелек отправителя);
- Доступ с любого устройства — как при централизованном хранении;
- Надежная и подтверждённая блокчейном доставка сообщений;
- Безопасность, обеспеченная шифрованием по схемам Ed25519 EdDSA, Curve25519, Salsa20, и Poly1305.

Несмотря на то, что доступ ко всем зашифрованным сообщениям имеет любой желающий, чтение (расшифровка) конкретных сообщений возможна только источником и получателем, что обеспечивается современными средствами криптографии. Блокчейн, и в частности, Bitcoin, доказали надежность такого подхода — при том, что баланс всех кошельков публично доступен, еще не было случаев получения к ним доступа путем “взлома” ключей шифрования.

Расчетная система

В современном мире остро стоит вопрос доступности удобных и надежных платежных инструментов, особенно на территориях, где применяются валюты с большой инфляцией, и где применение традиционных платежных систем ограничено в силу различных причин.

Технологии Bitcoin и Blockchain уже показали, что способны решить эти проблемы. В настоящее время существует множество цифровых валют, со своими преимуществами и недостатками.

АДАМАНТ включает собственную платежную единицу — токен ADM, которая:

- Используется для обеспечения инфраструктуры в виде комиссий за передачу сообщений, прямые переводы, и дополнительные функции системы;
- Обладает большой скоростью транзакций (время блока — 5 сек.);
- Удобна для прямых переводов собеседнику прямо в окне чата;
- Не зависит от сторонних сервисов и блокчейнов (АДАМАНТ построен на независимом блокчейне).

ADM является Utility-токеном инфраструктуры АДАМАНТ, который используется для поддержания внутренних операций.

Бонусы для владельцев токенов

Все нераспределенные в рамках ICO-кампании токены АДАМАНТа, будут постепенно и пропорционально начислены на балансы всех текущих владельцев. Таким образом в течение года-двух, мы стимулируем владельцев к принятию стратегии накопления токенов вместо обычной спекулятивной продажи в момент выхода на биржи. Эта акция стимулирует пользователей к активному использованию сети АДАМАНТ.

Подробный план этого процесса распределения нераспроданных токенов смотрите в финансовой части настоящего документа — раздел “АДАМАНТ Растет”.

АДАМАНТ Бизнес

Помимо стандартных для мессенджеров функций передачи сообщений и файлов, АДАМАНТ будет включать возможность цифровой подписи передаваемых документов для организации договорных соглашений.

АДАМАНТ предусматривает интеграцию внутренней “платежной системы”, то есть, возможность передачи токенов прямо в рамках чата, помимо присоединения документов и файлов. Таким образом, во время диалога можно заключить

какое-либо соглашение, и произвести его оплату. Поскольку данные хранятся в блокчейне, они не могут быть изменены в будущем.

В ряде случаев компаниям будет интересно использовать не общий блокчейн ADM, а аналогичный частный блокчейн, работающий только внутри компании и между ее партнерами. Такую возможность предоставляет АДАМАНТ Бизнес.

Для территориально-распределенных компаний блокчейн позволяет значительно снизить издержки при внутренних взаиморасчетах: стоимость трансграничного перевода может быть сокращена в тысячи раз. Это особенно актуально, когда одна сумма переводится между ограниченным числом участников несколько раз в течение года, и нет необходимости конвертировать эти средства в фиатные валюты.

Расчеты внутри компании производятся в токенах, а затем, в определенные периоды, компания конвертирует их в фиат.

Другим возможным применением блокчейна для организаций является связка токенов с каким-либо ресурсом — таким, как премиальные, трудоемкость, или стаж работы.

Платформа АДАМАНТ станет удобным и эффективным бизнес-инструментом.

Обзор альтернативных решений и их сравнение

Мессенджеры — наиболее популярный и доступный способ коммуникаций в современном мире. Количество различных мессенджеров исчисляется сотнями, а количество пользователей в мире, которые используют хотя бы один мессенджер приближается к 100% от всего числа пользователей смартфонов и ПК.
Однако количество мессенджеров, работающих без централизованного сервера, а также ориентированных на безопасность и анонимность, значительно меньше.

Поскольку основными особенностями АДАМАНТа являются безопасность и анонимность, в этом сравнении присутствуют только альтернативные решения (поэтому из сравнения исключены такие мессенджеры как Kik Messenger, Skype, Google Hangouts и прочие).

Из-за того, что безопасность-анонимность и удобство в ряде случаев стоят по разные стороны, в нашем сравнении в качестве преимущества учитывается соответствие мессенджера именно критериям безопасности и анонимности. Например, если мессенджер отображает статус сообщения как “прочитано” — это ущерб анонимности в угоду удобства.

Из сравнения исключены также мессенджеры, которые в настоящее время не имеют работающего прототипа: Echo, Status, Crypviser; и мессенджеры, которые работают только на настольных компьютерах (и не работают на смартфонах): RetroShare, Tox, Bitmessage, Ricochet.

	ADAMANT	WhatsApp	Telegram	Facebook Messenger	Connect.im	Signal	Dust	Ring
Открытый исходный код протокола и приложения	Да	Нет	Закрытый код серверной части, открытый код протокола передачи и клиентов	Нет	Закрытый код серверной части, открытый код протокола передачи и клиентов	Да	Нет	Да
Отсутствие централизованного хранения данных	Все данные распределённо хранятся в Blockchain	Оператор хранит данные всех переписок – включая изображения, видео и файлы	Оператор хранит всё, кроме данных «зашифрованных чатов»	Оператор хранит данные всех переписок – включая изображения, видео и файлы	Peer-to-peer, но есть промежуточные серверы для хранения недоставленых сообщений	Оператор может логировать все данные на серверах	Всё хранится и просматривается оператором	Peer-to-peer, но есть промежуточные серверы для хранения недоставленых сообщений
Разработчики / провайдер не имеет возможности заблокировать аккаунт пользователя	Да	Имеет / Блокируют	Имеет / Блокируют	Имеет / Блокируют	Имеет	Имеет	Имеет / Блокируют	Имеет
Отсутствие явной идентификации пользователя	Да	Идентификация по номеру телефона	Идентификация по номеру телефона	Идентификация по аккаунту Facebook или номеру телефона	Идентификация по номеру телефона	Идентификация по номеру телефона	Идентификация по профилю Facebook или номеру телефона	Создание аккаунта в децентрализованной сети Ring
End-to-end шифрование (без возможности чтения сообщений разработчиком)	Да	Потенциально есть возможность чтения разработчиком	Потенциально есть возможность чтения разработчиком	Потенциально есть возможность чтения разработчиком	Да	Да	Потенциально есть возможность чтения разработчиком	Да
Не получает адресную книгу	Да	С разрешения пользователя	С разрешения пользователя	С разрешения пользователя	С разрешения пользователя	С разрешения пользователя	С разрешения пользователя	С разрешения пользователя
Не получает местоположения	Да	С разрешения пользователя	С разрешения пользователя	С разрешения пользователя	С разрешения пользователя	Да	С разрешения пользователя	Да
Не передает приватный ключ по сети	Да	Исходный код для проверки закрыт.	Исходный код для проверки закрыт.	Исходный код для проверки закрыт.	Хранит на сервере в зашифрованном виде	Да	Исходный код для проверки закрыт.	Да
Не хранит историю сообщений и другую информацию об использовании на устройстве	Да	Хранит	Хранит	Хранит	Хранит	Хранит	Удаляет сообщения с устройств обоих конечных пользователей	Хранит
Не раскрывает IP-адрес пользователя	Да	Доступен оператору	Доступен оператору	Доступен оператору	Доступен оператору	Доступен оператору	Доступен оператору	Взаимодействует с децентрализованной сетью Ring
Невозможность получения уведомления о прочтении и статуса пользователя	Да	Все уведомления Включены по-умолчанию	Можно скрыть только статус “Last Seen”	Только переключение в статус “Неактивен”	Да	С разрешения пользователя	Принудительное уведомление о прочтении. Статуса не просмотрено.	Да

Таблица сравнения находится по ссылке:
https://adamant.im/docs/ru-adamant-messenger-comparison-table-plain.png

Таким образом, АДАМАНТ призван решить вопросы конфиденциальности и безопасности.

Техническое решение

Архитектура системы

АДАМАНТ — децентрализованная система на основе алгоритма с делегированным доказательством доли (DPoS). Этот выбор основан на необходимости соответствовать определенным критериям:

- DPoS позволяет надежно подтверждать сделки за 5 секунд.
  Это время критично для реализации быстрой передачи сообщений;
- DPoS уменьшает стоимость поддержания системы — для этого не требуется вычислительных мощностей и расхода электричества (по сравнению с PoW);
- Фиксированные комиссии за транзакции;
- Хорошая масштабируемость и надежность.

Система АДАМАНТ состоит из двух видов узлов:

1. Полных нод, которые распределенно хранят и обслуживают всю базу данных блокчейн, а также участвуют в формировании новых блоков;
2. Легких клиентов (лайт-клиенты), которые занимаются шифрованием данных на своей стороне с последующей их передачей в блокчейн.

Однако, все операции с базой blockchain выполняются полными нодами, с которыми легкие клиенты общаются по защищенному протоколу HTTPs (End-to-End шифрование), используя специальное API для передачи данных в формате JSON.

В качестве программной основы полных нод используется:

- Сервер на ОС Linux (Ubuntu). Возможна установка на других платформы через приложение Docker;
- Сервер приложений Node.JS;
- PostgreSQL Server для хранения блокчейна.

Лайт-клиенты представляют из себя:

- Прогрессивное Веб-приложение (PWA) — веб-приложение для современных браузеров;
- HTML5, JS, CSS, Vue — программные языки и Веб-технологии;
- Интерфейс взаимодействия с полными нодами посредством специального API.

Для взаимосвязи между собой все узлы используют P2P-соединения поверх протокола HTTPs.

Спецификация токена АДАМАНТ

- Название токена: ADAMANT (ADM)
- Технология DPoS, Delegated Proof of Stake
- Максимальное количество токенов: 200 млн ADM
- Первоначальная эмиссия (Genesis-блок): 98 млн ADM
- Время блока: 5 секунд (17 280 блоков в день, около 6 307 200 блоков в год)
- Размер блока: вариативный (без ограничений)
- Вознаграждение за блок:
    - Первый год: 0.5 ADM за блок
    - Следующие года: вознаграждение уменьшается на 0.05 ADM до достижения 0,1 ADM
    - Период начала получения вознаграждений: с блока номер 2,000,000
- Вознаграждения за транзакции (плата за транзакции):
    - Прямая передача токенов: 0.5 ADM
    - Передача сообщения: 0.001 ADM за каждые 256 символов в UTF-8 (примерно). Комиссия за передачу сообщения может быть адаптирована в дальнейшем в зависимости от рыночной цены токена.
    - Обновление информации профиля: 0.05 ADM
    - Загрузка аватара: 0.1 ADM
    - Передача изображения (без хранения в блокчейне): 0.05 ADM за каждые 100 КБ
    - Передача документа (с хранением в блокчейне): 10 ADM за 1 КБ
    - Подписание документа: 100 ADM
    - Регистрация делегата: 3000 ADM
    - Голосование за делегата: 50 ADM
- Первоначальное начисление при создании кошелька:
    - 0.49 ADM до блока 6 300 000 (около года) — 490 бесплатных сообщений
    - Далее каждые 125 000 блоков первичное начисление уменьшается на 0.01 ADM до достижения минимума 0.01 ADM (еще около года)
- Программный код: открытый (GNU GPLv3)
- Порты по умолчанию: 36666 для MainNet, 36667 для TestNet

Независимый блокчейн

Современные тенденции использования блокчейна Ethereum в случае АДАМАНТа не подходят. Это объясняется довольно высокой стоимостью “газа” (комиссии), который необходим для проведения каждой транзакции, включая все транзакции по передаче сообщений. АДАМАНТ же построен на независимом блокчейне, поэтому стоимость передачи сообщений значительно ниже и может быть адаптирована в зависимости от цены токена в будущем.

Кроме того, не подходит и технология Proof of Work, поскольку стоимость поддержания такой инфраструктуры высока, и с увеличением количества участников комиссия за транзакции также будет расти.

По этим причинам для реализации серверной части (блокчейна) использован программный код проекта Lisk, который был расширен для получения необходимой функциональности.

Архитектура АДАМАНТ достаточно адаптивна, чтобы при необходимости можно было вносить изменения в цену комиссий за транзакции.

Транзакции в АДАМАНТе

Каждый блок включает в себя вариативное количество транзакций. Для того, чтобы транзакция была подтверждена, необходимо от 6 до 10 подтверждений (это важно только для транзакций передачи токенов и подписания документов, сообщения же приходят после первого подтверждения). Виды транзакций в сети:

1. Прямая передача токенов
2. Передача сообщения
3. Обновление профиля, адресной книги, и настроек, хранимых в блокчейне
4. Загрузка аватар-изображения
5. Создание группового чата
6. Закрытие (сокрытие) чата
7. Передача документа (хранение на нодах)
8. Подписание документа
9. Регистрация делегата
10. Голосование за делегата

Транзакции требуют оплату за их проведение, она делится между делегатами в виде платы за поддержание сети (см. спецификацию токенов).

Поддержка инфраструктуры и майнинг (форжинг) ADM

Инфраструктура АДАМАНТ поддерживается системой распределенных серверов, на которых выполняются полные ноды (узлы). Расходы на поддержку серверов покрываются токенами ADM (“майнинг”):

1. Комиссии за транзакции
2. Вознаграждение за создание блоков

Чтобы участвовать в майнинге, нода должна зарегистрироваться в качестве делегата сети, и получить голоса других пользователей АДАМАНТа. Плата за регистрацию делегата — 3000 ADM. Пользователь АДАМАНТа, голосующий за делегата, оплачивает 50 ADM.

Протокол/алгоритм функционирования схемы DPoS базируется на голосовании, происходящем в режиме реального времени (на основе уровня репутации участников сети), что позволяет выбрать перечень лиц (делегатов-узлов), наделенных доверием. Эти лица, после избрания, имеют право создавать и верифицировать блоки для включения их в цепь блокчейна, а также препятствовать вторжению посторонних в этот процесс. Этот перечень доверенных лиц создает блоки по очереди, в случайном порядке, который меняется каждый раунд.

Делегаты производят новые токены при создании блоков.

Количество производимых токенов постепенно увеличивается. В начале существования системы — 0.5 ADM за 1 блок, но каждые 6 307 200 блоков (приблизительно год) это число будет уменьшаться на 0.05 ADM до достижения 0,1 ADM. Увеличение вознаграждения будет мотивировать делегатов справляться с возрастающей нагрузкой сети.

Исходя из расчетов, делегаты будут получать вознаграждения в течение более 140 лет. В дальнейшем инфраструктура будет поддерживаться только благодаря комиссиям за транзакции.

Количество активных делегатов, участвующих в процессе создания блоков — 101. В случае, если делегатов меньше, 101 голос распределяется среди существующих узлов сети (полных нодов). Минимальное количество узлов — 3.

Система становится более стабильной и надежной с увеличением количества узлов.

Для создания каждого нового блока с использованием DPoS происходит голосование, в результате которого выбираются 101 делегат из пула делегатов для создания последующих 101 блоков.

Голосование проводят узлы автоматически на основании доверия к делегату, а также времени его нахождения в онлайн. После того как делегаты выбраны, им выделяется

порядок формирования блоков, и они начинают их создавать. Создание 101 блока занимает приблизительно 8 минут.

Выплаты за создание блоков начинаются с 2,000,000 блока. Такая мера гарантирует, что первые участники не получат токены с наименьшими усилиями. А это в свою очередь обеспечивает создание интереса у новых пользователей и поддержание равноправия среди всех пользователей блокчейна.

Информация о блоках рассылается с интервалом в 5 секунд, каждый пакет блоков рассылается один раз от исходного узла, и по два раза от каждого получившего его узла для более быстрого распространения в рамках сети.

Транзакции, не размещенные в новом блоке, ожидают в очереди транзакций, очередь может хранить до 5000 транзакций, при этом время жизни транзакции 1080 блоков.

Если за это время транзакция не была добавлена в блок, она считается неподтвержденной и не принимается в блокчейн, удаляясь из пула ожидающих транзакций (состояние кошельков не меняется).

Для определения актуальности блокчейна используется broadhash, это хэш сформированный на основе последних 5 транзакций в блокчейне. Он позволяет быстро удостовериться, что все ноды имеют одинаковое состояние блокчейна.

Плата за транзакции равномерно делится между делегатами, участвующими в процессе формирования блока, и производится в конце каждого цикла из 101 блока.

Надежность и безопасность системы

АДАМАНТ является надежной системой, построенной на блокчейне и осуществленной благодаря реализации концепций:

- Распределенность. Блокчейн представляет из себя иммутабельную (неизменяемую) распределенную базу данных, позволяющую записывать данные, и не позволяющую вносить в них изменения, за счет чего можно использовать его для безопасного, открытого, и надежного хранения информации.
- Технология DPoS позволяет создателям контролировать блокчейн в большей мере по сравнению с PoW. В случае с PoW можно подключить к сети компьютер значительно большей мощности, получив контроль над сетью.
- За счет механизма broadhash консенсуса, выбирающего наиболее длинный форк, система обеспечивает устойчивость перед воздействиями типа временной десинхронизации части сети.
- При создании кошелька генерируется BIP39-мнемокод, на основе которого вычисляется приватный ключ. Данный приватный ключ используется для

генерации публичного ключа, который однозначно определяет адрес кошелька. После этого пользователь может начинать пользоваться системой. Количество адресов кошельков стремится к бесконечности.

- Все транзакции подписаны приватным ключом, используя устойчивый алгоритм электронной подписи Ed25519 EdDSA.
- Все сообщения мессенджера шифруются на устройстве-отправителе (алгоритмы Curve25519, Salsa20, и Poly1305[1]) и расшифровываются на устройстве-получателе.
- Клиентское приложение не передает приватный ключ или мнемоник-фразу по сети. Вся работа производится на устройстве.
- В отличие от P2P-мессенджеров, нельзя получить IP-адрес пользователя.

Объем хранимых данных

В настоящее время сложно оценить объем данных, хранимых на нодах АДАМАНТа, однако можно сделать некоторые предположения.

Предполагаемый объем сообщений мессенджера — в среднем около 10,000 сообщений в день в первый год, с увеличением до 100,000 через несколько лет.

В случае длины сообщения в 100 символов, средний объем хранимого сообщения будет вычисляться как 100 символов * 2 байта * коэффициент увеличения при шифровании 1.5, то есть, около 300 байт.

В таком случае, объем хранимых сообщений в первый год можно вычислить как 10,000 сообщений * 365 дней * 300 = 1 ГБ, с вероятным нарастанием до 10 ГБ в год. Объем блокчейна АДАМАНТа в течение 10 лет может быть равен 50 ГБ или более.

Размер комиссий, полученных делегатами блокчейна для такого объема сообщений — 10,000 * 365 * 0.001 ADM = 3,650 ADM в первый год, с нарастанием до 36,500 ADM в последующие годы.

Учитывая, что делегаты будут получать вознаграждение за блоки, а также рост рыночной цены за токен ADM и низкую стоимость хранения данных — инфраструктура АДАМАНТа будет эффективно поддерживаться, а участники-делегаты будут получать заслуженные токены.

[1] Cryptography in NaCl https://cr.yp.to/highspeed/naclcrypto-20090310.pdf

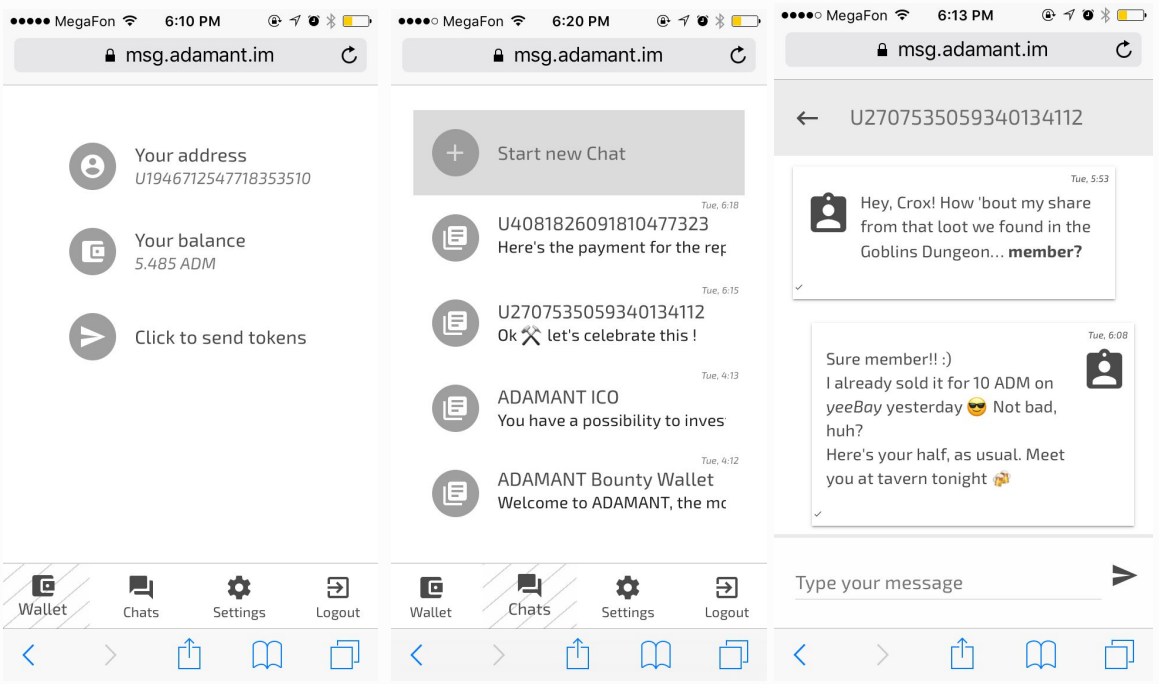
Текущее состояние проекта

На момент проведения ICO АДАМАНТ представляет собой уже функционирующий продукт с основными возможностями:

- Передача шифрованных сообщений (мессенджер)
- Хранение и передача токенов
- Получение информации о текущем состоянии блокчейна
- Инфраструктура полных узлов, доступная для масштабирования

Мессенджер АДАМАНТ

Мессенджер АДАМАНТ доступен по ссылке https://msg.adamant.im



Мессенджер АДАМАНТ на данный момент реализован в виде прогрессивного веб-приложения, работающего в большинстве браузеров. В настоящее время ведётся разработка приложений для мобильных операционных систем Android и iOS.

Рекомендованные требования для мессенджера:

- Для мобильных устройств:
  - iOS 9+
  - Android 5.0+, на других версиях ОС — мобильный браузер Chrome (версия 62+)
- Для ПК:
  - Любой современный браузер

Мессенджер включает функции хранения и передачи токенов ADM (веб-кошелёк).

Текущие возможности мессенджера:

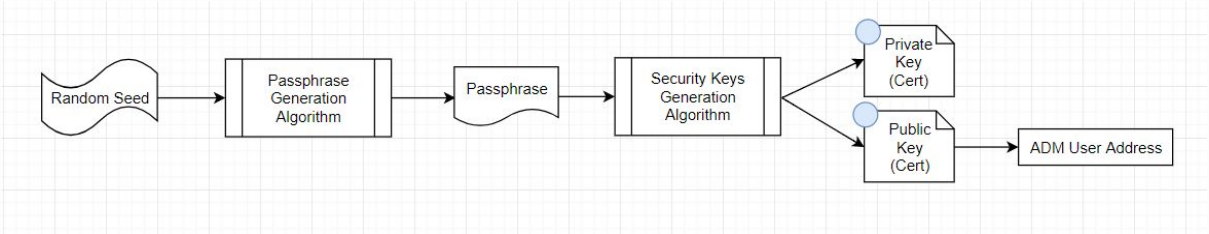
- Передача шифрованных сообщений;
- Отображение списка чатов;
- Отображение списка транзакций;
- Отображение информации о транзакции;
- Оповещения о поступающих сообщениях;
- Задание имени (ника) для кошелька в чате;
- Поддержка Emoji;
- Поддержка Markdown.

Планируемые функции:
(также см. раздел “Дорожная карта” этого документа)

- Внутренняя адресная книга;
- Профили и настройки, хранимые в блокчейне;
- Перевод токенов из чата;
- Отображение информации о переводах в чате;
- Передача изображений;
- Передача документов с хранением в блокчейне;
- Цифровая подпись документов;
- Пометка диалогов и сообщений как избранных;
- Поиск по контактам и сообщениям;
- Упрощенный вход в систему по пин-коду;
- Закрытие (сокрытие) чата;
- Групповые чаты.

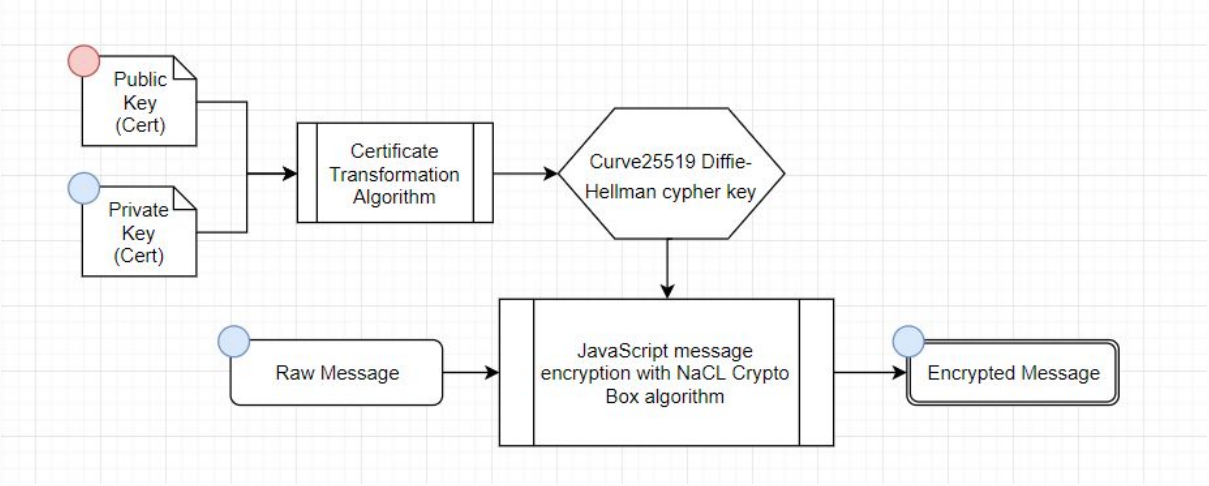
Преимущества и особенности мессенджера смотрите в разделе “Концепция АДАМАНТ” этого документа.

Схема создания аккаунта мессенджера — на устройстве пользователя:



1. Генерируется случайный Seed (порождающий элемент для генератора псевдослучайных чисел)
2. На основе Seed генерируется пароль (мнемоническая пассфраза)
3. На основе пассфразы генерируется публичный и приватный ключи
4. На основе публичного ключа генерируется ADM-идентификатор (адрес кошелька) пользователя

Схема работы мессенджера — на устройстве пользователя:



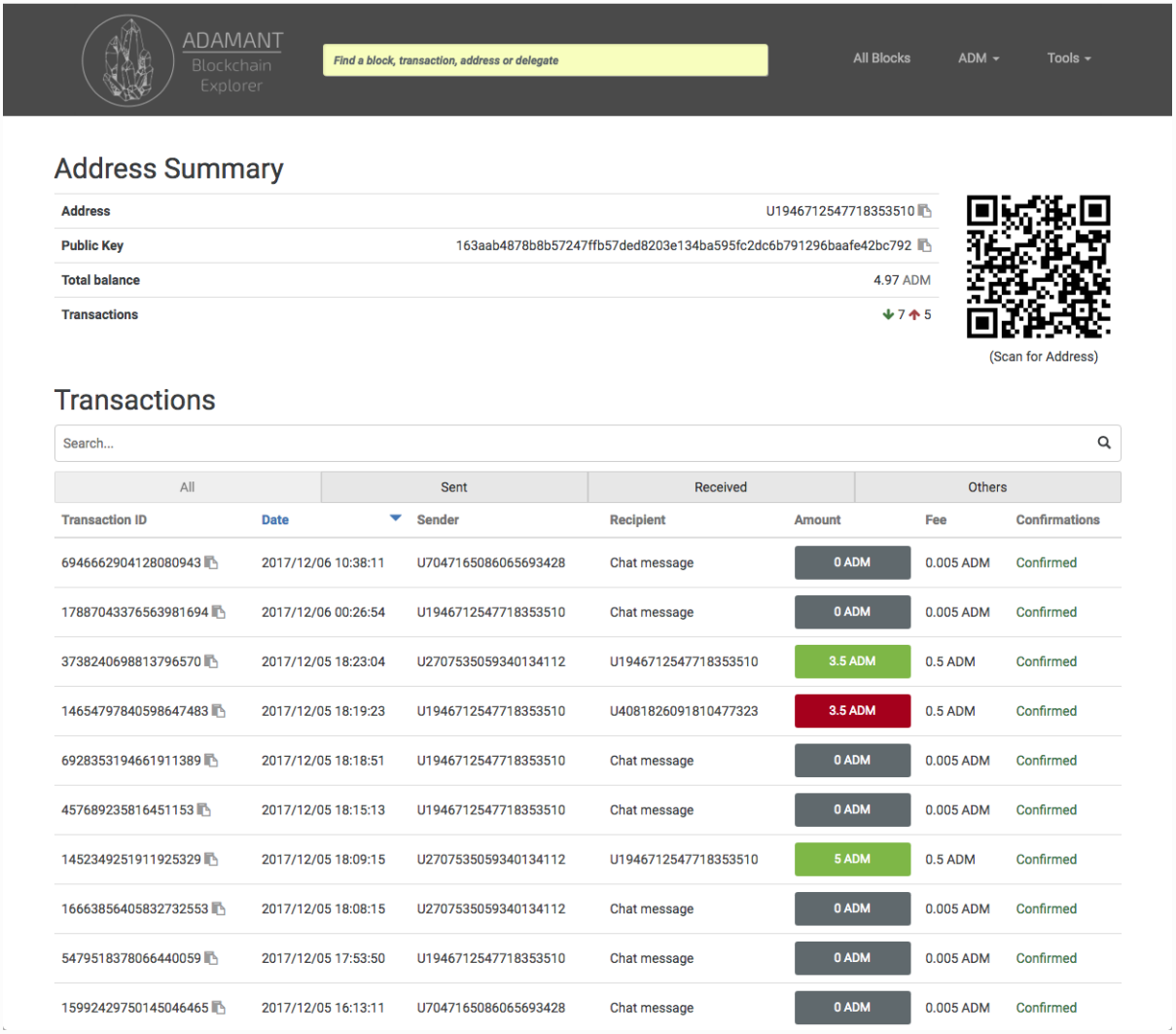
1. Сообщение пользователя шифруется на его устройстве (алгоритмы Curve25519, Salsa20, и Poly1305)
2. Зашифрованное сообщение пользователя передается на случайно выбранную ноду

Поскольку сообщения шифруются на устройстве пользователя и приходят в блокчейн уже в зашифрованном виде, а длину сообщения узнать невозможно, комиссия за передачу сообщения рассчитывается ориентировочно — 0.001 ADM за 255 символов UTF-8. Комиссия за передачу сообщения может быть адаптирована в дальнейшем в зависимости от рыночной цены токена.

Мессенджер доступен каждому желающему. В течение двух лет при создании нового аккаунта на баланс зачисляется часть токена ADM для того, чтобы с работой мессенджера можно было ознакомиться бесплатно.

Blockchain Explorer

Blockchain Explorer отображает информацию о состоянии блокчейна АДАМАНТ, показывает список блоков, список транзакций и информацию по ним, включает график активности, информацию о делегатах и сети.



Blockchain Explorer доступен по ссылке https://explorer.adamant.im

Дистрибутив полного узла

Каждый, кто хочет поддержать инфраструктуру АДАМАНТ, может развернуть полный узел, зарегистрироваться как делегат и получать вознаграждение за блоки и комиссии за транзакции (для регистрации в качестве делегата предусмотрена плата 3000 ADM, а так же нужно получить голоса пользователей).

Инструкция по установке на сайте https://adamant.im/devs/

Экономический аспект

Обоснование ценности токена

ADM — токен с ценностью, обеспеченной платой за передачу сообщений и данных. Это плата за гарантированные анонимность и защищенность данных. АДАМАНТ Бизнес также включает функции подписи документов.

Дополнительный интерес токена ADM обеспечивается распределением нераспроданных на ICO токенов. Пользователи, которые хранят на своих кошельках токены ADM, ежемесячно получают их прирост, пропорциональный своим балансам.

ADM является Utility-токеном, используемым для внутренних целей системы, и не предназначен для спекулятивных целей или извлечения прибыли.

Эмиссия токенов

С момента запуска блокчейна создан генезис-блок — кошелек первоначальной эмиссии в размере 98 млн ADM.

Распределение первоначальной эмиссии:

- 75% (73,500,000 ADM) — кошелек для проведения ICO;
- 4% (3,920,000 ADM) — резерв на разработку и поддержку инфраструктуры;
- 4% (3,920,000 ADM) — резерв на маркетинговые кампании АДАМАНТ Бизнес;
- 9% (8,820,000 ADM) — вознаграждение учредителей;
- 8% (7,840,000 ADM) — кошелек Adoption на обеспечение кампании Bounty и первоначальных начислений пользователям.

Максимальное (конечное) количество токенов — 200 млн единиц.

Таким образом, 102 млн ADM (а также комиссии за транзакции) будут использованы в качестве платы майнерам за поддержку сети.

О вознаграждениях за форжинг смотрите в разделе “Поддержка инфраструктуры и майнинг (форжинг) ADM”.

Привлечение средств на разработку и развитие проекта (кампания ICO)

Для завершения разработки АДАМАНТа, его поддержки и развития, планируется привлечь средства партнёров на Pre-ICO и ICO, благодаря распределению токенов ADM из генезис-блока (объем кошелька для проведения ICO — 73,500,000 ADM).

Поскольку ADM является Utility-токеном, направленным на поддержание инфраструктуры АДАМАНТа и обеспечивающим внутренние транзакции, покупка токенов ADM возможна гражданам всех стран мира, во всех юрисдикциях.

Все нераспределенные токены кошелька ICO будут начислены пользователям кошельков АДАМАНТа согласно плану, представленному в разделе “АДАМАНТ Растёт”.

Этап Pre-ICO прошел с 14.12.2017 по 25.01.2018. На текущий момент проходит этап ICO, сроки проведения которого: 30.01.2018—30.06.2018.

- Способ проведения: автоматическая система приема криптовалюты на странице https://adamant.im/ico/
- Получение токенов ADM: автоматическая отправка токенов на кошелёк партнёра;
- Принимаемые криптовалюты (планируется): ETH, BTC, BCH, DASH, DOGE, LTC, ETC, LSK;
- Цена токена: от 0.0002 ETH до 0.0004 ETH за 1 ADM. Цена токена в других криптовалютах пересчитывается по отношению к ETH;
- Минимальная сумма участия: нет
- Этапы ICO:
    - Первый:
        - 30.01.2018—14.02.2018
        - Цена токена: 1 ADM = 0.0002 ETH
    - Второй:
        - 15.02.2018—28.02.2018
        - Цена токена: 1 ADM = 0.0003 ETH
    - Третий:
        - 01.03.2018—30.06.2018
        - Цена токена: 1 ADM = 0.0004 ETH
- Бонусы (действуют на каждом этапе):
    - от 20 до 30 ETH: +20% ADM
    - от 30 до 50 ETH: +30% ADM

    - от 50 до 90 ETH: +40% ADM
    - от 90 и более ETH: +50% ADM

Планирование бюджета проекта

Собранные в ходе ICO средства будут расходоваться на завершение разработки АДАМАНТа, его поддержку и развитие.

Soft cap — $500,000. Hard cap — $8,000,000.

Нижний порог бюджета обеспечивает разработку основных функций мессенджера и поддержку инфраструктуры, а средства, его превышающие позволяют ускорить разработку и привлечь максимальное количество пользователей.

Общий план расхода привлеченных средств на два года:

- Поддержка инфраструктуры — 10%
    - Серверы
    - Зарплаты сотрудникам
- Разработка — 30%
    - Зарплаты сотрудникам
    - Аренда офисных помещений
    - Техническое оснащение
    - Выход на криптовалютные биржи
    - Внешние консультанты
- Внешний аудит кода и безопасности — 10%
- Привлечение пользователей — 50%
    - Оффлайн-кампании и участие в конференциях
    - Зарплаты сотрудникам
    - Контекстная реклама
    - Реклама на тематических ресурсах
    - Размещение тематических статей

«АДАМАНТ Растёт»

С целью реализации справедливого распределения токенов и увеличения активности использования мессенджера, все нераспроданные на ICO токены ADM кошелька ICO будут равномерно начислены на балансы текущих обладателей — ежемесячно каждый несистемный кошелек с балансом больше 100 ADM будет расти на 5%.

Поскольку ADM является Utility-токеном, который используется для поддержания инфраструктуры сети, система АДАМАНТ Растет создана исключительно для защиты концептуального аспекта и не направлена на извлечение прибыли.

Срок начислений — до исчерпания кошелька ICO.

Таким образом, чем раньше вы поддерживаете АДАМАНТ, и чем дольше храните токены, тем больше бонусного начисления вы получаете.

- Старт распределения: 11.04.2018
- Периодичность распределения: ежемесячно
- Процент начислений: 5%
- Окончание распределения: до исчерпания кошелька ICO

Не участвуют в распределении токенов:

1. Системные кошельки (ICO, вознаграждение учредителей, Adoption, кошельки резерва)
2. Кошельки, баланс которых менее 10 ADM

Информация о каждом раунде распределения открыта, доступна в эксплорере, и будет публиковаться на официальных ресурсах Проекта.

Размещение токена ADM на криптовалютных биржах

После завершения кампании ICO планируется размещение токенов ADAMANT (ADM) для свободного обмена на криптовалютных биржах.

Адаптация и продвижение

Мессенджеры являются удобным средством коммуникаций. Пользователей мессенджеров становится все больше, постепенно приближаясь к отметке в 100% населения.

АДАМАНТ найдет свою категорию пользователей, которым важна безопасность передаваемых сообщений в совокупности с удобством передачи токенов.

Особенностью релиза нового мессенджера является его неравномерная скорость прироста количества пользователей. Изначально количество новых пользователей растет медленно, в дальнейшем, по мере того, как новые пользователи приглашают своих друзей и знакомых, начинается экспоненциальный рост количества активных пользователей.

Проект АДАМАНТ предусматривает следующие кампаний для увеличения количества активных пользователей:

- Проведение ICO, привлечение пользователей крипто-сообщества;
- Bounty-кампания;
- Кампании в социальных сетях;
- Рекламные кампании (онлайн и оффлайн);
- Участие в конференциях;
- Первоначальные начисления на кошельки пользователей;
- АДАМАНТ Бизнес для бизнес-пользователей.

Первоначальные начисления на кошельки пользователей

Все транзакции в блокчейне требуют минимальной комиссии.
Это необходимо для поддержания инфраструктуры сети.

Для того, чтобы пользователи могли ознакомиться с преимуществами АДАМАНТа бесплатно, предусмотрены первоначальные начисления при создании нового кошелька:

- 0.49 ADM до блока 6 300 000 (около года) — 490 бесплатных сообщений
- Далее каждые 125 000 блоков первичное начисление уменьшается на 0.01 ADM до достижения минимума 0.01 ADM (еще около одного года)

Поскольку комиссия за прямой перевод составляет 0.5 ADM, первичного начисления недостаточно для злоупотребления и накопления полученных токенов в одном кошельке.

Первоначальные начисления производятся в первые минуты создания аккаунта из кошелька Adoption (7,840,000 ADM). Таким образом, ориентировочное количество пользователей, которые смогут протестировать работу системы бесплатно — от 7 до 14 миллионов.

Кампания Bounty

Кампания позволяет каждому пользователю сделать вклад в продвижение мессенджера АДАМАНТ и получить вознаграждение в ADM-токенах.

Bounty-программа продлится с 14.12.2017 по 30.03.2018, и будет включать:

- Signature на сайте Bitcointalk.org;
- Активность в социальных сетях;
- Перевод и поддержка основной ветки на Bitcointalk и ветки Bounty на Bitcointalk.org;
- Перевод сайта, приложения-мессенджера, Whitepaper;
- Статьи в блогах и на сайтах;
- Размещение баннеров на веб-сайтах.

Более подробная информация о кампании Bounty — на странице https://adamant.im/bounty/

Дорожная карта проекта (2017-2018)

✓ 2017, квартал 2

✓ Разработка концепции АДАМАНТ
✓ Консультирование со специалистами отрасли
✓ Развертывание тестовой сети АДАМАНТ

✓ 2017, квартал 3

✓ Разработка Веб-приложения (кошелек и мессенджер)
✓ Создание Whitepaper

2017, квартал 4

✓ Разработка Веб-сайта
✓ Запуск рабочей сети АДАМАНТ
✓ Подготовка пакета дистрибутива узла сети (full node)
✓ Создание ADAMANT Blockchain Explorer
✓ Настройка информационных ресурсов (социальные сети, форумы и блоги)
✓ Запуск Bounty-кампаний (поощрение активных участников)
✓ Внутренний аудит безопасности
✓ Начало Pre-ICO (14.12.2017)

2018, квартал 1

✓ Завершение Pre-ICO (25.01.2018)
✓ Начало ICO (30.01.2018)
✓ Адаптация мессенджера АДАМАНТ и продвижение (маркетинг)
✓ Перевод информационных ресурсов на популярные языки
- Расширение функционала мессенджера АДАМАНТ (профили пользователей, упрощённый логин, передача файлов и токенов прямо из чата)

2018, квартал 2

- Публикация мессенджера АДАМАНТ для мобильной ОС iOS
- Масштабирование всей рабочей инфраструктуры
- Расширение функциональности мессенджера АДАМАНТ (адресная книга, групповые чаты, поиск по списку сообщений, скрытие чата)
- Завершение ICO (30.06.2018)

2018, квартал 3

- Размещение токена ADM на криптовалютных биржах
- Запуск Бизнес-версии системы АДАМАНТ (с функциями подписи документов и их хранения в базе blockchain)
- Публикация мессенджера АДАМАНТ для мобильной ОС Android
- Маркетинговые кампании

2018, квартал 4

- Независимый аудит безопасности
- Установка АДАМАНТ Бизнес компаниям-партнерам
- Маркетинговые кампании

Коллектив АДАМАНТа

Коллектив проекта включает более 20 участников
(ведущие из которых представлены ниже)

Руководитель проекта — Евгенов Павел Сергеевич

Менеджер и инноватор, под руководством которого завершены
множество проектов в ИТ и финансах. Степень MBA.
Закончил ИМЕИ по специальности Государственное и муниципальное управление.
Секретарь Молодёжной Общественной Палаты г. Москвы.

http://vk.com/p.evgenov

Ведущий разработчик — Лебедев Алексей Юрьевич

Блокчейн-энтузиаст. Сертифицированный специалист: IBM Certified Solution Designer
— IBM Rational Unified Process. Опыт работы в IT-проектах 15 лет.
Руководитель компаний ИнфоРешения и irSoftware.

lebedevau@gmail.com

Ведущий разработчик — Солодухин Дмитрий Александрович

Магистр кафедры Информационных Систем ВлГУ. Разработчик и системный архитектор информационных систем различного назначения, включая блокчейн. Специалист ИТ широкого профиля. Интересы: Lego, фото.

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

Главный дизайнер — Пихтовников Максим Константинович

Выпускник факультета Микроприборов и технической кибернетики (МИЭТ). Дизайнер и маркетолог с опытом работы в крупных международных компаниях. С 1999 года увлекается вопросами сетевой безопасности и защиты информации. IT-консультант и руководитель, коуч.

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

Менеджер продукта — Воробьев Артем Владимирович

Выпускник факультета Микроприборов и технической кибернетики (МИЭТ).

Опыт работы в IT-проектах более 10 лет.

Опыт работы в IT-стартапах более 7 лет.

Специалист IT широкого профиля.

art.vorobev@gmail.com

Связи с общественностью — Лебедев Сергей Юрьевич

Закончил архитектурно-строительный факультет Владимирского Государственного Университета.

Главный инженер проектов, предприниматель. Под руководством сдано более 50 проектов, прошедших Государственную экспертизу в области проектирования.

https://vk.com/id405481034

iOS-разработчик — Анохов Павел Викторович

Выпускник Московского Института Управления.

12 лет опыта работы в IT, от техподдержки до участия в команде разработки высоконагруженных серверных приложений.

Увлечения: разработка, сноуборд и Portal 2.

https://vk.com/realbonus

Ресурсы АДАМАНТа

- Веб-сайт: https://adamant.im
- Мессенджер: https://msg.adamant.im
- Обозреватель блоков: https://explorer.adamant.im
- Исходный код в Github: https://github.com/Adamant-im
- Твиттер: 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